kancellár.hu
az informatikai biztonság szakértője

Spambiznisz – A kéretlen levelek útja a támadótól az áldozatig

Krasznay Csaba
Kancellár.hu Kft.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Az előadás célja

- Az eddigi Networkshopokon a kéretlen levelek számos aspektusával foglalkoztak:
  - Jogi kérdések
  - Védelmi megoldások
  - Címgyűjtési technikák
  - A szűrési megoldásokkal kapcsolatos tapasztalatok
- Eddig azonban egyszer sem került szóba (a Google szerint), hogy a spamek kitől származnak és hogyan jutnak el hozzánk.
- Előadásom célja, hogy ezt az útvonalat felvázoljam.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

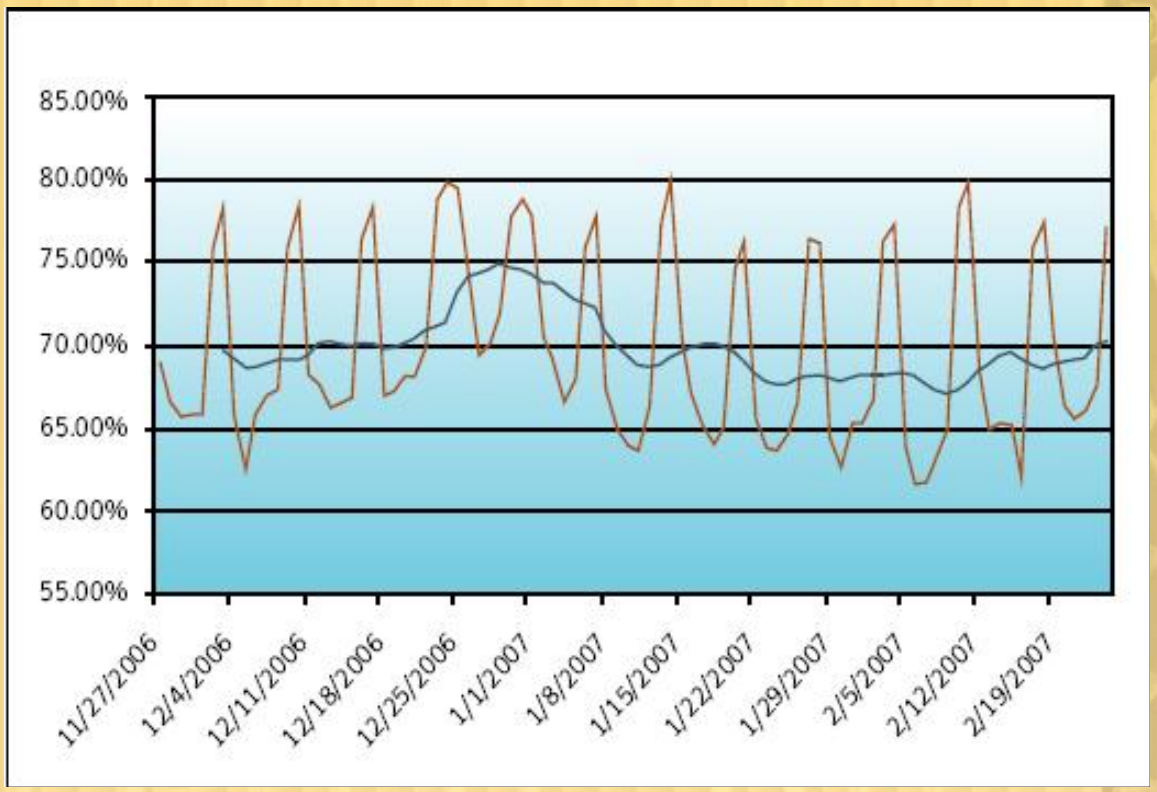
Mennyire rossz a helyzet?

- Iparági statisztikák szerint az összes elküldött e-mail kb. 40%-a minősül kéretlennek.
- Ez naponta 10 milliárd kéretlen levelet jelent.
- Ami felhasználónként átlagosan 2200 spam.
- Hála a spamvédelmi technikáknak, ezen levelek nagy részével nem találkozunk.
- Vajon ez az internet teljes sávszélességének hány százalékát jelentheti?

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

A spamek aránya az e-mail forgalomban



Forrás: Symantec, The State of Spam – March 2007

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

A kéretlen levelek típusai

- Termékekkel kapcsolatos levelek: általános termékeket és szolgáltatásokat kínáló üzenetek. Például órák, ékszerek, befektetési szolgáltatások.
- 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.
- Üzleti levelek: olyan kéretlen levelek, melyek pénzzel, tipikusan tőzsdei, vagy más üzleti befektetéssel kapcsolatosak. Például tőzsdei levelek, kölcsönök, jelzálogok hirdetései.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

A kéretlen levelek típusai

- Csalások: olyan levelek, melyek valamilyen széleskörű csalásba próbálják bevonni az áldozatot. Például ilyenek a nigériai levelek, a piramisjátékok hirdetései, a lánclevelek.
- Egészséggel kapcsolatos levelek: gyógyászati termékek és szolgáltatások hirdetései. Például ide sorolhatjuk az impotencia elleni szerek, nyugtatók, gyógynövények reklámozását.
- 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.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

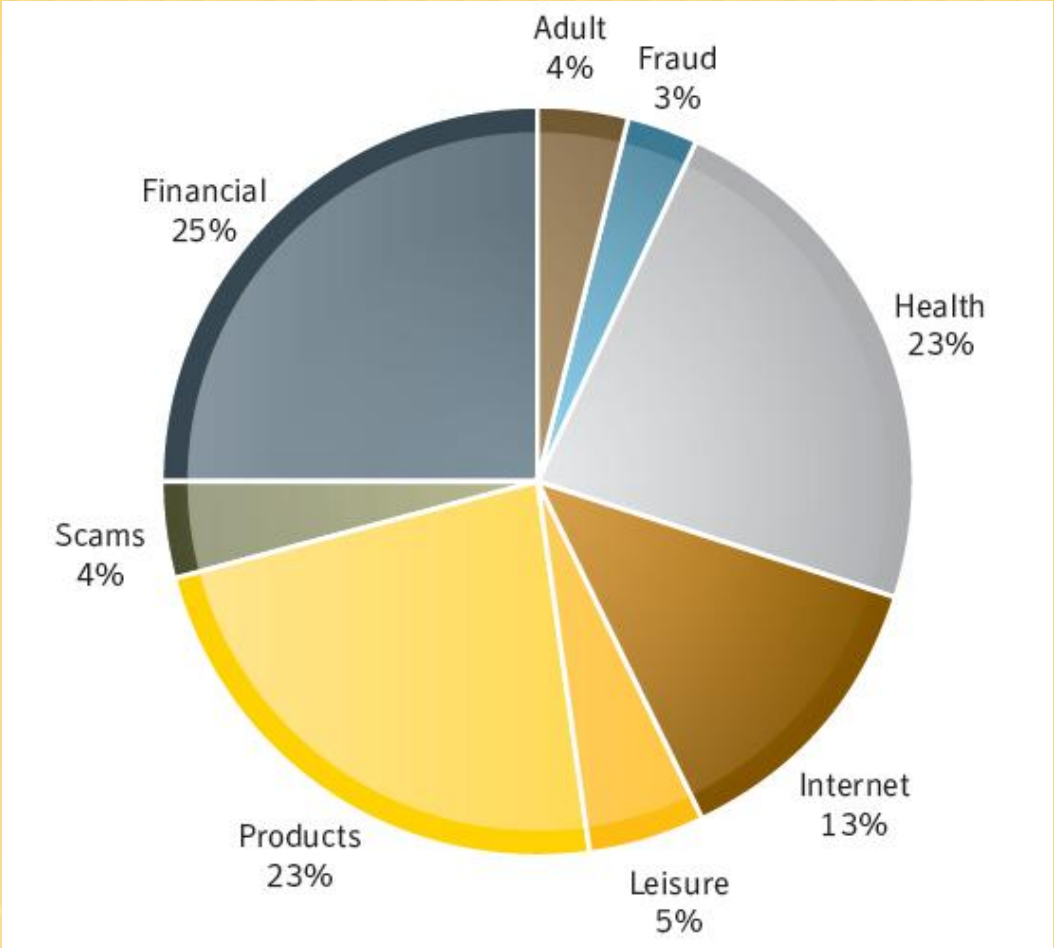
A kéretlen levelek típusai

- Szabadidővel kapcsolatos levelek: díjakkal, nyereményekkel, nyerési lehetőségekkel csábító üzenetek. Például online kaszinók hirdetései, nyaralási ajánlatok.
- Internettel kapcsolatos levelek: internetes vagy más számítógéppel kapcsolatos termékek és szolgáltatások hirdetései. Például webhostolás, web design, szoftverek.
- Politikai levelek: ilyenek egy jelölt vagy párt hirdetése kampányidőszakban. Például szavazatszerző, anyagi támogatást kérő levelek.
- Spirituális levelek: egyházi, spirituális közösségek kéretlen hirdetései. Például tagtoborzás, asztrológiai hirdetések.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

A kéretlen levelek típusai



Forrás: Symantec, The State of Spam – March 2007

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Tőzsdei csalások

- A tőzsdei spamekről a kívülálló azt hihetné, hogy a hirdetett cég áll mögötte.
- Valójában:
  - A támadó részvényeket szerez a vállalatnál;
  - A támadók hozzáférést szereznek olyan számítógépekhez, melyről a tőzsdei rendszerek elérhetők (trójai programok, phishing, stb.);
  - A mit sem sejtő vállalat kiad egy átlagos közleményt;
  - A támadó a megszerzett azonosítókon keresztül elkezd vásárolni – más pénzén;
  - Elkezdődik a spamáradat az eredeti közlemény „felturbózott” változatával;
  - A tömeg is elkezd vásárolni, amire a cég kiad egy közleményt a csalásról;
  - A cég részvénye a támadás előtti szint alá süllyed, mindenki rosszul jár, kivéve a támadót, aki a magas árfolyamon már eladott.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Tőzsdei csalások

Investors Report: 03/06/2007
THIS STOCK WILL EXPLODE ON WEDNESDAY 03/07/2007

This Weeks TOP PICK
IFTC.OB

-LOOK AT OUR RECENT NEWS!!!-

Company	:	Infotec Business SYS
Symbol	:	IFTC.OB
Current Price	:	$0.06
5 Day Target	:	$0.80
Last Traded	:	226,600

-IN THE NEWS-
Wavelit.com Announces Strategic Relationship
with Broadband Enterprises

Thursday March 1, VANCOUVER,

British Columbia--(BUSINESS WIRE)--(OTCBB:IFTC)
and Broadband Enterprises. Considered the premier
online video network, Broadband Enterprises
has been contracted to sell the pre-roll video
commercials shown before all video content on
Wavelit.com

READ OUR NEWS NOW!
IFTC.OB

THIS STOCK WILL EXPLODE ON WEDNESDAY 03/07/07

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

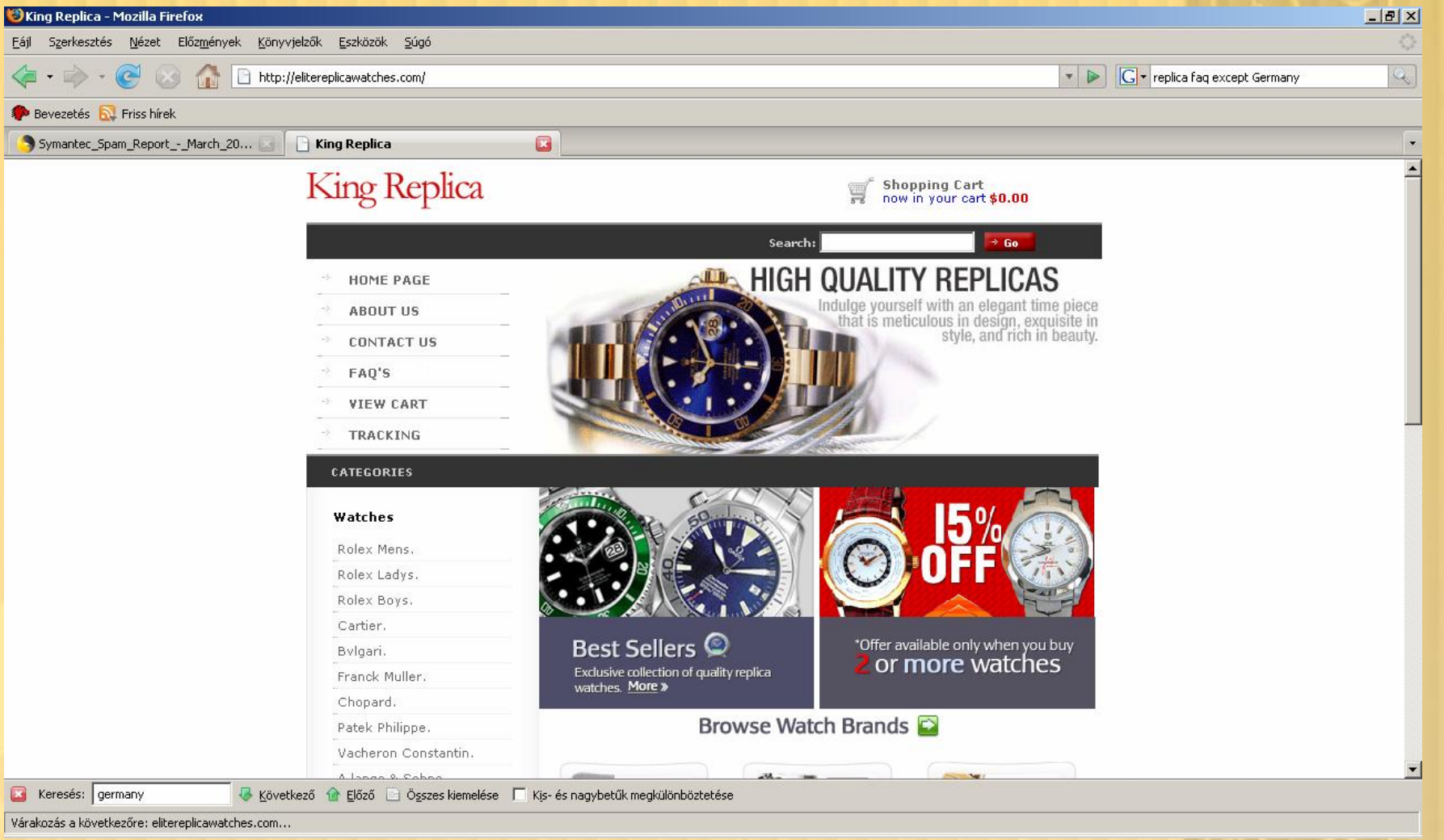
Termékhamisítások

- Idézet az Európai Bizottság 2005. október 11-én kelt sajtóközleményéből:
- ***„2005. október 10-én az Európai Bizottság újabb konkrét lépéseket hirdetett meg a termékhamisítás leküzdésére. (…) 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 jelentős szerepet játszott a másolatok kéretlen levelekben történő reklámozása és ezek webes kereskedelme.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Termékhamisítások



Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Termékhamisítások

- Idézet az oldal FAQ-jából:
  - - ***Miért vegyek másolt órát az eredeti helyett?***
  - - Azért, mert anélkül keltheted a jólét látszatát, hogy több ezer dollárt kéne kifizetned.
  - - ***Hogyan léphetek kapcsolatba az áruházzal?***
  - - Kattints ide, és küldj nekünk e-mailt!
  - - ***Világszerte szállítanak?***
  - - Igen, kivéve Svájcot, Németországot, Koreát és Szingapúrt.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Gyógyszerreklámok

- Szintén prosperáló üzletág a potencianövelők és nyugtatók illegális kereskedelme.
- Ezeket tipikusan kínai és indiai illegális gyárakban állítják elő.
- Sajnos a tét nagyobb, mint a hamisított óráknál.
- Egy 57 éves kanadai nő bizonyíthatóan olyan gyógyszertől halt meg, amit az interneten rendelt egy hamis gyógyszereket forgalmazó oldalról.
- De vajon miért találtak ezekben a gyógyszerekben stronciumot, higanyt és urániumot?

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

A spamek postásai

- A kéretlen levelekben kínált dolgok tehát a „hagyományos” alvilágtól származnak.
- De kik azok, akik képesek több milliárd ilyen üzenetet kiközvetíteni?
- A spamhaus.org szerint ők:
  - 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.

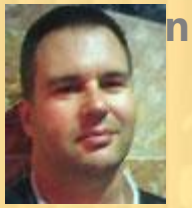
  - Leo Kuvajev: orosz származású, amerikai spammer. 2005-ben 37 millió dolláros büntetést szabott ki rá egy amerikai bíróság, azóta szökésben van.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

A spamek postásai

- 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 SpamHaus állítása szerint cége teljes körű domainszolgáltatást nyújt a spammereknek.



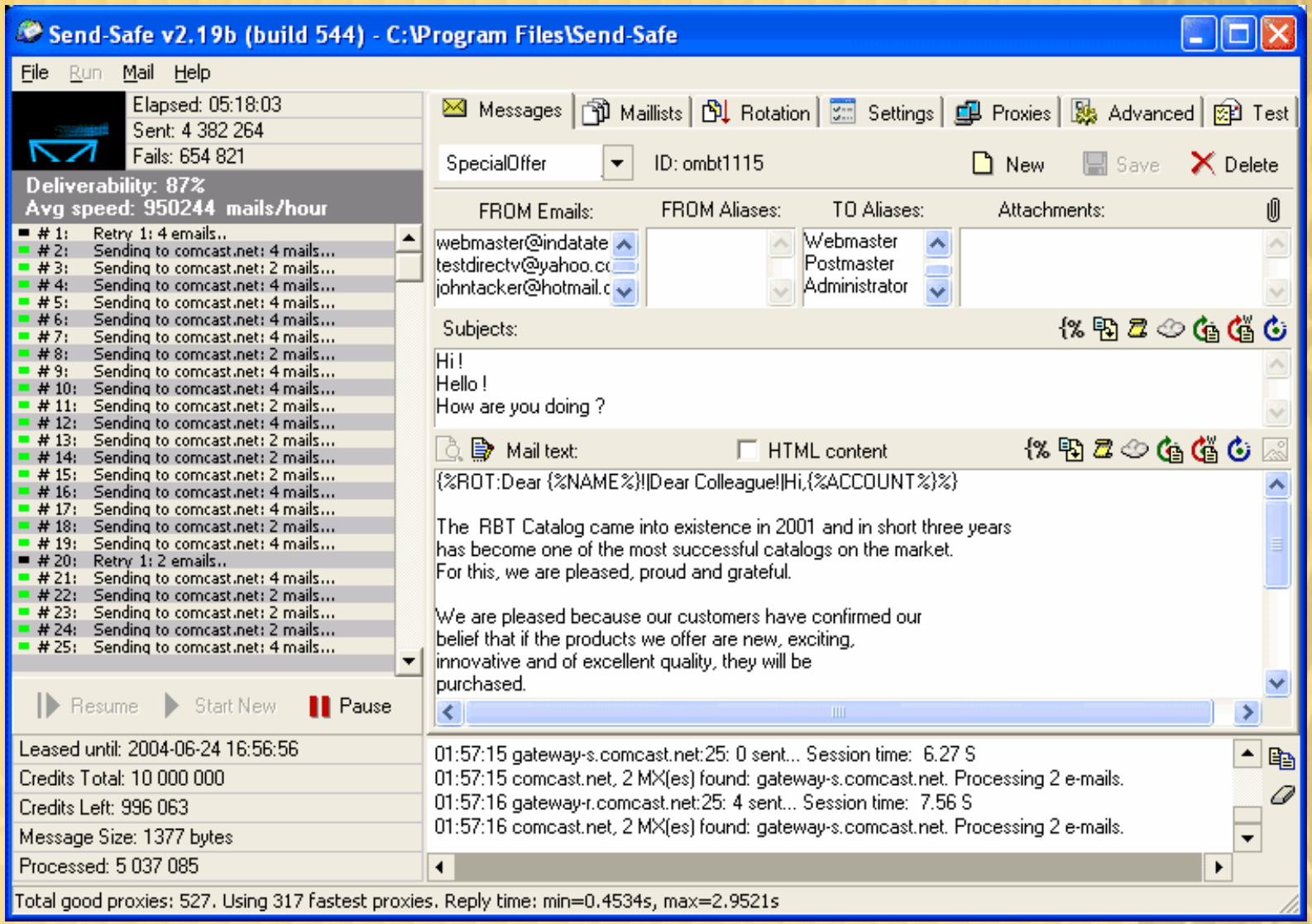
Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

Spamküldési technikák

- A spamhez két dolog kell: sok számítógép és még több e-mail cím.
- Az előző dián felsorolt személyek rendelkeznek olyan botnetekkel, melyekkel a spamküldés egyszerű.
- A botnet kialakításához 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.

kancellár.hu
az informatikai biztonság szakértője

Spamküldési technikák



Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

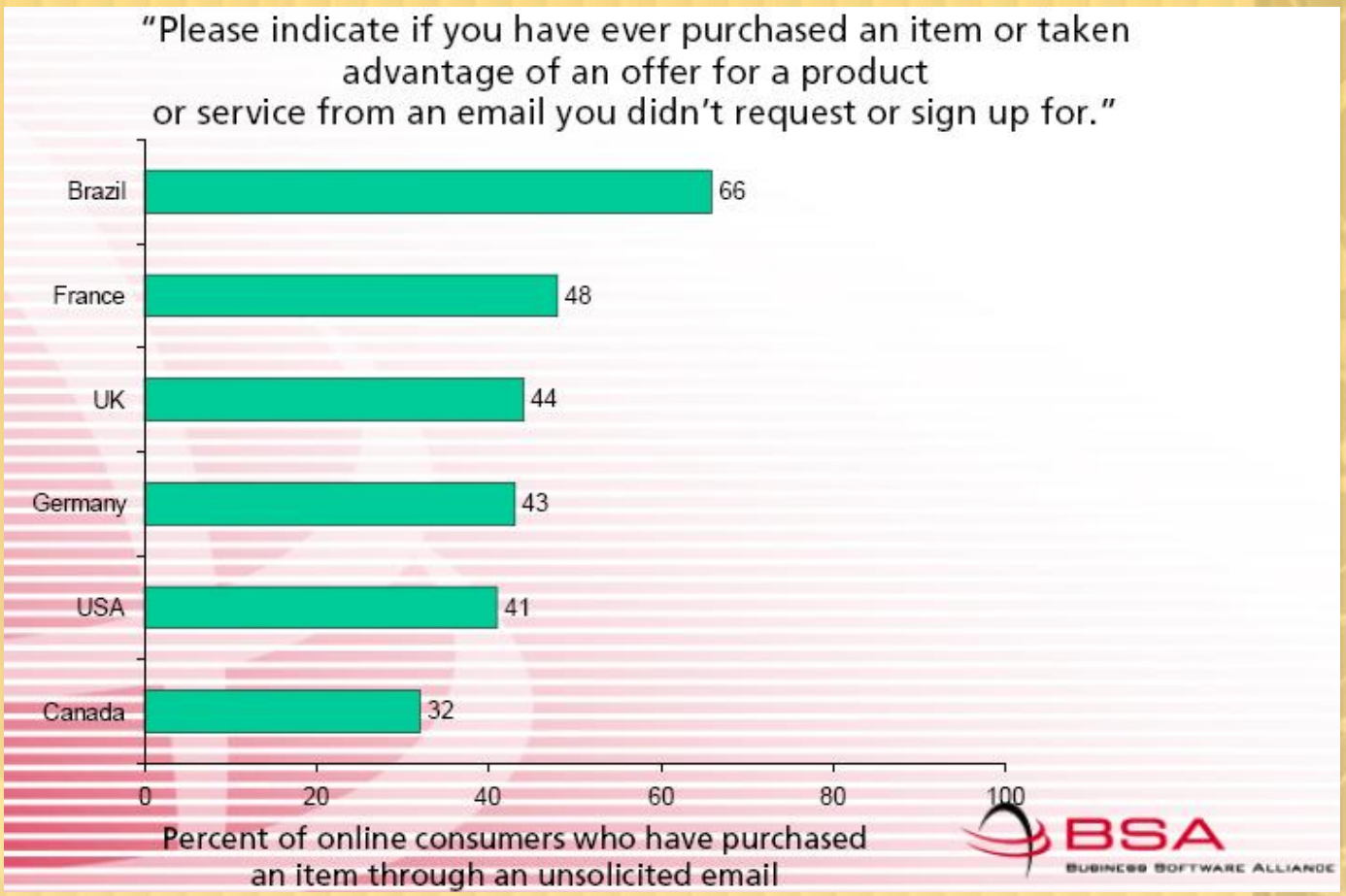
Spamküldési technikák

- Honnan szedik az e-mail címeket?
- Vírusok, férgek útján: régóta ismert a károkozóknak az a funkciója, hogy a megfertőzött gépen e-mail címek után kutatnak.
- Nyilvános forrásokból: az interneten számtalan helyen találhatók e-mail címek. Weboldalakon, Usenet oldalakon, fórumokban.
- Találgatással: az e-mail címek gyűjtése hasonlóan tud működni a jelszavak brute-force jellegű feltöréséhez. 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.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

A spamek áldozatai(?)



Forrás: Consumer Attitudes Toward Spam in Six Countries, Business Software Alliance

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Összefoglalás

- Spamet küldeni megéri, ahogy a való életben is megéri csalni.
- Az úgynevezett áldozatok ugyanazzal az attitűddel rendelkeznek, mint a való életben. Hagyják magukat becsapni.
- Amíg tehát kereslet van, addig kínálat is lesz.
- A spamvédelmi technikák éppen ezért csak tüneti kezelések.
- A valódi megoldást a hagyományos bűnüldözés jelentheti, ahogy minden más internetes támadás esetében is.

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu

kancellár.hu
az informatikai biztonság szakértője

Köszönöm szépen!

E-mail cím: krasznay.csaba@kancellar.hu
Cégünk weboldala: www.kancellar.hu
Az előadás letölthető: www.krasznay.hu

Duna Tower
1138 Budapest, Népfürdő u. 22. t: +36 1 2704tel, f: +36 1 2704fax, w: kancellar.hu