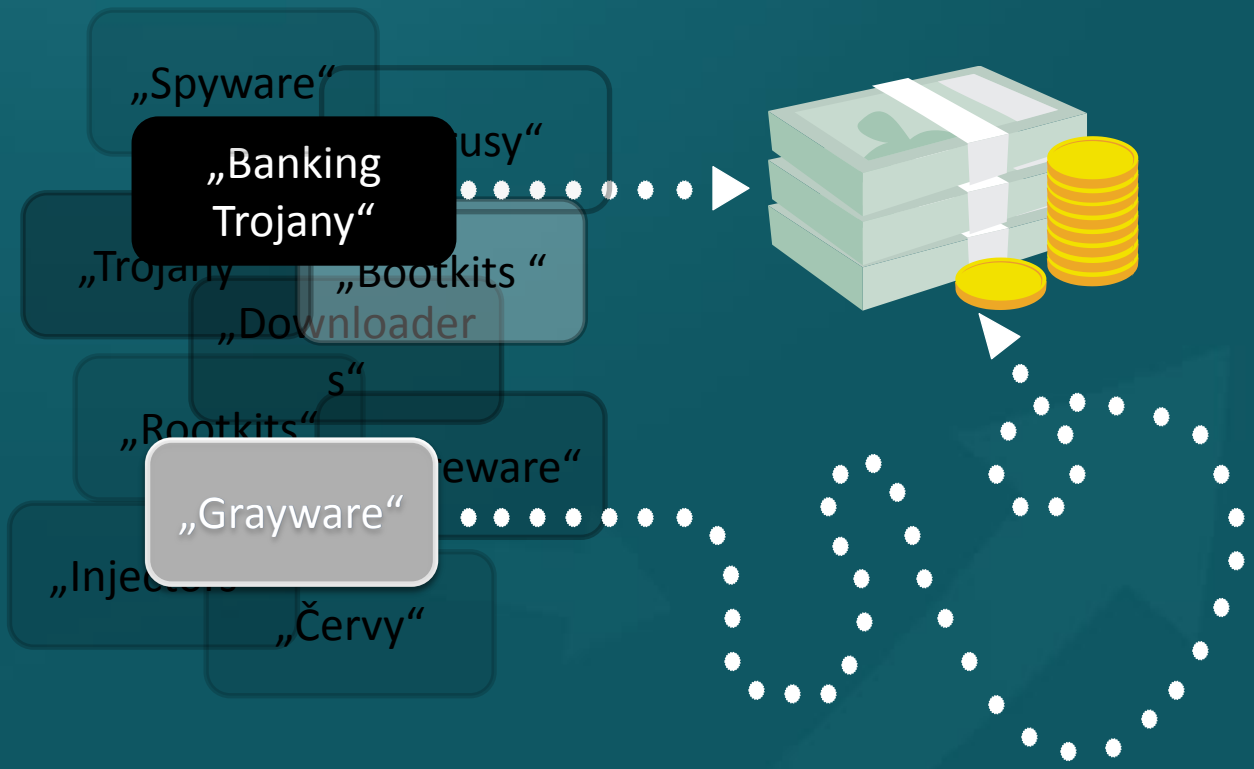
ESET SECURITY DAYS 2013

Robert Lipovský, *Malware Researcher*
Peter Stančík, *Security Evangelist*

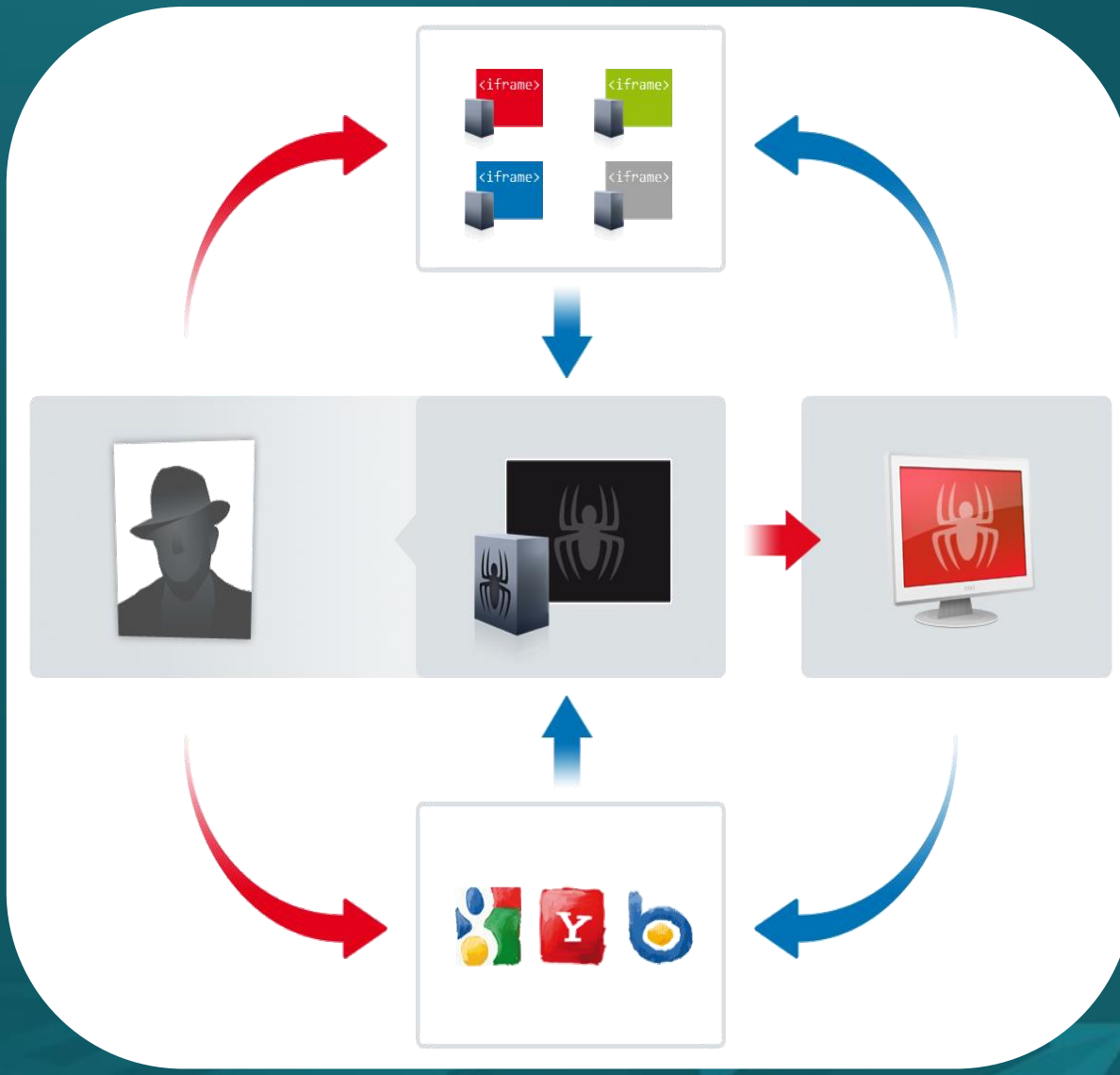
ÚTOKY NA BANKOVÉ KONTÁ A PRÍSTUPOVÉ ÚDAJE K FINANČNÝM ZDROJOM

Malware včera a dnes

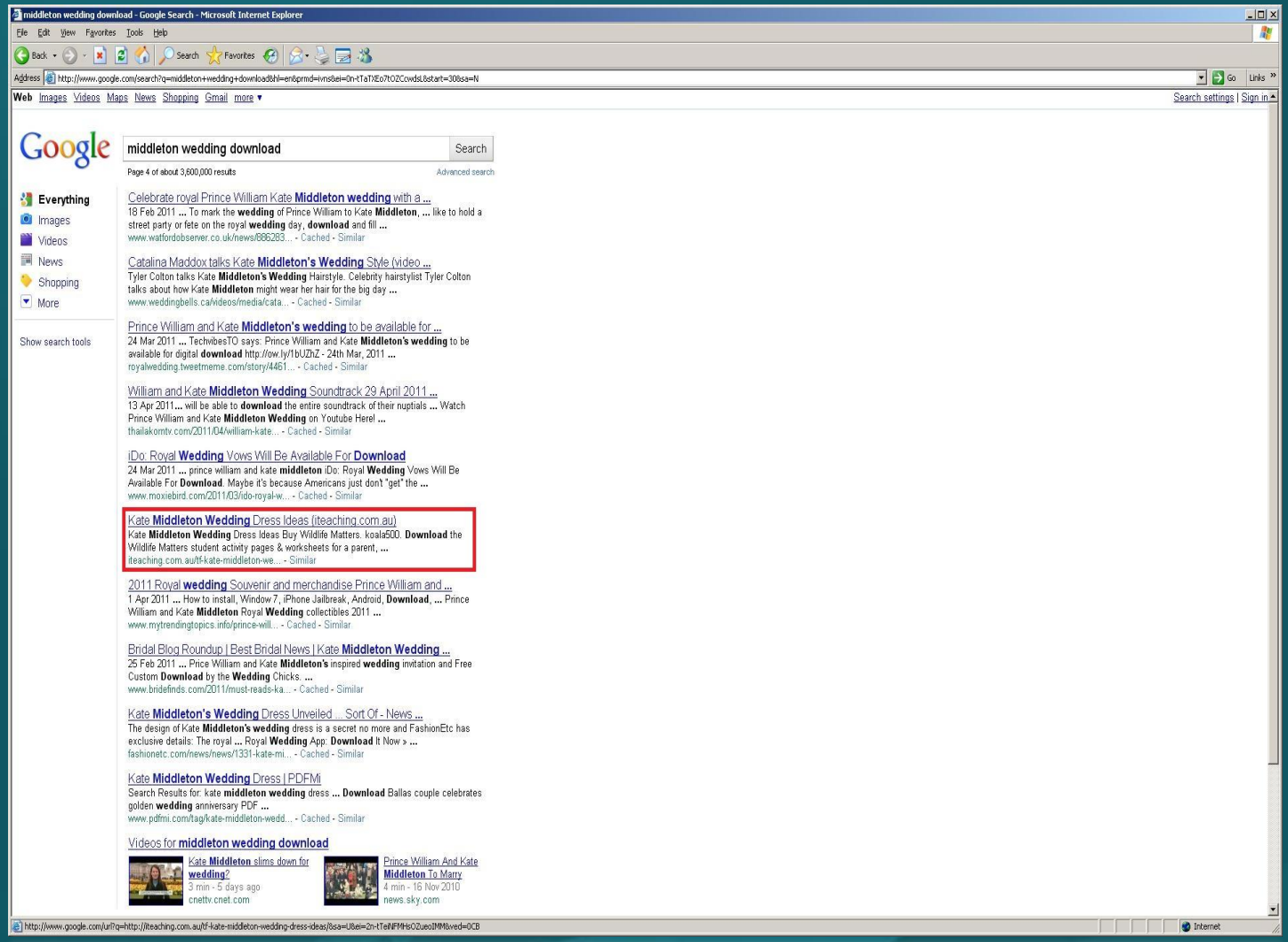
Malware včera a dnes



Drive-by download



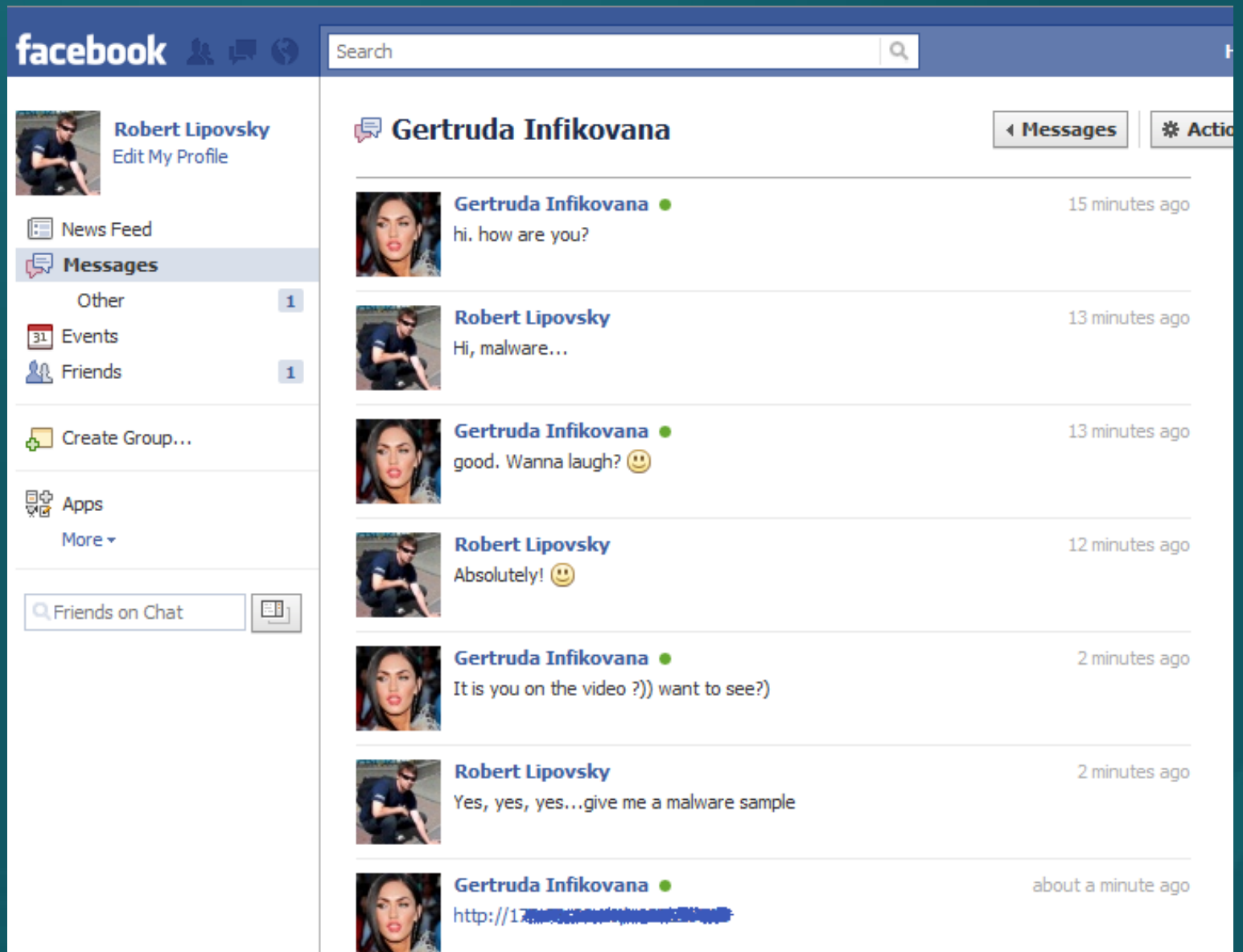
Blackhat SEO



Blackhat SEO

Blackhat SEO

Malware na sociálnych sieťach



You Tube
Search
Browse
Upload
Robert Lipovsky is in the leading role. Shoking performance!
Yourfavoritemartian
11 videos
Subscribe
Suggestions
You need to upgrade your Adobe Flash Player to watch this video.
Download it from Adobe.
Opening Flash-Player.exe
You have chosen to open
Flash-Player.exe
which is a: Binary File
from: http://178.78.33.10
Would you like to save this file?
Save File
Cancel
I like this
Add to
Share
23473
Uploaded by Yourfavoritemartian on Jun 15, 2011
568 likes, 6 dislikes
You have to see it, few can do that :))) Lipovsky is on a streak!!!
see all
He must have been shamed to do that :)))
[redacted] 5 minutes ago
I had to update Flash Player, but it was worth it :)) this video is the very best!
[redacted] 6 minutes ago
one word for it – TERRIBLE!!
[redacted] 7 minutes ago
He's the new TV star! Put him on the tonight show! :)))))

“Lockscreeny”, Ransomware

POLÍCIA DE SEGURANÇA PÚBLICA PORTUGUESA

DEPARTAMENTO PARA COMBATER O CIBERCRIME

GOVERNO D
PORTUGA

Atenção!!!

Foi detectado um caso de atividade ilegal. O sistema operacional foi bloqueado por violação das leis da República Português! Foi detectada a violação seguinte:

Do seu endereço IP com o número de "**89.153.252.45**" foi feita para acessar sites que contenham pornografia, pornografia infantil, bestialidade, também como a violência sobre as crianças. N computador também foram encontrados arquivos de vídeo contendo pornografia, violência e os elementos de pornografia infantil. Uma vez que também spamming e-mail foi feito com subtext de terrorismo.

O bloqueio do computador é feito para eliminar a possibilidade de ações ilegais por parte deles.

Seus detalhes:	**IP:89.153.252.45** Localização: Portugal, Lisbon ISP: TVCABO Autonomous System

Para remover o bloco em seu computador, você deve pagar uma multa de 100 €.

Você tem duas formas de pagamento:

1) Efetuar o pagamento pelo Ukash:

Para isso, digite o código que você recebeu na linha de pagamento e clique em OK (se você tiver vários códigos, inseri-los um após o outro, em seguida, pressione OK).

Se o sistema falhar, você deve enviar e-mail de código (deposito@cyber-psp.pt).

2) Efetuar o pagamento via Paysafecard:

Para isso, digite o código que você recebeu (se necessário juntamente com a senha) na linha de pagamento, e clique em OK (se você tiver vários códigos, inseri-los um após o outro, e então clique em OK).

Se o sistema falhar, você deve enviar e-mail o código (deposito@cyber-psp.pt).

Ukash Onde posso comprar Ukash?

Pode adquirir Ukash a partir de centenas de milhar de localizações globais, online, através de carteiras, de quiosques e do Multibanco.

Payshop - Pode adquirir vouchers Ukash em qualquer um dos mais de 3.600 agentes payshop em Portugal, como **papelarias**, **tabacarias**, **quiosques e supermercados**. Basta indicar ao Agente payshop o montante que pretende. Após o pagamento, o Agente payshop entregar-lhe-á um talão com o código.

OK

paysafecard Onde posso comprar Paysafecard?

pay cash. pay safe.

Podes obter paysafecards nas cerca de 4.000 lojas da rede **PayShop**, nas 1.000 estações-dos-correios dos **CTT** e em toda a rede de caixas automáticas **Multibanco**.

OK

Firefox

http://195.189.227.109/

195.189.227.109

Google

Attention!!!

This operating system is locked due to the violation of the laws of the United Kingdom! Following violations were detected:

Your IP address is "**84.55.117.251**". This IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video f
Pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

Your details:	**IP:84.55.117.251** Location: Sweden, Malmö ISP: Ownit Broadband AB

To unlock the computer you are obliged to pay a fine of £ 100.

You could pay the forfeit in two ways:

1) Paying through Ukash:

To do this, you should enter the 19 digits code in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address surcharge@cyber-metropolitan-police.co.uk.

2) Paying through Paysafecard:

To do this, you should enter the 16 digits resulting code (if necessary

Ukash Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your cour

Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.

PayPoint - Get Ukash wherever you see the PayPoint sign.

Payzone - Ukash available from Payzone terminals around the UK.

Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using you internet bank.

OK

Firefox

http://195.189.227.109/

195.189.227.109

Google

BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNIT
ACHTUNG!!!

Achtung!!!

Das Betriebssystem wurde im Zusammenhang mit Verstoßen gegen die Gesetze der Bundesrepublik Deutschland gesperrt!

Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet "**46.165.196.182**" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen
Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

IP:46.165.196.182
Location: Germany
ISP: LeaseWeb B.V.

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Solte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamt.eu versenden.

2) Die Zahlung per Paysafecard begleichen:

Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Solte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamt.eu versenden.

Ukash Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich beifolgenden Tankstellen: Agip, Avia, Esso, OMV, Ql und Westfalen.

AVIA Agip Esso OMV Q1 Westfalen

Epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call- Shops, in denen Sie dieses Logo sehen.

OK

paysafecard
pay cash. pay safe.

Du bekommst deine paysafecard z.B. bei Rossmann Drogeriemarkten, Netto Marken-Discount, vielen Tankstellen sowie Lotto Annahmestellen und Handykartenautomaten.

Shell ARAL ROSSMANN Westfalen eni Netto Marken-Discount TOTAL

OK

IPA

POLICAJNY ZBOR SLOVENSKEJ REPUBLIKY

Pozor!

IP: {ip}
Lokalita: {location}

Pozor! Váš počítač je zablokovaný kvôli aspoň jedného z dôvodov uvedených nižšie.

Boli ste porušenie «autorského práva a súvisiacich práv» (Video, Hudba, Software) a nedovolené použitie alebo distribúciu obsah chránený autorskými právami, a tým porušil článok 128 trestného zákonníka Slovenskej Republiky.

Článok 128 trestného zákonníka stanovuje pokuty 2-500 minimálnej mzdy alebo pozbavenie slobody na 2 až 8 rokov.

Boli ste chytení pri prezeraní alebo distribúciu zakázané produkcie pornografickým obsahom (Detská pornografia / Zoofília a atď). A tým porušujete článok 202 trestného zákonníka Slovenskej Republiky.

Článok 202 trestného zákonníka stanovuje odňatia slobody na 4 až 12 rokov.

Protiprávne prístup k počítačovým údajom bol zahájený z počítača, alebo ste boli...

paysafecard Ukash

Code

Sum 2000

1 2 3 4 5 6 7 8 9 0

Pay PaySafeCard | Pay Ukash

Článok 208 trestného zákonníka stanovuje pokutu až do výšky **SKK 100.000** a / alebo odňatia slobody po dobu **4** až **9** rokov.

Protiprávne prístup bol zahájený z vášho počítača bez vášho vedomia alebo súhlasu, môže váš počítač infikovaný škodlivým softvérom, tak ste porušil zákon o zanedbanej Použitie osobného počítača.

Článok 210 trestného zákonníka stanovuje pokuty **SKK 2.000** libier na **SKK 8.000**.

Spam distribúcia alebo iné protiprávne inzercia bola uskutočnená z vášho počítača ako usilujúce o zisk činnosti alebo bez vášho vedomia, môže váš počítač infikovaný škodlivým softvérom.

Článok 212 trestného zákonníka stanovuje pokutu až do výšky **SKK 250.000** a zbavenie osobnej slobody až na **6** rokov. V prípade, že je táto činnosť bola uskutočnená bez vášho vedomia, ste spadajú do vyššie uvedeného článku 210 trestného zákonníka Slovenskej Republiky.

Vaša osobnosť a adresa sú v súčasnej dobe určené kriminálny prípad sa začne proti vám v rámci jedného alebo viacerých článkov uvedených vyššie, počas nasledujúcich **72** hodín.

Podľa novely trestného zákona Slovenskej Republiky 28. augusta 2012, tento zákon porušenie (ak sa neopakuje - prvýkrát) možno považovať za podmienenej prípad, že by ste zaplatiť pokutu štátu.

Pokuty môžu byť vyplatené až až počas **72** hodín po porušení. Akonáhle **72** hodín uplynutí, možnosť zaplatiť pokutu vyprší, a trestné konanie je začaté proti Vas automaticky počas najbližších **72** hodín!

Výška pokuty je SKK 2000 alebo €100. Môžete zaplatiť pokutu pomocou PaySafeCard alebo Ukash.

Kde môžem kúpiť PaySafeCard?

PaySafeCard dostaneš na viac ako 101 čerpací staniciach Agipu a OMV, vo vybraných pobočk stávkovej kancelárie Tipsport a vo všetkých predajných miestach GG Tabaku.

TABAK Agip Tipspor OMV AXASOFT

Kde môžem kúpiť Ukash?

Dalo by sa kúpiť trestný zákonník na mnohý miestach, napríklad: obchody, stánky, samostatné terminály, on-line alebo prostredníctvom elektronickej peňaženky (electronic cash).

Čerpacie stanice - Ukash je teraz k dispozícii od čerpacích staníc.

epay

epay - Získajte Ukash z tisícov supermarketov a call obchody, kde epay znamenie.

Zostávajúci čas: 47:56:09

paysafecard

VAROVANIE! Váš osobný počítač je uzamknutý z bezpečnostných dôvodov by z nasledujúcich dôvodov:

Ste obvinený z prezerania/skladovania a/alebo distribúcia pornografických materiálov zakázané obsahu (detská pornografia/zvieratkosti atď) Že ste porušil Všeobecnú deklaráciu o boji proti šíreniu detskej pornografie a obvinený z trestného činu podľa článku 161 trestného zákonníka Slovenské republiky.

Článok 161 trestného zákonníka Slovenské republiky ustanovuje ako trest odňatia slobody v trvaní 5-11 rokou.

Tiež ste osoba podozrivá z porušenia "zákon o autorskom práve a právach súvisiacich s právom" (sťahovanie pirátskej hudby, videa neletsenzionnogo softvér) a použitia a/alebo šírenie obsahu chráneného autorským právom. Tým ste osoba podozrivá z porušenia článku 148 trestného zákonníka Slovenské republiky.

Článok 148 trestného zákonníka Slovenské republiky, musí byť trest pokuta 150 až 550 základných jednotiek alebo odňatím slobody na dobu 3-7 rokov.

S počítačom došlo k neoprávnenému prístupu k obmedzenému prístupu verejnosti k informáciám a informáciám celoštátneho významu v Internete.

Neautorizovaný prístup si môžete dojednať zámerne z sebeckých motívov alebo neoprávneným prístupom môže dôjsť bez vášho vedomia alebo súhlasu, ako váš osobný počítač môže byť napadnutý škodlivým softvérom. Preto, ste podozrenie, že skúmať, neúmyselné porušenie článku 215 trestného zákonníka Slovenské republiky (ďalej len "zákon neopatrní a nedbalé používanie

PIN kód

100

1 2 3 4 5 6 7 8 9 0

Odoslať

Kde môžem získať peňažné poukážku PaySafeCard?

Prehľad predajcov: PaySafeCard dostaneš v mnohých supermarketoch, trafikách. PaySafeCard dostaneš na viac ako 101 čerpacích staniciach Agipu a OMV, vo vybraných pobočkách stávkovej kancelárie Tipsport, všetkých predajných miestach GG Tabaku a vo CBA.

OMV Agip Tipsport GP TABAK

CYBER CRIME UNIT

INTERPOL

INTERPOL

INTERPOL

INTERPOL

FileCoder


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
16. 9. 2013
7:53
Time left
5903 : 04 : 24
Next >>

FileCoder

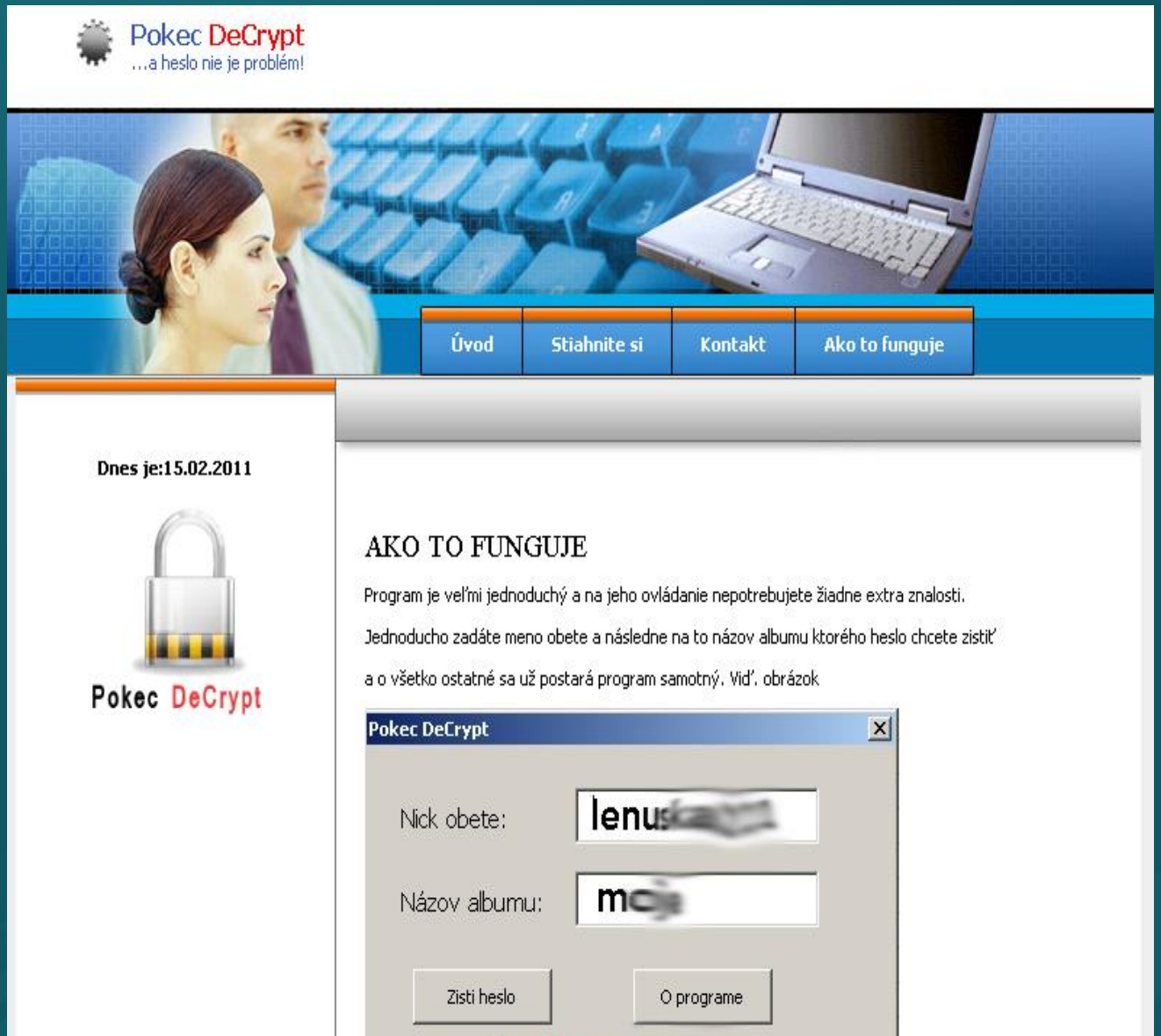

CryptoLocker
Payment for private key
Choose a convenient payment method:
Ukash
Ukash
use your cash online
Ukash is electronic cash and e-commerce brand. Based on a prepaid system, Ukash allows users to purchase and then spend money online.
Money can be purchased from one of the reported 420,000 participating retail locations worldwide, or by using the company's website. This electronic money can then be used to pay online, or loaded on to a prepaid card or eWallet.
You can combine multiple values of your Ukash into a single amount and have your new Ukash Code and value emailed to you if you want. You will need to register at Ukash.com, login and then go to the Manage Ukash area to use the Combine tool.
Home Page
Get Ukash
Enter the code of the card, select card currency, and press «Pay»:
300 USD
Private key will be destroyed on
16. 9. 2013
7:53
Time left
5903 : 02 : 42
<< Back
PAY

FileCoder


CryptoLocker
Payment for private key
Choose a convenient payment method:
Bitcoin (most cheap option)
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.
You have to send below specified amount to Bitcoin address 1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh and specify the transaction ID, which will be verified and confirmed.
Home Page
Getting started with Bitcoin
Private key will be destroyed on
16. 9. 2013
7:53
Time left
5903 : 02 : 03
Enter the transaction ID and press «Pay»:
2 BTC
<< Back
PAY

Pokec Sniffer

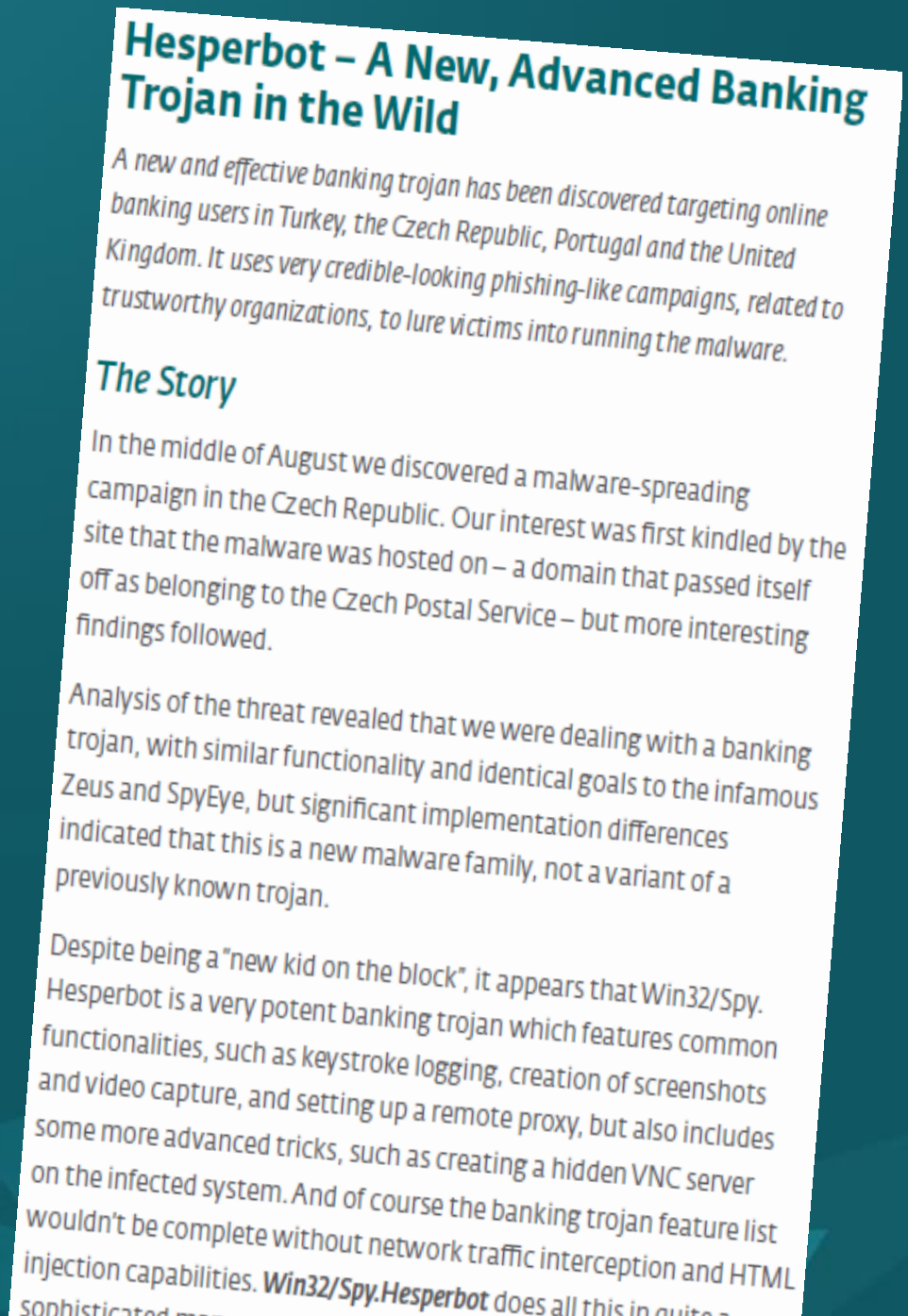
Pokec Sniffer



Banking trojany

DEMO

Hesperbot



Hesperbot – A New, Advanced Banking Trojan in the Wild

A new and effective banking trojan has been discovered targeting online banking users in Turkey, the Czech Republic, Portugal and the United Kingdom. It uses very credible-looking phishing-like campaigns, related to trustworthy organizations, to lure victims into running the malware.

The Story

In the middle of August we discovered a malware-spreading campaign in the Czech Republic. Our interest was first kindled by the site that the malware was hosted on – a domain that passed itself off as belonging to the Czech Postal Service – but more interesting findings followed.

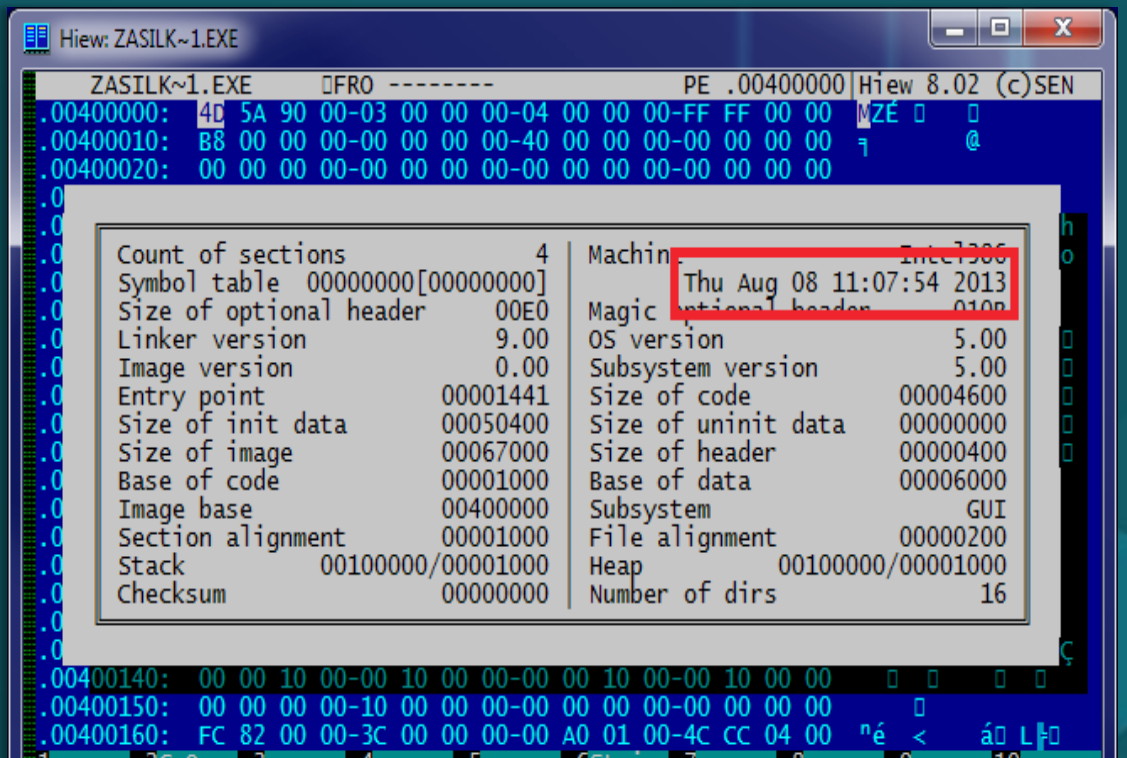
Analysis of the threat revealed that we were dealing with a banking trojan, with similar functionality and identical goals to the infamous Zeus and SpyEye, but significant implementation differences indicated that this is a new malware family, not a variant of a previously known trojan.

Despite being a "new kid on the block", it appears that Win32/Spy. Hesperbot is a very potent banking trojan which features common functionalities, such as keystroke logging, creation of screenshots and video capture, and setting up a remote proxy, but also includes some more advanced tricks, such as creating a hidden VNC server on the infected system. And of course the banking trojan feature list wouldn't be complete without network traffic interception and HTML injection capabilities. ***Win32/Spy.Hesperbot*** does all this in quite a

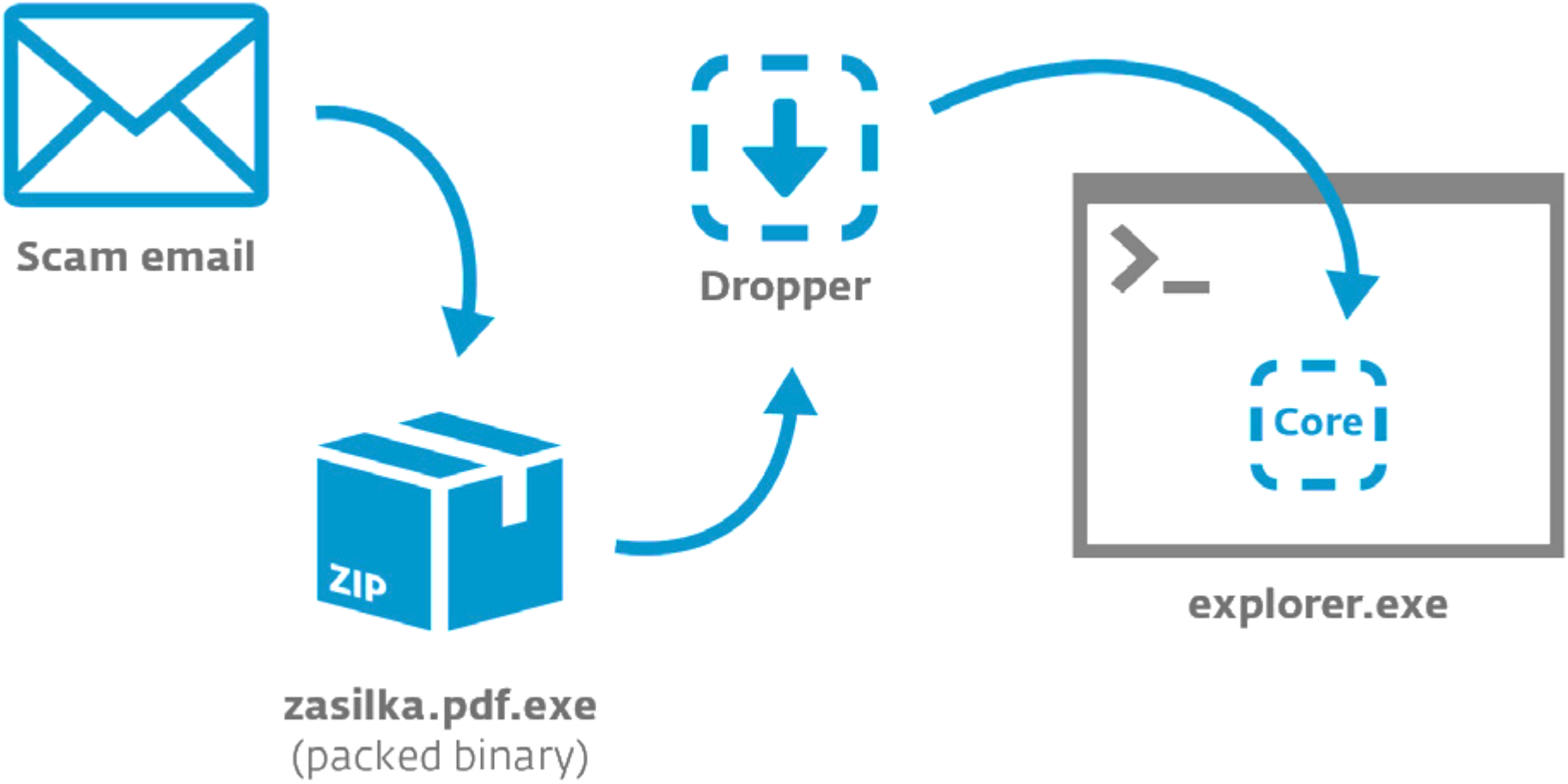
Šírenie

www.ceskaposta.net vs. *www.ceskaposta.cz*

- Česká kampaň začala 8. augusta 2013
- Turecko
- Portugalsko
- Veľká Británia



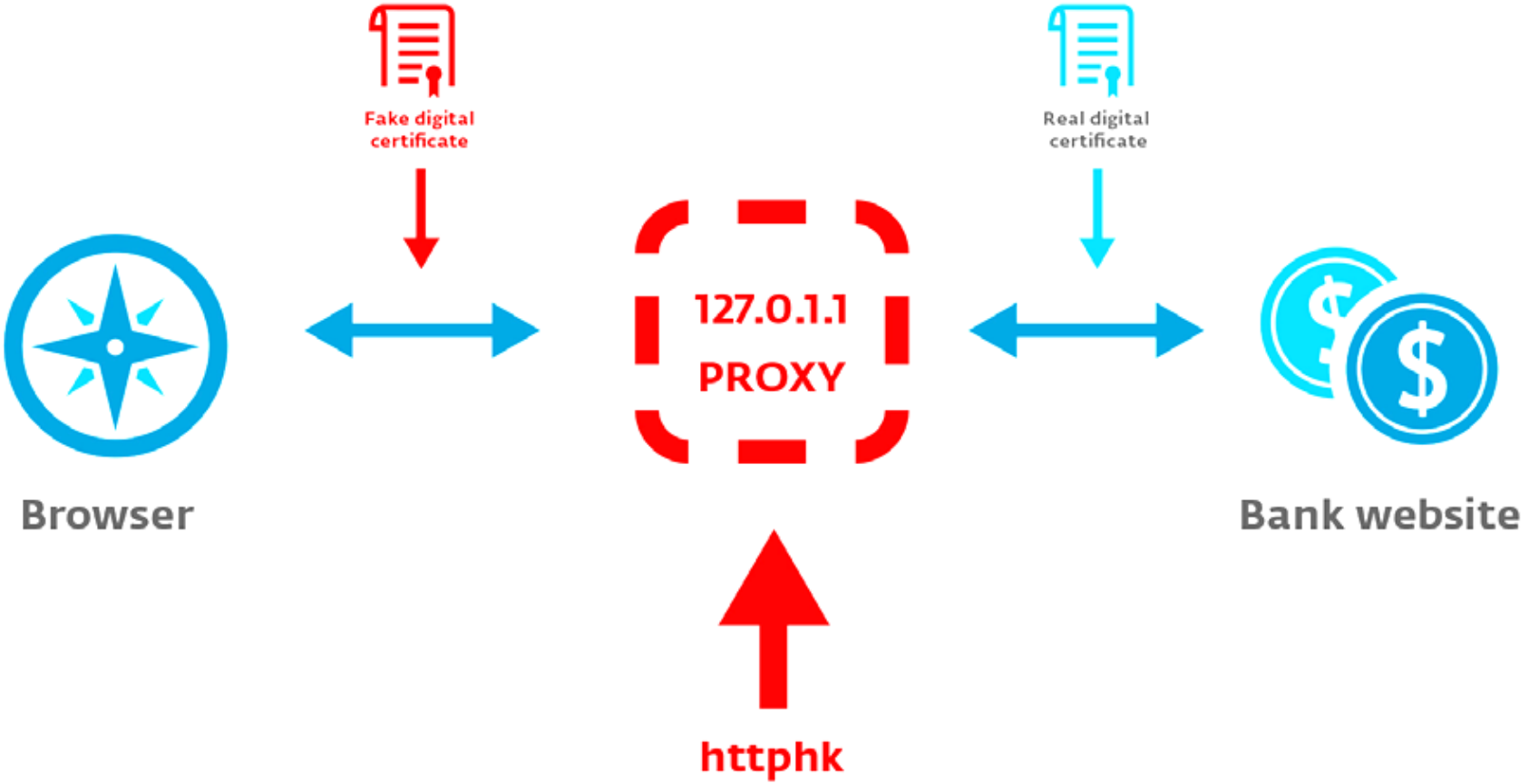
Čo a ako?

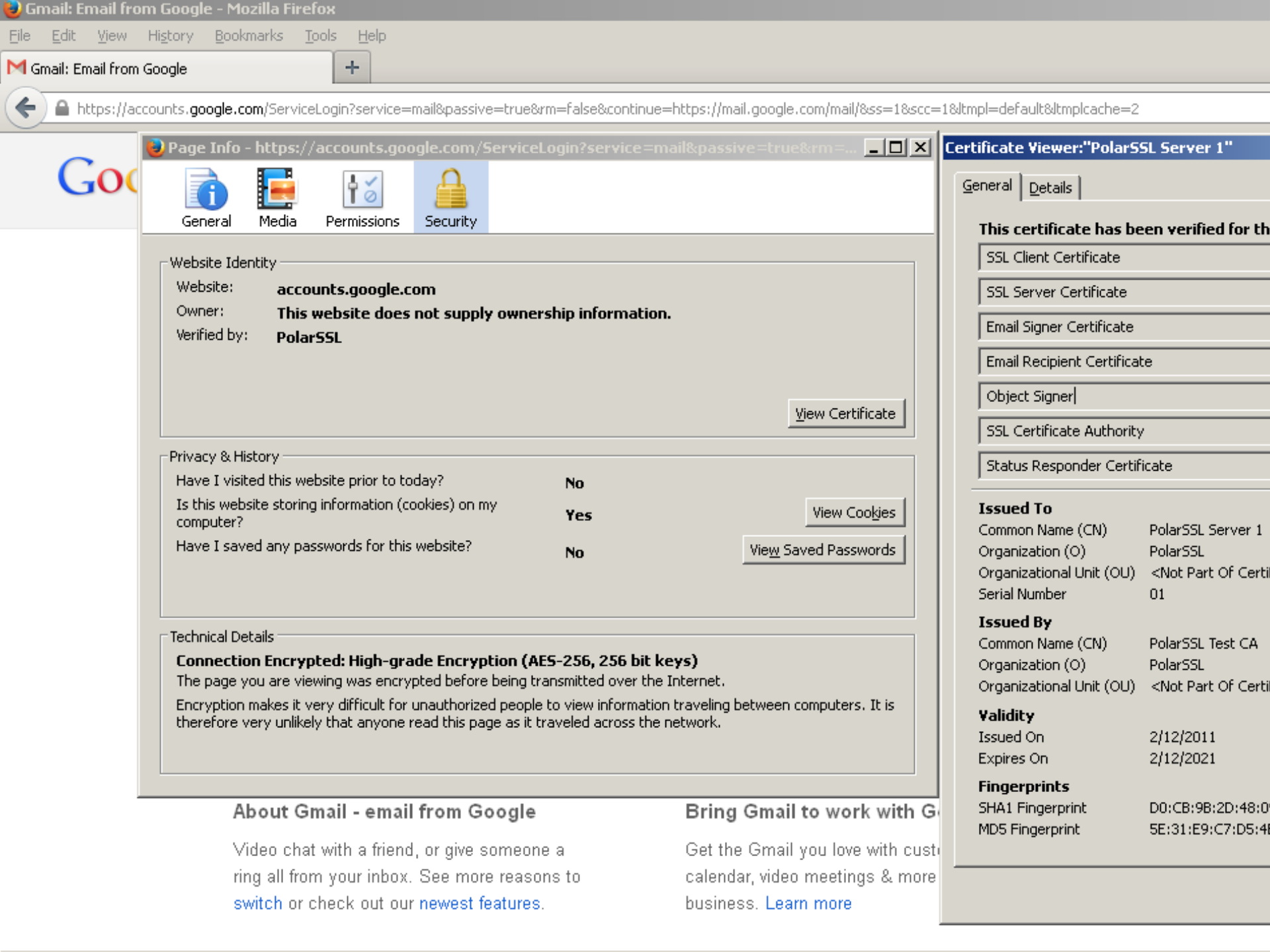

Scam email
ZIP
zasilka.pdf.exe
(packed binary)
Dropper
Core
explorer.exe

Schopnosti

- Keylogger
- Screenshots
- Video capture
- Proxy server
- VNC server
- Form grabbing
- Web-Injects

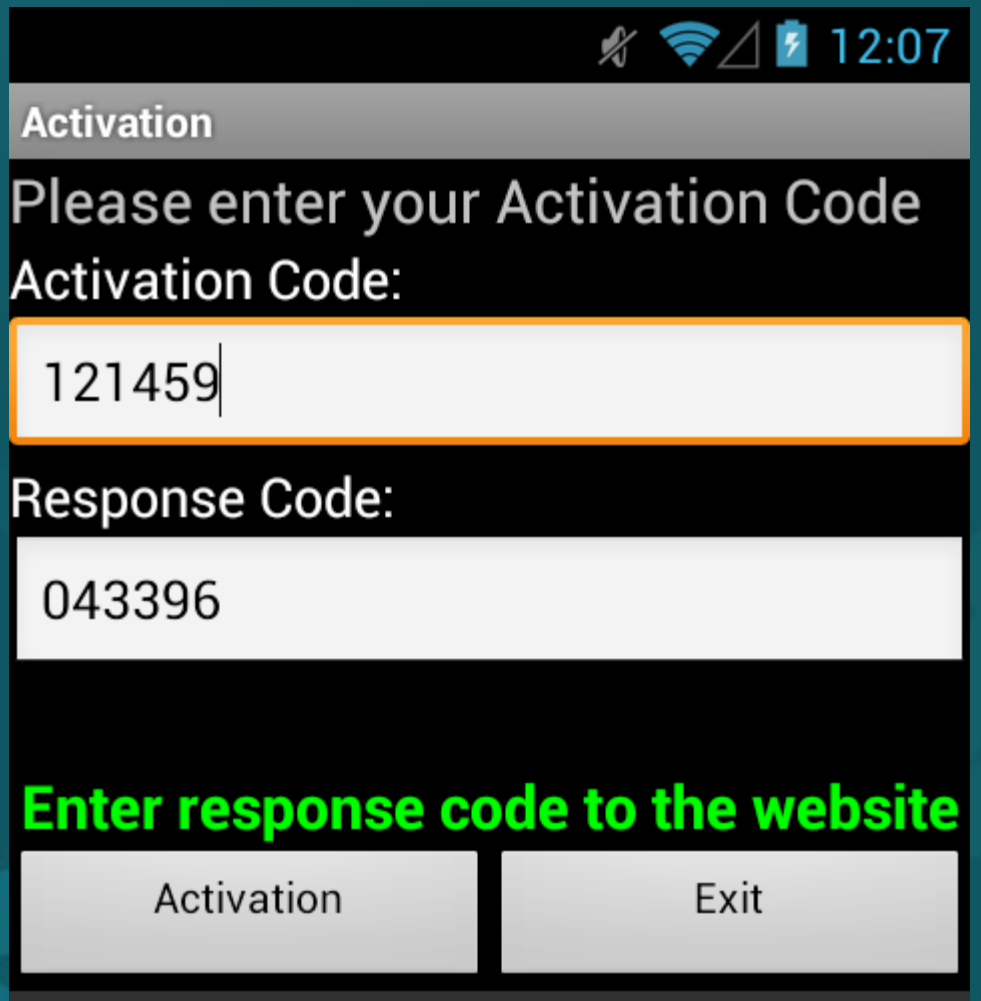
Odpočúvanie HTTPS




Gmail: Email from Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Gmail: Email from Google
https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=1&ltmpl=default&ltmplcache=2
Page Info - https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=...
General
Media
Permissions
Security
Website Identity
Website: accounts.google.com
Owner: This website does not supply ownership information.
Verified by: PolarSSL
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted: High-grade Encryption (AES-256, 256 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.
Certificate Viewer:"PolarSSL Server 1"
General
Details
This certificate has been verified for th
SSL Client Certificate
SSL Server Certificate
Email Signer Certificate
Email Recipient Certificate
Object Signer
SSL Certificate Authority
Status Responder Certificate
Issued To
Common Name (CN) PolarSSL Server 1
Organization (O) PolarSSL
Organizational Unit (OU) <Not Part Of Certi
Serial Number 01
Issued By
Common Name (CN) PolarSSL Test CA
Organization (O) PolarSSL
Organizational Unit (OU) <Not Part Of Certi
Validity
Issued On 2/12/2011
Expires On 2/12/2021
Fingerprints
SHA1 Fingerprint D0:CB:9B:2D:48:0
MD5 Fingerprint 5E:31:E9:C7:D5:4
About Gmail - email from Google
Video chat with a friend, or give someone a ring all from your inbox. See more reasons to switch or check out our newest features.
Bring Gmail to work with G
Get the Gmail you love with cust calendar, video meetings & more business. Learn more

Mobilná komponenta

- ***Android***
- *Symbian*
- *Blackberry*



Ďakujeme za pozornosť! Otázky?