Stinnou stránkou elektronické komunikace nejsou jenom HOAXy

Josef Džubák
www.hoax.cz

HOAX

H O A X ? Co to je?

Anglické slovo, znamená v překladu:

- Mystifikace
- Podvod
- Žert
- Novinářská kachna

Kde je začátek?

Fámy se nejdříve šířily ústně - JPP

Využívá se dostupná technologie

Kliknout je tak snadné...

Hoaxy v době Internetu

Smyšlená varování před virem

PŘEDEJTE DÁL !!!

V PŘÍŠTÍCH DNECH MUSÍTE DÁVAT VELKÝ POZOR A NEOTEVŘÍT ZADNY E-MAIL NAZVANÝ POZVANKA-"INVITATION", NEZÁVISLE NA TOM, OD KOHO JE.

JEDNÁ SE O VIRUS, KTERÝ " OTEVÍRA OLYMPIJSKOU POCHODEŇ" A KTERÝ SPALÍ HARD DISK. TENTO VIRUS BUDE ODESLAN OSOBOU, KTERA VÁS MÁ VE SVÝCH KONTAKTECH. TAKŽE POKUD OBDRŽÍTE E-MAIL S NAZVEM "INVITATION" NEOTVÍREJTE HO JE TO NEJHORŠÍ VIRUS OHLAŠENÝ CNN A KLASIFIKOVANÝ SPOLECNOSTÍ MICROSOFT JAKO NEJDESTRUKTIVNEJŠI VIRUS, KTERY KDY EXISTOVAL!!!!!!!

BYL OBJEVEN VČERA ODPOLEDNE POSLETE TENTO E-MAIL VSEM, KOHO ZNATE, VASIM PRATELUM,| VSEM VASIM KONTAKTUM ČÍM VÍCE OSOB UPOZORNÍTE PŘEDEM, TÍM HŮŘE SE BUDE VIRUS ŠÍŘIT!!!

HOAX

Hoaxy v době Internetu

Vymyšlené prosby o pomoc

Nemocné děti, týraní pejsci...

Když to vymažete... tak opravdu nemáte srdce.

Ahoj, jsem 29letý otec. Já a moje žena máme spolu překrásný život. Bůh nás také obdaroval dítětem. Jméno naší dcery je Rachel a je jí 10 měsíců.
Před nedávnem lékaři zjistili rakovinu mozku v jejím malém tělíčku. Existuje jen jeden způsob, jak jí zachránit... OPERACE.
Bohužel nemáme dostatek peněz na její zaplacení. AOL a ZDNET souhlasili, že nám pomohou.Jediný způsob, jakým nám mohou pomoct je tento: Já posílám tento e-mail vám a vy jej pošlete dalším lidem. AOL bude sledovat tento e-mail a počítat, kolik lidí jej obdrželo. Každá osoba, která otevře tento e-mail a pošle ho nejméně 3 lidem nám přinese 32 centů.

Hoaxy v době Internetu

Opravdové prosby o pomoc

Kolují i několik let, přestože nejsou aktuální

● ONKOLOGICKÝ ÚSTAV Alexandra Gala v Bratislavě se obrací na nositele krevní skupiny A1B RH negativní, která by mohla zachránit život jednoho z pacientů, který zde pomalu umírá a k záchraně by potřeboval tuto neobvyklou krevní skupinu. Pokud by se našel vhodný dárce, ať zavolá na slovenské tel. číslo 00421-7-59378681. **(sch)**

+ leden 2001

Vyšlo v tisku: 4.12.2004

Hoaxy v době Internetu

Fámy z reálného života

Komunikaci po internetu využívá většina lidí a přenáší sem věci z reálného světa

Upravené polopravdy s určitým úmyslem

Účelové upravené polopravdy za účelem poškodit určitý subjekt nebo skupinu lidí

Co mají hoaxy společného

Snaží se přesvědčit svojí důležitostí

Nové nebezpečí, aktuální ohrožení, naléhavá pomoc

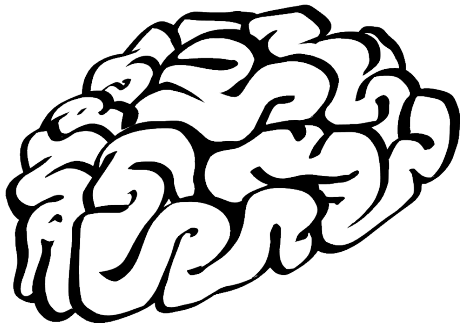
Údajný důvěryhodný zdroj

Microsoft varuje, Symantec objevil, laboratoř NASA zjistila

Výzva k dalšímu rozeslání !!!

Pošlete všem..., raději 20x dostat než..., varuj všechny...

Jak se bránit



Je-li k dispozici mozek - použij ho!

- Jednej s chladnou hlavou – rozmysli se
- Zkus najít informace z jiných zdrojů
- Jestli se tím nehodláš zabývat, raději zprávu vymaž
- Totéž platí pro „Like“ a sdílení

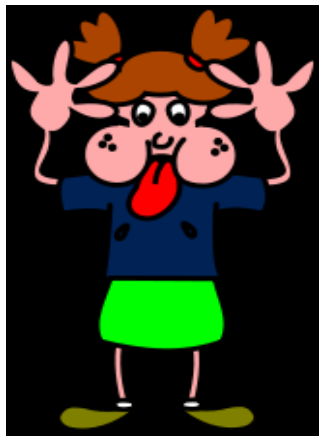
www.hoax.cz

www.snopes.com

www.cernasanitka.cz

www.museumofhoaxes.com

Je to marný



...je to marný...

je to marný...

“Já to stejně raději pošlu, co kdyby to náhodou byla pravda!“

HOAX

Řetězák neuškodí?

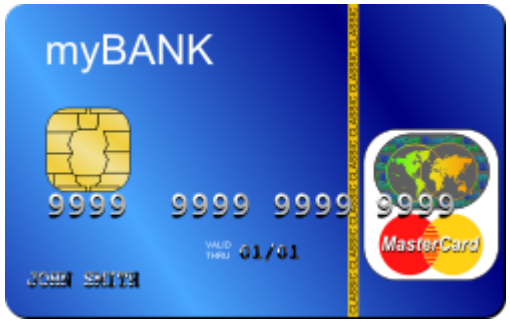
250 adres

Co si třeba zarhybařit?

P*assword*

H*arvesting*

*f*ISHING

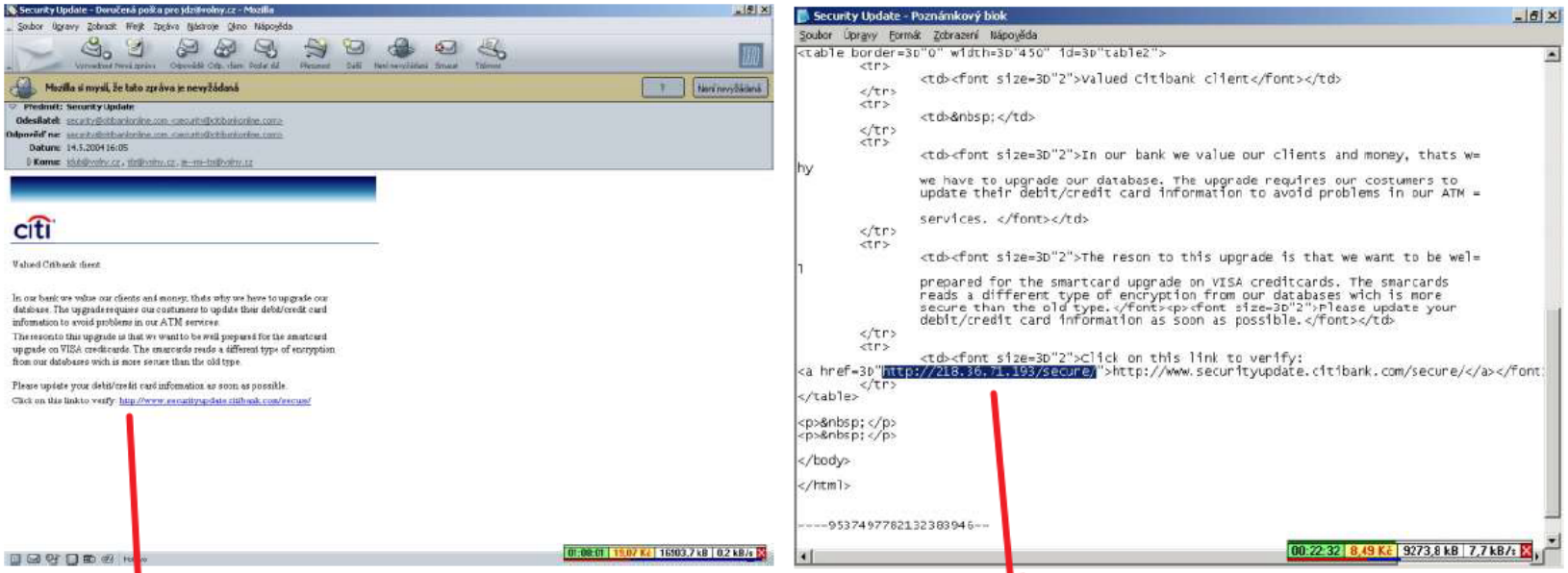


(rhybaření)

Konference SOOM 15.3.2013

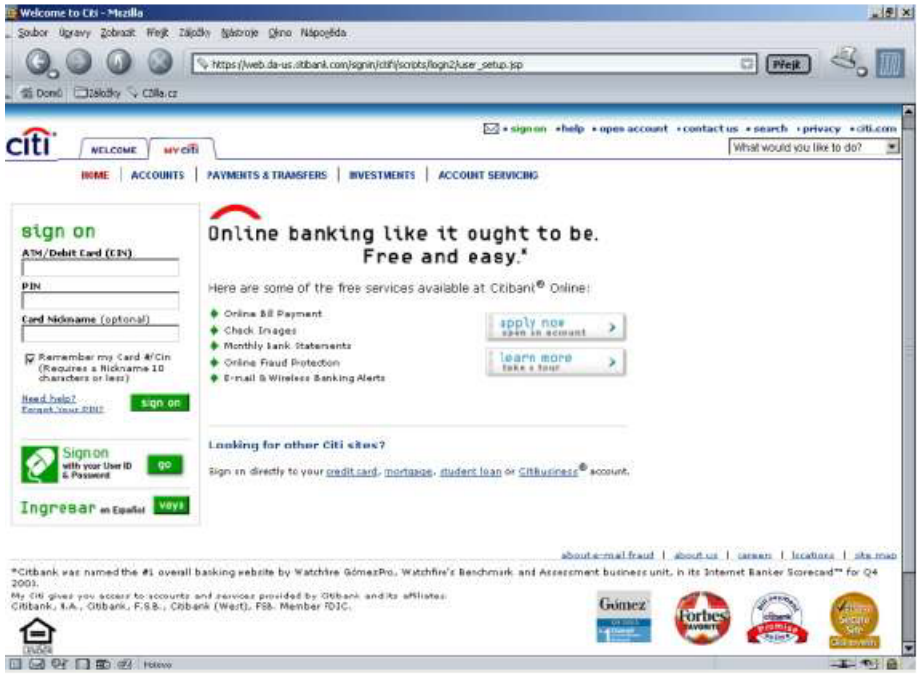
HOAX

Krok 1 - nahození návnady

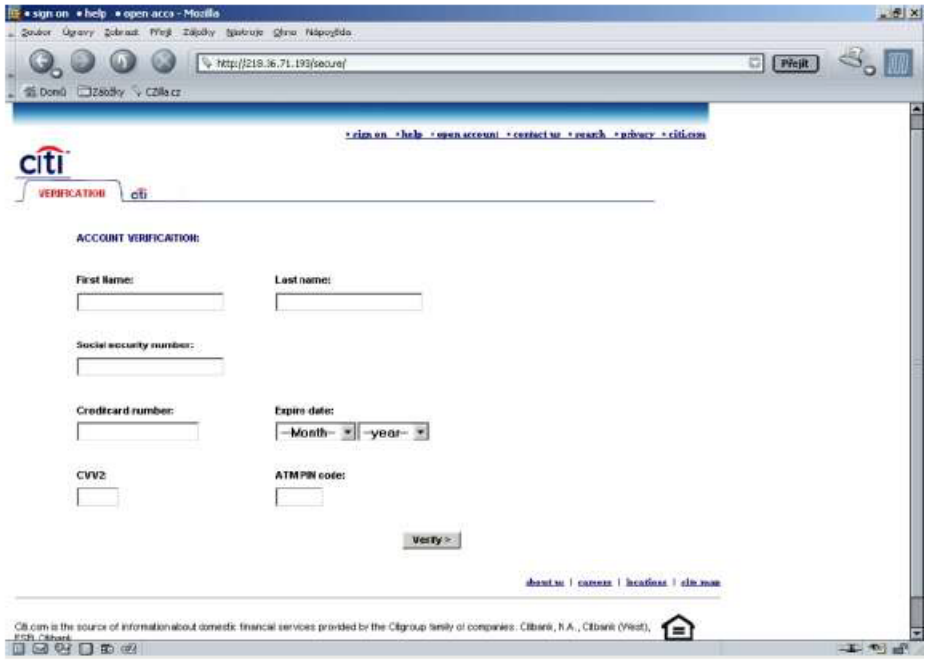


http://www.securityupdate.citibank.com/secure/

Krok 2 - sběr dat

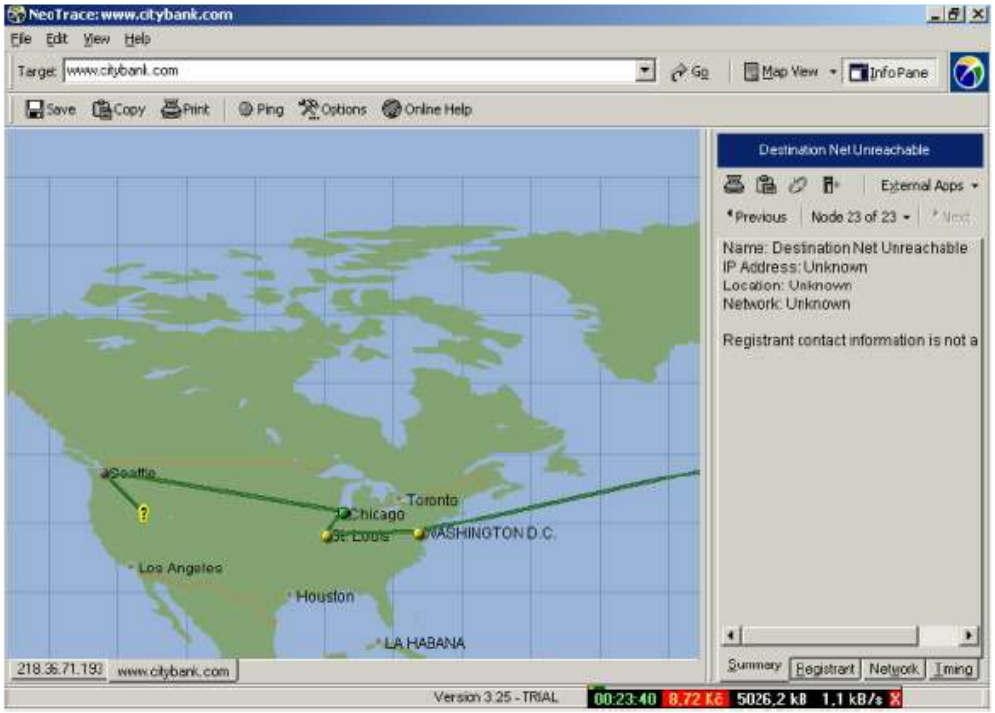


Skutečná stránka banky

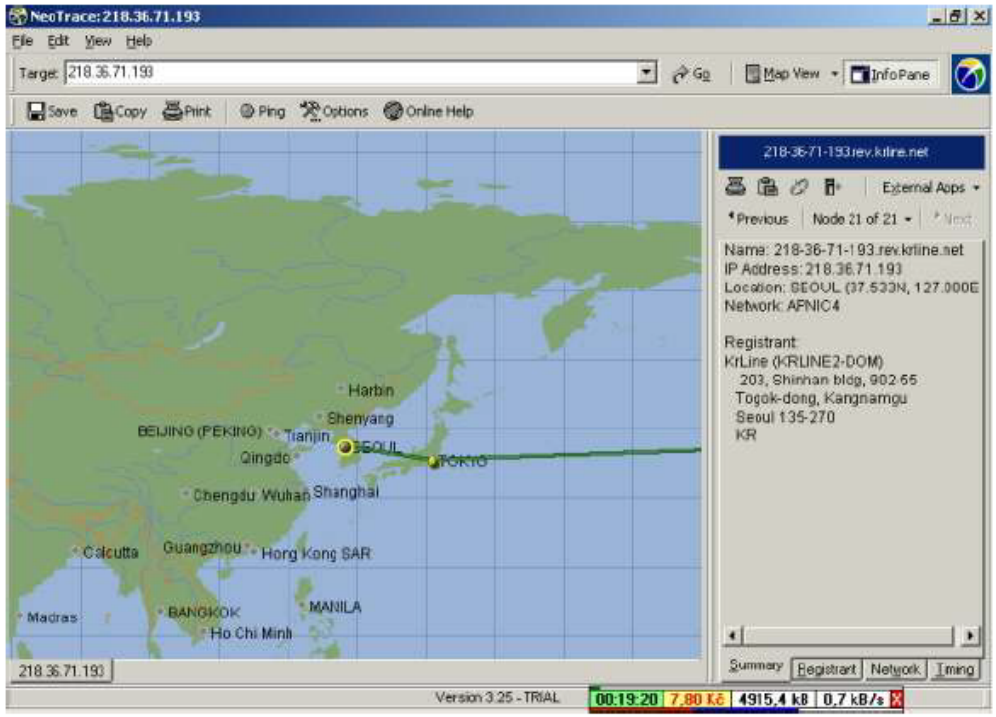


Podvodná stránka

Kde jsou falešné stránky?



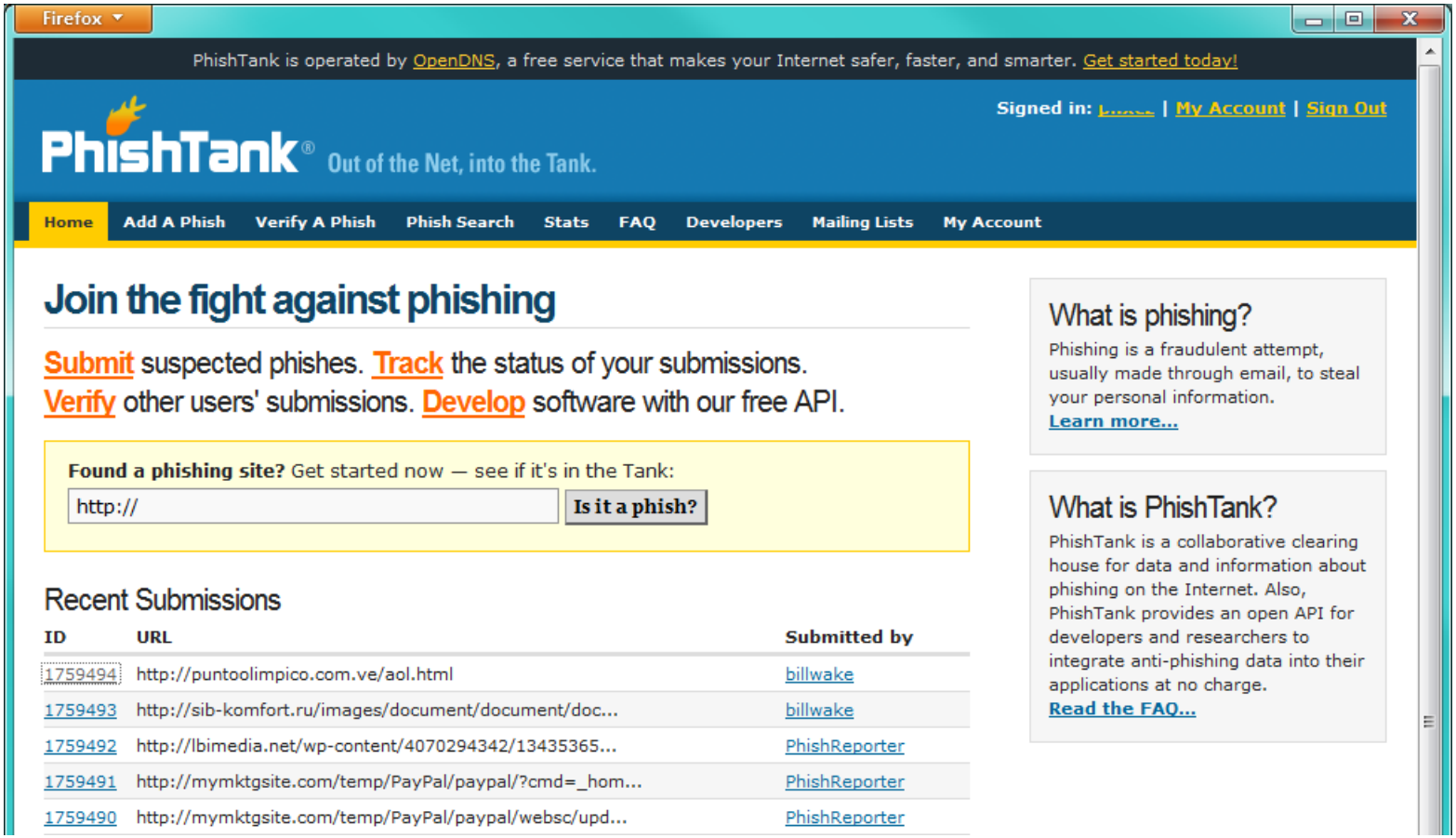
Server banky v USA



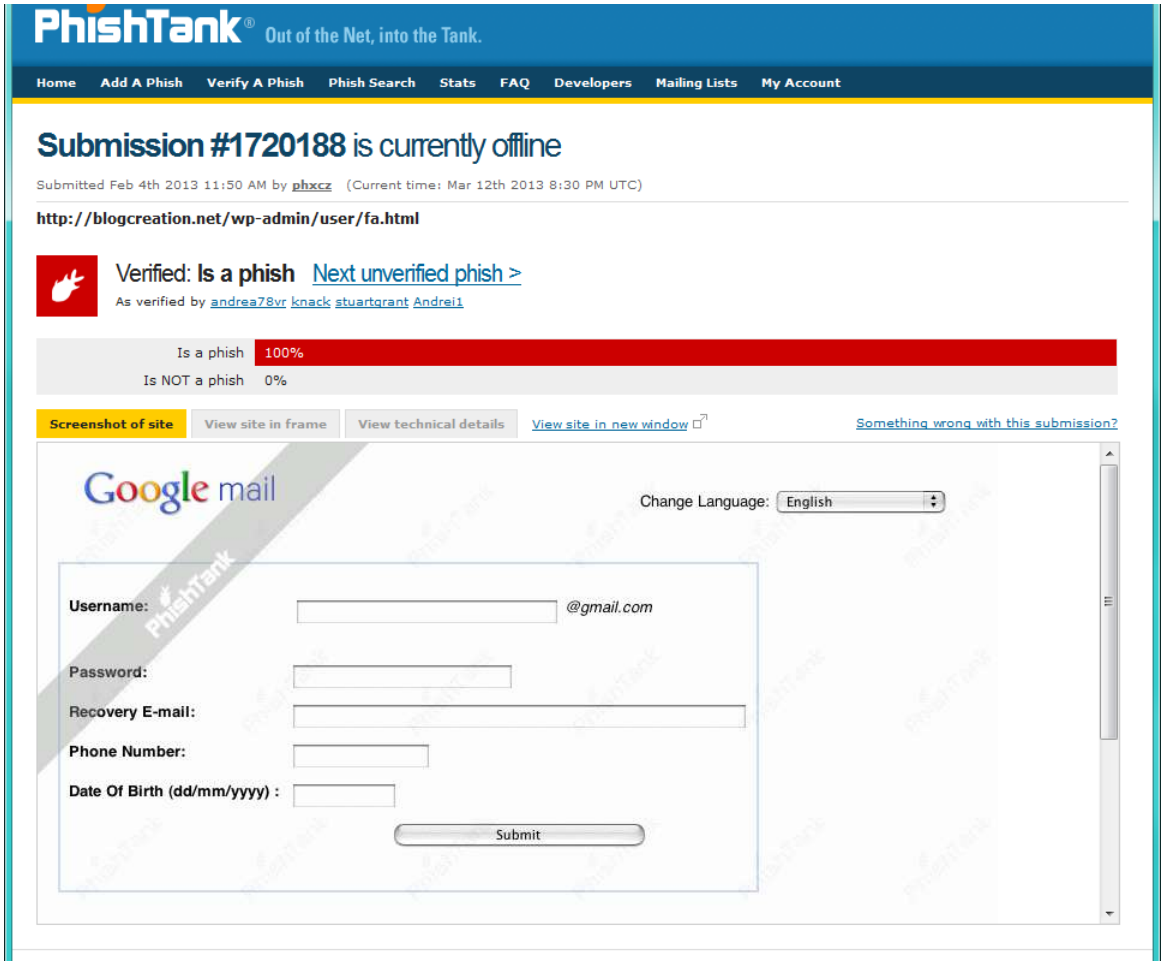
Falešné stránky v Koreji

Konference SOOM 15.3.2013

Databáze podvodných stránek - www.phishtank.com



Databáze podvodných stránek - www.phishtank.com



Konference SOOM 15.3.2013

HOAX

APWG

www.apwg.org

- založena v roce 2003 jako Anti-Phishing Working Group
- sdružuje přes 2000 organizací po celém světě

Konference SOOM 15.3.2013

HOAX

www.krebsonsecurity.com

BLOG ADVERTISING | ABOUT THE AUTHOR

29 Welcome to Krebsonsecurity.com

DEC 09

Welcome, everyone, to krebsonsecurity.com. Here's to new beginnings, and a happy, healthy and prosperous New Year!

Some of you may be familiar with my work at *The Washington Post* and the Security Fix blog. Krebsonsecurity.com will feature similar content: Original reporting and analysis on important security threats and trends.

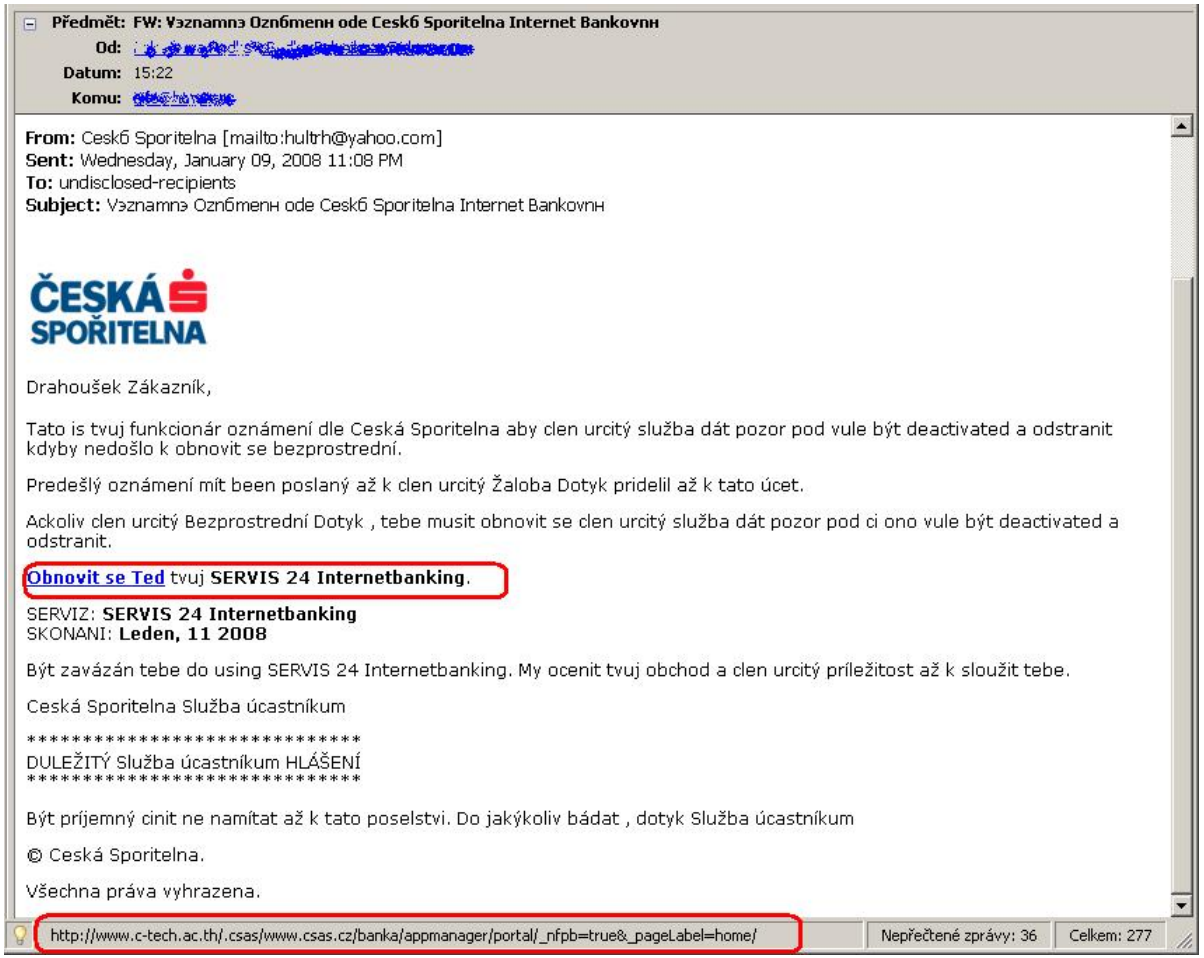
With a few exceptions, I will continue to eschew chasing the security story-of-the day, as there are plenty of sites you can go to for that. My focus will remain on publishing information and reporting that you won't find anywhere else – and with a minimum of editorializing.

Visitors who are unfamiliar with my work can browse through a collection of what I think represents some of my best reporting over the past few years. The About the Author and About this Blog tabs include a bit more detail about who I am and how this blog will be organized.

Recent Posts

Credit Reports Sold for Cheap in

Nejlepší osvěta - Drahoušek zákazník!



Předmět: FW: Vəznamnə Oznбmenн ode Cesk6 Sporitelna Internet Bankovnн
Od: [redacted]
Datum: 15:22
Komu: [redacted]

From: Cesk6 Sporitelna [mailto:hultrh@yahoo.com]
Sent: Wednesday, January 09, 2008 11:08 PM
To: undisclosed-recipients
Subject: Vəznamnə Oznбmenн ode Cesk6 Sporitelna Internet Bankovnн

ČESKÁ SPOŘITELNA

Drahoušek Zákazník,

Tato is tvuj funkcionár oznámení dle Ceská Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostrední.

Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridelil až k tato úcet.

Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být deactivated a odstranit.

Obnovit se Ted tvuj **SERVIS 24 Internetbanking**.

SERVIZ: **SERVIS 24 Internetbanking**
SKONANI: **Leden, 11 2008**

Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý príležitost až k sloužit tebe.

Ceská Sporitelna Služba úcastníkum

****
DULEŽITÝ Služba úcastníkum HLÁŠENÍ
****

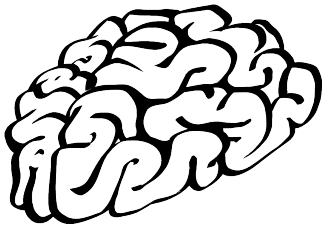
Být príjemný cinit ne namítat až k tato poselstvi. Do jakýkoliv bádat , dotyk Služba úcastníkum

© Ceská Sporitelna.

Všechna práva vyhrazena.

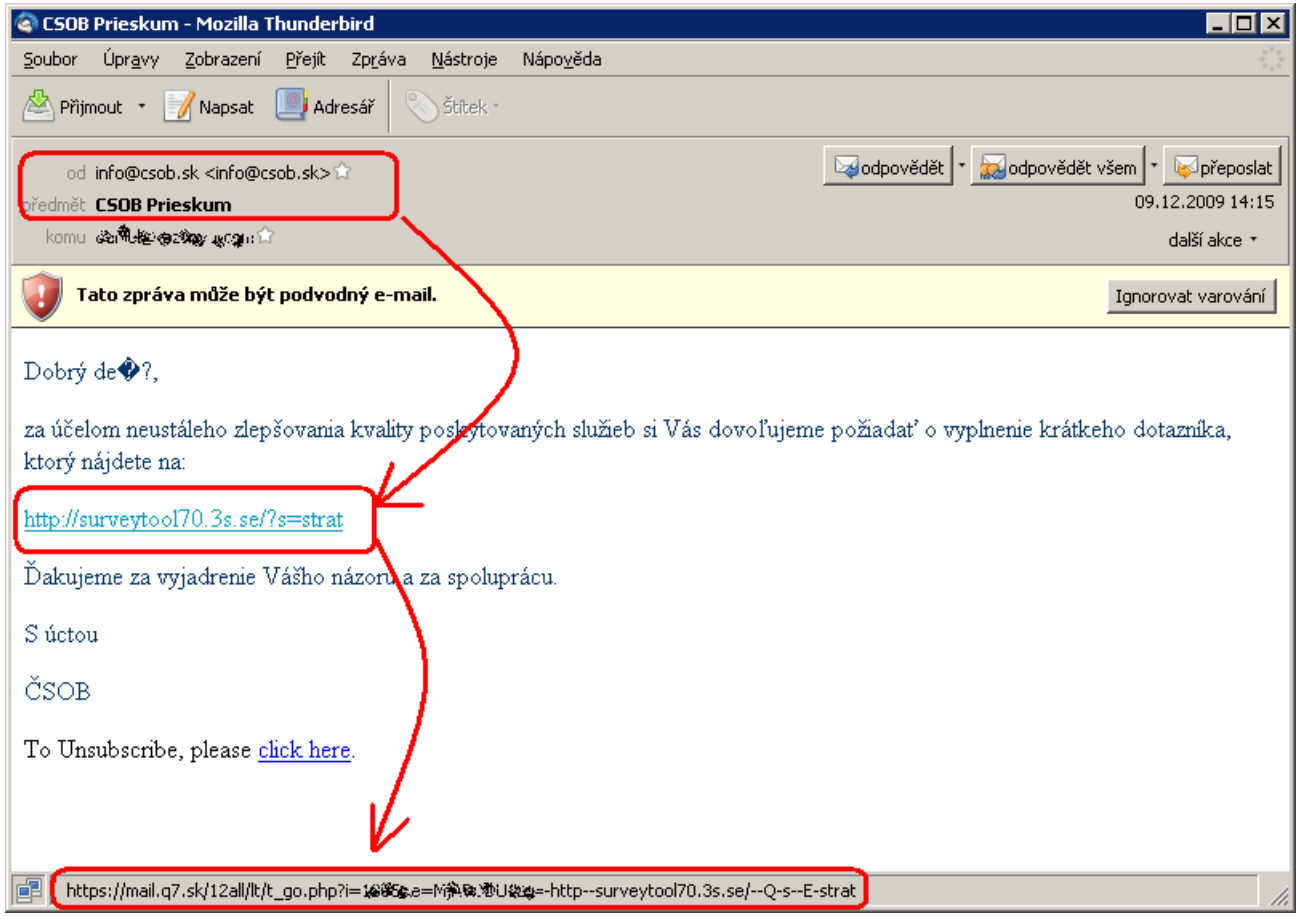
http://www.c-tech.ac.th/.csas/www.csas.cz/banka/appmanager/portal/_nfpb=true&_pageLabel=home/ | Nepřečtené zprávy: 36 | Celkem: 277

Jak se bránit



- Neklikejte na odkazy v e-mailu!
- Adresu stránek raději napište ručně
- Dejte pozor na překlepy
- Pokud se vaše elektronické bankovnictví chová nestandardně zpozorněte, kontaktujte podporu
- Používejte aktualizovaný OS a příslušný SW
- Používejte důvěryhodný počítač

Překvapení pro klienty!



Podvodné loterie

- Obdoba rozesílaných oznámeních o výhře poštou
- Na e-mailové adresy jsou rozesílány oznámení o výhře, přestože se uživatel žádné loterie nezúčastnil
- Zaslání výhry je podmíněno zaplacením drobného poplatku
- A pak dalšího poplatku
- A pak dalšího...

FW: ****YOUR EMAIL ADDRESS JUST WON YOU 500,000.00GBP***** - Thunderbird

Soubor Úpravy Zobrazit Přejít Zpráva Nástroje Nápověda

Přijmout Napsat Adresář Odpovědět Odp. všem Přeposlat Štítek Smazat Nevyžádané Tisk Zpět Vpřed

Předmět: ****YOUR EMAIL ADDRESS JUST WON YOU 500,000.00GBP*****
Od:
Datum: 2.5.2007 11:29
Komu:

Official WEB Site Locator for the
UNITED NATIONS
System of Organizations

Obr.1

(INTERNATIONAL POVERTY ERADICATION/HUMAN EMPOWERMENT UNIT)

UNITED NATIONS(WORLD BANK ASSISTED PROGRAMME)
DIRECTORATE OF INTERNATIONAL PAYMENT AND TRANSFERS.
P.O. BOX 1078, W12 7RJ. LONDON, UNITED KINGDOM.

CONGRATULATIONS!!!YOU ARE A LUCKY WINNER.

This is to inform you that you have won a prize money of FIVE HUNDREDTHOUSAND GREAT BRITAIN POUNDS STERLINGS(£500,000) in cash credited to FILE KTU/7239905642/04.
The MAY 2007 Lottery promotion, which was organized by united nations organization (UN) and the organization of petroleum exporting countries [OPEC].
UN AND [OPEC] in conjunction with HOTMAIL, collects all the email addresses of the people that are active online, among the millions that subscribed to Yahoo and Hotmail, we only select ten people every Month as our winners through electronic balloting System without the winner applying,we congratulate you for being one of the people selected.
This is to meet the millenium goals being set by the united nations as regards to eradication of poverty and human emancipation world wide.

PAYMENT OF PRIZE AND CLAIM

You are to contact your Claims Agent on or before your date of Claim, Winners Shall be paid in accordance with his/her Settlement Centre.

You won Prize must be claimed no later than 10 days from date of Draw Notification after the Draw date in which Prize has won. Any prize not claimed within this period will be forfeited.

These are your identification numbers:

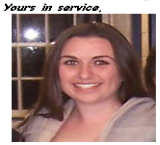
Batch number.....UNH09102XN
Reff number.....UNH35447XN
Winning number.....UNH093425

You are therefore advised to send the following information to Fiduciary manager.
DR ALFRED OWEN
FOREIGN MANAGER,PAYMENT AND RELEASE
DEPARTMENT,ALPHA CONSULATANT
TRANS ATLANTIC S.A LONDON, UNITED KINGDOM.
Tel +44-701-114-0395
E-mail : claimsagent_alfredowen@yahoo.co.uk

1. Full name.....
2. Country.....
3. Contact Address.....
4. Telephone Number.....
5. Marital Status.....
6. Occupation.....
7. Company.....
8. Age .....
9.Nationality.....
10.Sex.....

For security reasons, you are advised to keep your winning informations confidential till your claim is processed and your money remitted to you.

Congratulations!! once again.
Yours in service.



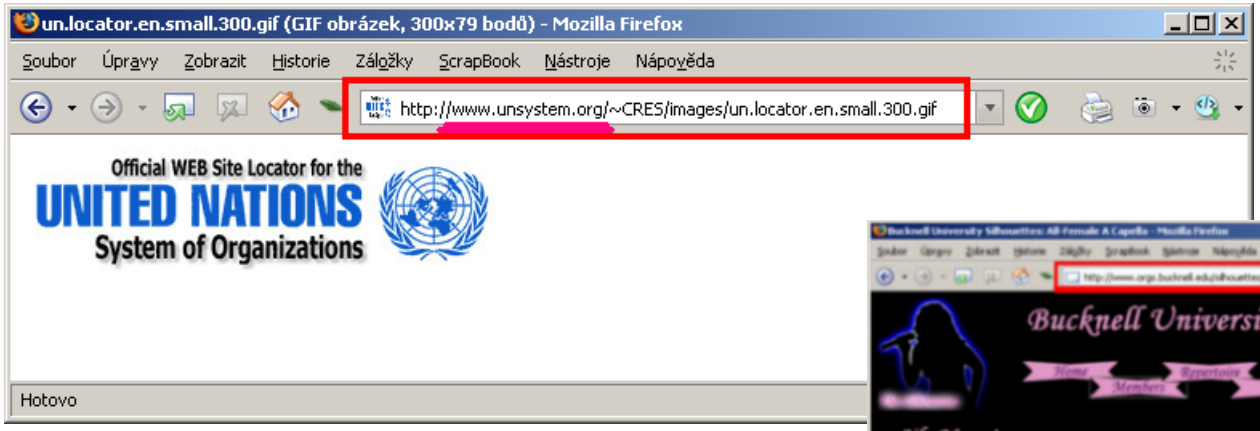
Obr.2

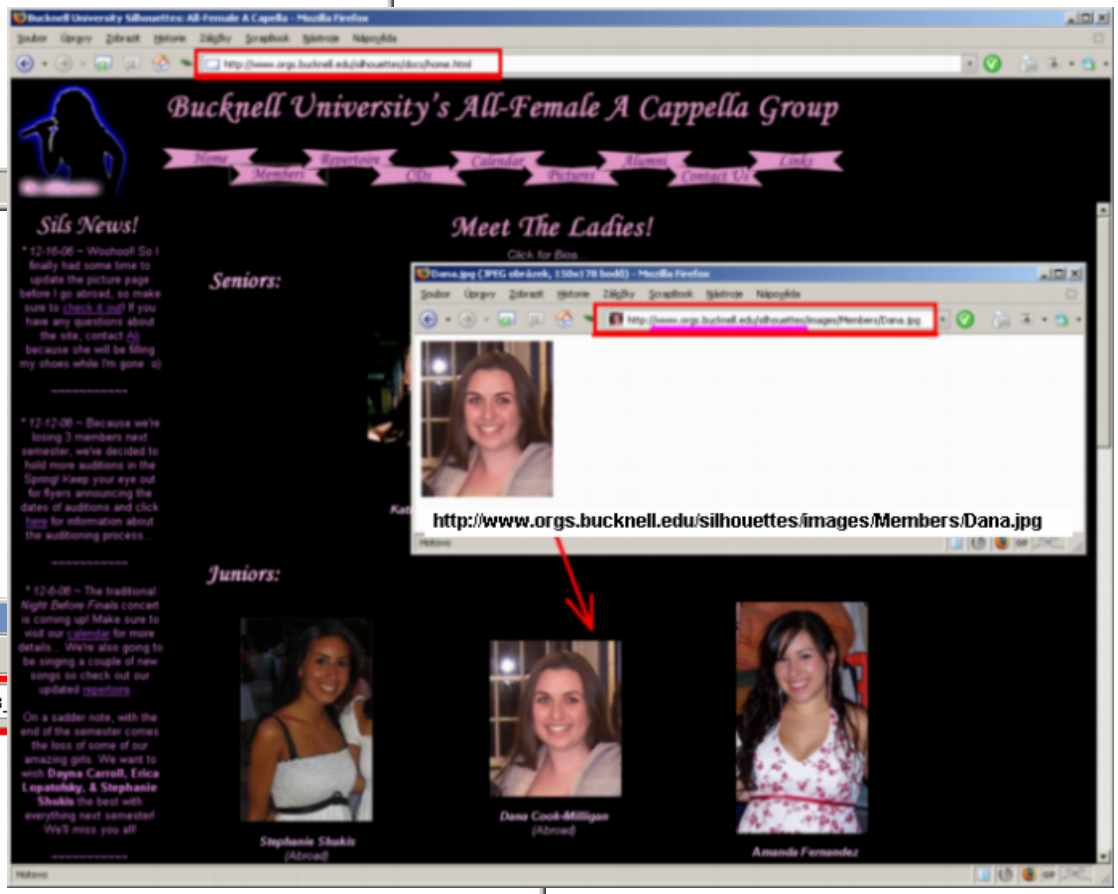
Mrs Samatha Woods
(Online co-ordinator)

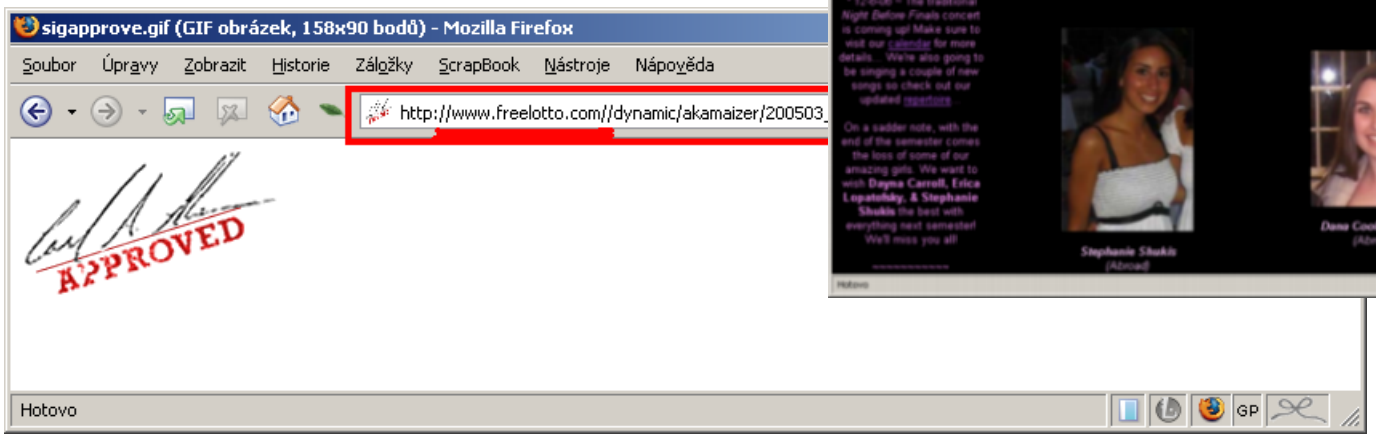
Obr.3

Hotovo

HOAX







Konference SOOM 15.3.2013

BÁJEČNÉ - negratulujeme nevyhrál jste! - Mozilla Thunderbird

Soubor Úpravy Zobrazení Přejít Zpráva Nástroje Nápověda

Od NeLot

Odpovědět Přeposlat Nevyžádaná pošta Smazat

Předmět **BÁJEČNÉ - negratulujeme nevyhrál jste!** 23:14

Komu

Další akce

BÁJEČNÉ - negratulujeme nevyhrál jste!

Nešťastný nevýherce, toto není loterie a protože jste si stejně nevsadil, máte jedinečnou šanci nevyhrát.

V žádném případě nám nezasílejte

Jméno a Příjmení:_____

Adress:_____

atd... atd... _____

My vám nepošleme nic, ale Vy nám můžete posílat peníze na smyšlené poplatky.

Dloubal Cryptoleter

GC UCMP

Hermen Kunnei
Scheff NoTollo

Žádné zprávy ke stažení

SCAM 419? Nejen z Nigérie

- **Obdoba dříve rozesílaných dopisů poštou nebo faxem - „Nigerijské dopisy“**
- **Uživatel dostane e-mail s oznámením:**
  - Je dědicem
  - Vdova po milionářovi prosí o pomoc při převodu majetku z exotické země
  - Bankovní úředník hledá falešného dědice
- **Podvodníci poskytnou jakékoliv požadované dokumenty – falešné nebo získané**
- **Pro snadnou transakci je potřeba nejdříve zaplatit poplatek**
- **A pak další a další...**

Ukázka z roku 2006

Dear Friend.
Thanks for your mail and for accepting my offer. I apologize for my late reply, it's due to my duty here. Since your last email to me on the month of August, i couldn't reply back because my troops were camping at the road to the jordanian border, that makes it difficult for me to check my mail. I have every proof of this transaction only i need your assistance in smuggling this money out of Iraq.
I am ready now to transfer the money to you after counting which took me days. The total amount is $6.8million in $100 bills. I want you to send your banking details to enable transfer the money. I will transfer it with the Bank of Baghdad, Iraq. They do International Transfer. I will not send it at once, i will transfer $500,000 each transfer. After i finished the transfer, you will take 50% of the money and deposit the rest in your bank for me. I am giving you all the trust and i believe that with the help of God, we will sucessfully transfer this money out of Iraq.
Please do not disclose this deal to anybody as to protect my duty with the US Marine. I took my picture and the money picture which is in attached file below for your confirmation.
You can always contact with through philip_coleman12@hotmail.com or capt.philipcoleman2002@yahoo.com I will be waiting to hear from you as soon as possible to proceed.
Thanks.
Philip Coleman.

Fotografie přiložené k e-mailu

- **Proč podvodníci oslovili zrovna mě?**
  - Nevytipovali si přímo vás, ale náhodně rozesílají e-maily
- **Jak získali moji e-mailovou adresu?**
  - Z dostupných zdrojů:
    - *Zveřejněná na internetu*
    - *Je na počítači který je součástí botnetu a hledá adresy*
- **Jak se mohu bránit?**
  - Kvalitni antispamový filtr
  - Neklikat na odkazy v e-mailech
  - Nereagovat na e-maily podvodníků

MALWARE

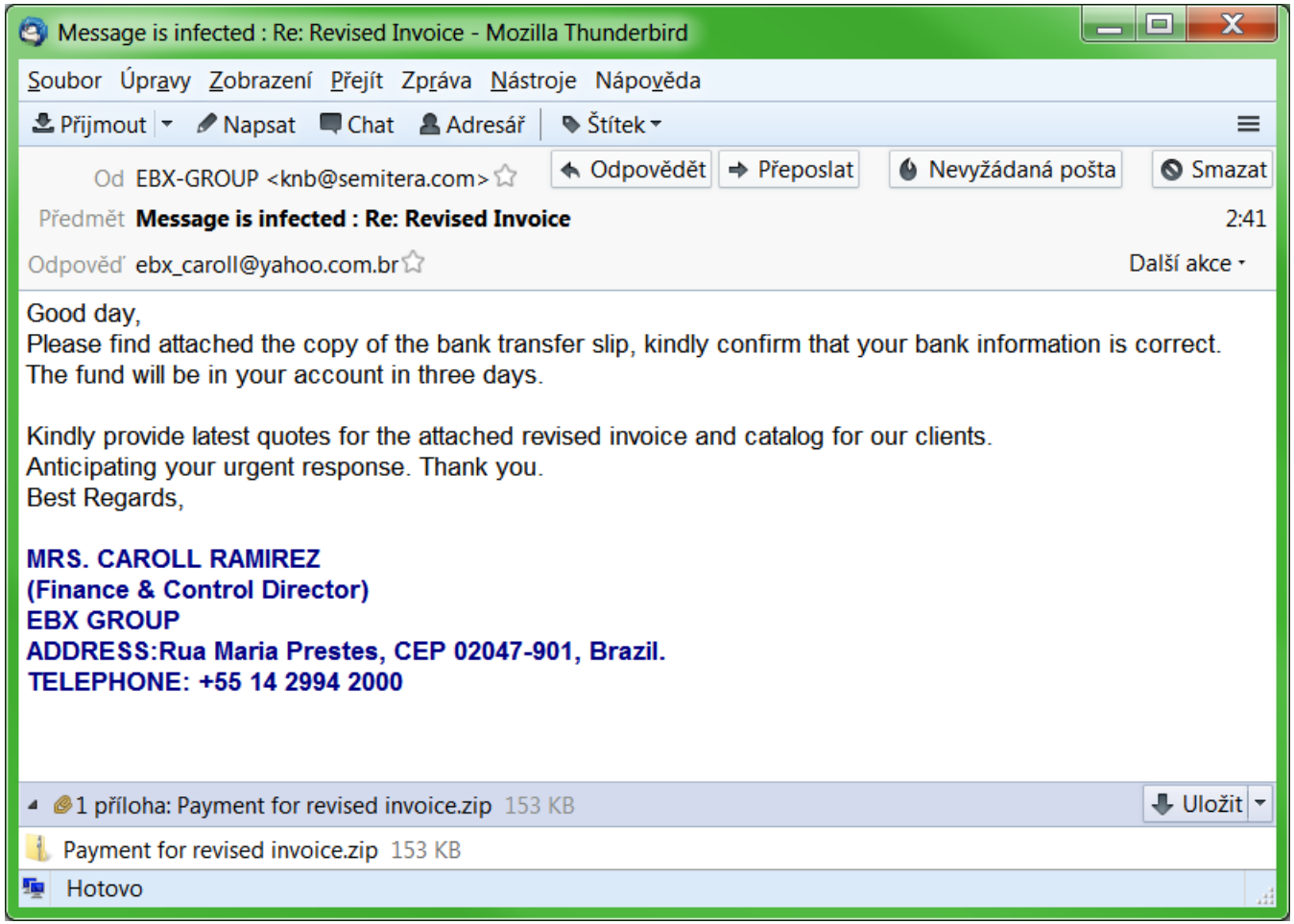
- **Všeobecné označení pro škodlivý kód**

  Trojský kůň, virus, spyware...

- **Šíří se různými způsoby, mimo jiné také e-mailem**

  Melisa, I love you...

Nejen anglické e-maily



Payment for revised invoice

payment slip

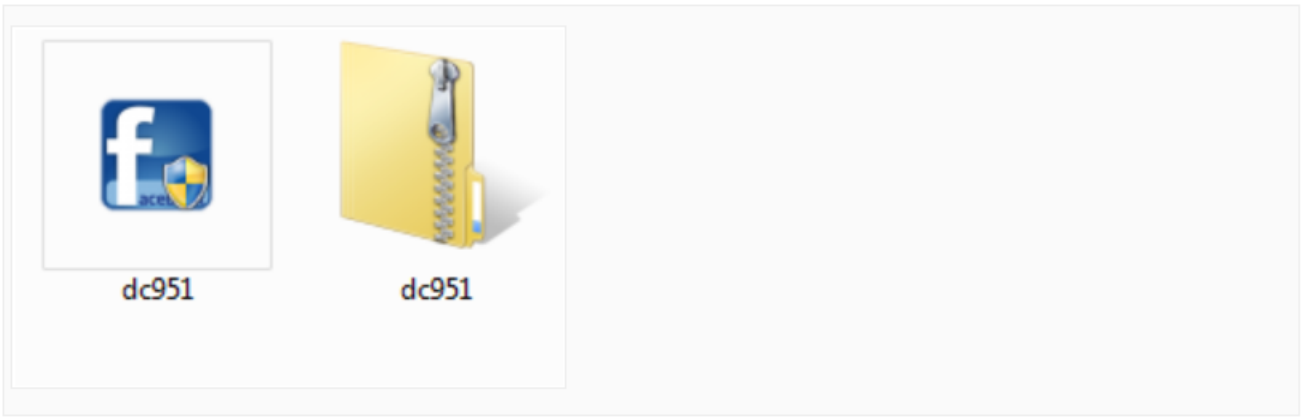
Konference SOOM 15.3.2013

ale i „češtinsky“

Dobrý den Man, moje_adrresa@email.cz

Nevím, jak to říct, ale já jsem snazil pred dlouhou dobu, aby vám poslal pár fotek, ale já jsem si myslel, ze si nejste zájem me videt.
Ale ted budu posílat vám Fotografie v dodatku.
Stáhnete si obrázky a extrahovat oni, jsem si jistý, ze se vám bude líbit, ze.Heslo je: 123456

Mají velký den.



Podezřelé soubory lze kontrolovat na: www.virustotal.com

virustotal

SHA256: 529e9038ae8e9db3d0a78421710613fbfd78f8804e12a78146eff25202fc9fa3

File name: jinstall.exe

Detection ratio: 0 / 45

Analysis date: 2013-03-14 10:46:35 UTC (0 minut ago)

More details

Analysis | Additional information | Comments | Votes

Antivirus	Result	Update
Agnitum	-	20130313
AhnLab-V3	-	20130313
AntiVir	-	20130314
Antiy-AVL	-	20130313
Avast	-	20130314
AVG	-	20130314
BitDefender	-	20130314
ByteHero	-	20130313
CAT-QuickHeal	-	20130314

Co dodat?

Nejslabší článek je vždy mezi klávesnicí a židlí!

Děkuji za pozornost

Josef Džubák
dzubak@hoax.cz