



ESET[®]
SECURITY
DAYS 2013

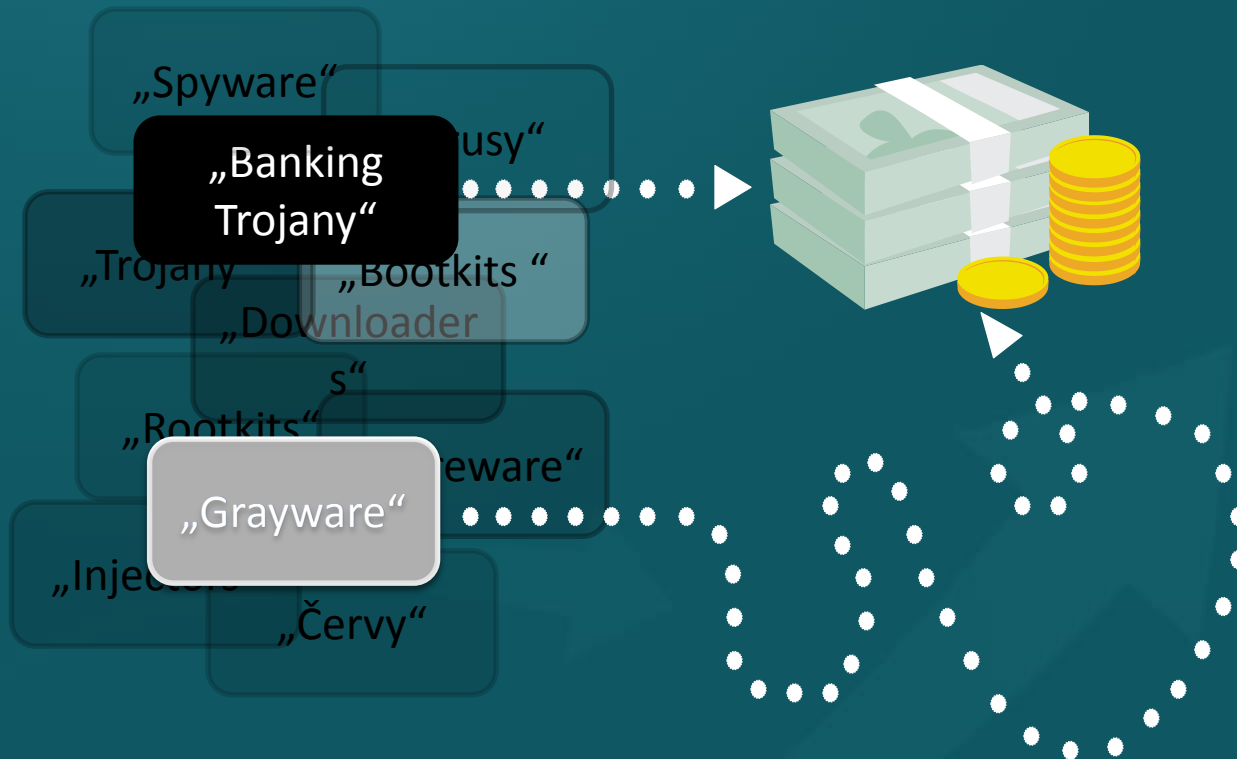
Robert Lipovský, *Malware Researcher*
Peter Stančík, *Security Evangelist*

ÚTOKY NA BANKOVÉ KONTÁ A PRÍSTUPOVÉ ÚDAJE K FINANČNÝM ZDROJOM

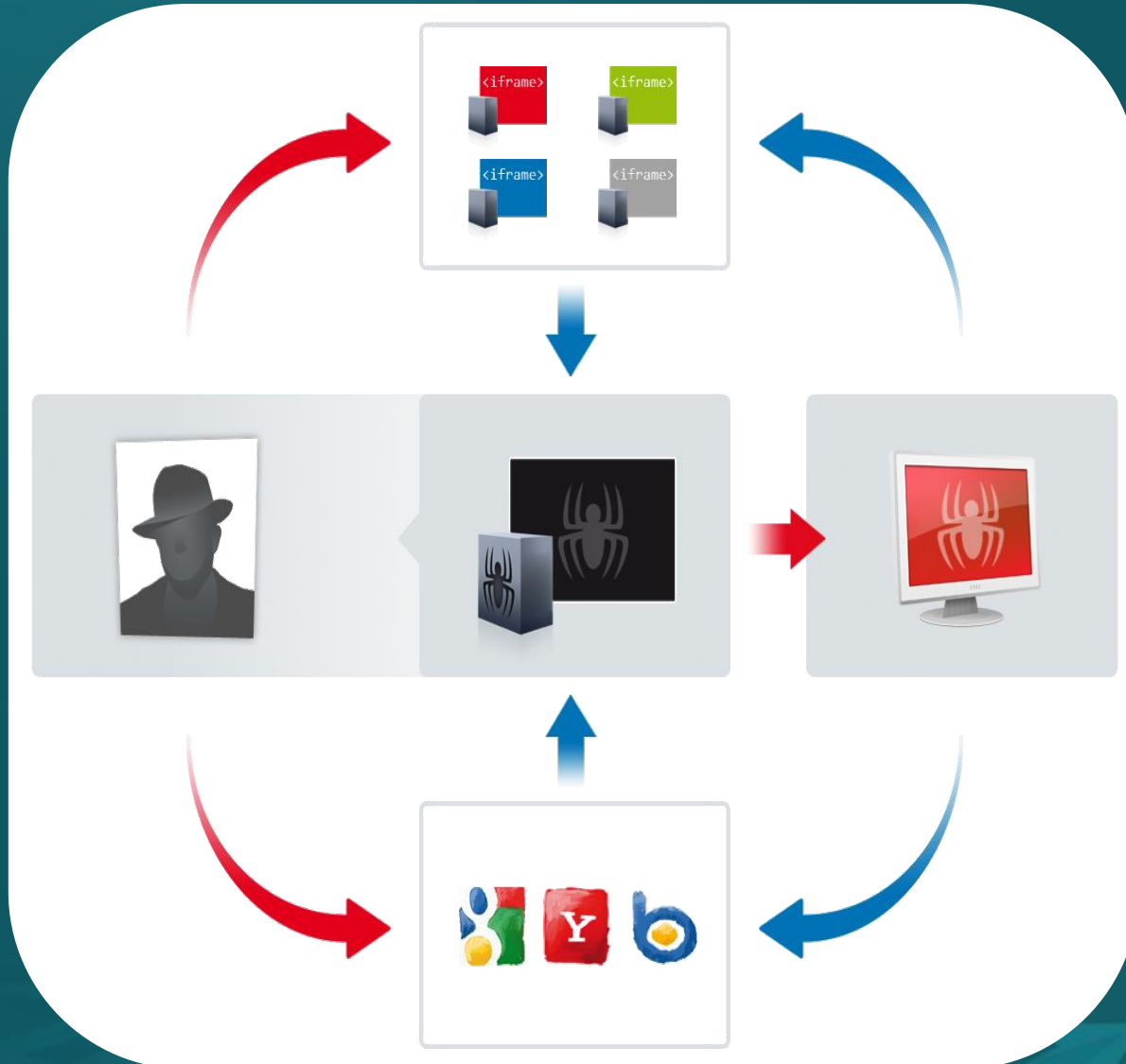
Malware včera a dnes



Malware včera a dnes



Drive-by download



Blackhat SEO

middleton wedding download

Page 4 of about 3,600,000 results

Advanced search

Everything

Images

Videos

News

Shopping

More

Show search tools

middleton wedding download

Search

[Celebrate royal Prince William Kate Middleton wedding with a ...](#)
18 Feb 2011 ... To mark the **wedding** of Prince William to Kate **Middleton**, ... like to hold a street party or fete on the royal **wedding day**, **download** and fill ...
[www.watfordobserver.co.uk/news/686263...](#) - Cached - Similar

[Catalina Maddox talks Kate Middleton's Wedding Style \(video ...\)](#)
Tyler Colton talks Kate **Middleton's Wedding** Hairstyle. Celebrity hairstylist Tyler Colton talks about how Kate **Middleton** might wear her hair for the big day ...
[www.weddingbells.ca/videos/media/cata...](#) - Cached - Similar

[Prince William and Kate Middleton's wedding to be available for ...](#)
24 Mar 2011 ... TechvibesTO says: Prince William and Kate **Middleton's wedding** to be available for digital **download** [http://ow.ly/1bUZhZ](#) - 24th Mar, 2011 ...
[royalwedding.tweetmeme.com/story/4461...](#) - Cached - Similar

[William and Kate Middleton Wedding Soundtrack 29 April 2011 ...](#)
13 Apr 2011... will be able to **download** the entire soundtrack of their nuptials ... Watch Prince William and Kate **Middleton Wedding** on Youtube Here! ...
[thailakomtv.com/2011/04/william-kate...](#) - Cached - Similar

[iDo: Royal Wedding Vows Will Be Available For Download](#)
24 Mar 2011 ... prince william and kate **middleton** iDo: Royal **Wedding** Vows Will Be Available For **Download**. Maybe it's because Americans just don't "get" the ...
[www.moxiebird.com/2011/03/ido-royal-w...](#) - Cached - Similar

[Kate Middleton Wedding Dress Ideas \(teaching.com.au\)](#)
Kate **Middleton Wedding** Dress Ideas Buy Wildlife Matters. koala500. **Download** the Wildlife Matters student activity pages & worksheets for a parent, ...
[teaching.com.au/kf-kate-middleton-we...](#) - Similar

[2011 Royal wedding Souvenir and merchandise Prince William and ...](#)
1 Apr 2011 ... How to install, Window 7, iPhone Jailbreak, Android, **Download**, ... Prince William and Kate **Middleton Royal Wedding** collectibles 2011 ...
[www.mytrendingtopics.info/prince-will...](#) - Cached - Similar

[Bridal Blog Roundup | Best Bridal News | Kate Middleton Wedding ...](#)
25 Feb 2011 ... Prince William and Kate **Middleton's** inspired **wedding** invitation and Free Custom **Download** by the **Wedding** Chicks. ...
[www.bridefinds.com/2011/must-reads-ka...](#) - Cached - Similar

[Kate Middleton's Wedding Dress Unveiled ... Sort Of - News ...](#)
The design of Kate **Middleton's wedding** dress is a secret no more and FashionEtc has exclusive details: The royal ... Royal **Wedding App**. **Download** it Now > ...
[fashionetc.com/news/news/1331-kate-mi...](#) - Cached - Similar

[Kate Middleton Wedding Dress | PDFM](#)
Search Results for: kate **middleton wedding dress** ... **Download** Ballas couple celebrates golden **wedding** anniversary PDF ...
[www.pdfm.com/tag/kate-middleton-wedd...](#) - Cached - Similar

[Videos for middleton wedding download](#)

[Kate Middleton slims down for wedding?](#)
3 min - 5 days ago
cnettv.cnet.com

[Prince William And Kate Middleton To Marry](#)
4 min - 16 Nov 2010
news.sky.com

Blackhat SEO

[World Earthquake](#) 🔍

Earthquake Information of **Japan**, **Japan** Meteorological Agency Christchurch quake: 'No bodies' in cathedral rubble · BBC News 2011-03-05 ...

[www.worldearthquake.com](#) - Cached

[Japan earthquake today news](#) 🔍

Mar 09, 2011 · Via: **japan earthquake today** - Yahoo! News Search Results Link: **japan ... Japan Earthquake News**. Mar 08, 2011 · LOS ANGELES (LALATE) – Honsu ...

[http://www.japan-earthquake-today-news.com](#) php?id=japan-earthquake-today-news - Cached

[japan earthquake march 2011 - AOL News Search Results](#) 🔍

9 Mar 2011 ... **Japan Earthquake**: Tsunami Follows Massive 8.9 **Quake**. Get Breaking News by Email ... **Japan Earthquake 2011**: 8.9 Magnitude **Earthquake** Hits,. ...

[http://www.aol.com/search?q=japan+earthquake...2011](#) - Cached

Blackhat SEO



Malware na sociálnych sieťach

The screenshot shows a Facebook chat interface. On the left is a sidebar with navigation options: News Feed, Messages (selected), Other, Events, Friends, Create Group..., Apps, and More. The main area displays a chat window with the title 'Gertruda Infikovana'. The chat history shows a conversation where Gertruda initiates contact, Robert responds with 'Hi, malware...', Gertruda asks to laugh, Robert agrees, Gertruda asks about a video, Robert confirms, and Gertruda provides a URL.

facebook Search

Robert Lipovsky
Edit My Profile

News Feed
Messages
Other 1
Events 31
Friends 1
Create Group...
Apps
More ▾
Friends on Chat

Gertruda Infikovana Messages Actions

Gertruda Infikovana 15 minutes ago
hi. how are you?

Robert Lipovsky 13 minutes ago
Hi, malware...

Gertruda Infikovana 13 minutes ago
good. Wanna laugh? 😊

Robert Lipovsky 12 minutes ago
Absolutely! 😊

Gertruda Infikovana 2 minutes ago
It is you on the video ?)) want to see?)

Robert Lipovsky 2 minutes ago
Yes, yes, yes...give me a malware sample

Gertruda Infikovana about a minute ago
<http://17...>

Robert Lipovsky is in the leading role. Shoking performance!

Yourfavoritemartian

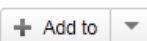
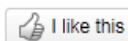
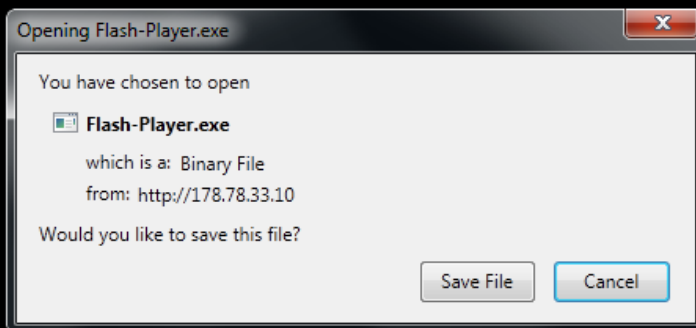
11 videos

Subscribe



You need to upgrade your Adobe Flash Player to watch this video.

Download it from Adobe.



23473



Uploaded by Yourfavoritemartian on Jun 15, 2011

You have to see it, few can do that :))) Lipovsky is on a streak!!!

568 likes, 6 dislikes

see all

He must have been shamed to do that :)))

5 minutes ago

I had to update Flash Player, but it was worth it :) this video is the very best!

6 minutes ago

one word for it – TERRIBLE!!

7 minutes ago

He's the new TV star! Put him on the tonight show! :))))))

10 minutes ago

“Lockscreeny”, Ransomware



POLÍCIA DE SEGURANÇA PÚBLICA PORTUGUESA

DEPARTAMENTO PARA COMBATER O CIBERCRIME



GOVERNO DA
PORTUGAL

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. No 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 subtexto 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 milhares 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 entregará-lhe 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



Specialist Crime Directorate Police Central e-crime Unit



**METROPOLITAN
POLICE**



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 files containing 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 with a password) in the payment form and press OK (if you have several

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 country.



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 your internet bank.

OK



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 verpflichtet 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, Q1 und Westfalen.



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

OK



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



OK



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 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 čerpacích staniciach Agipu a OMV, vo vybraných pobočkách stávkovej kancelárie Tipsport a vo všetkých predajných miestach GG Tabaku.



Kde môžem kúpiť Ukash?

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



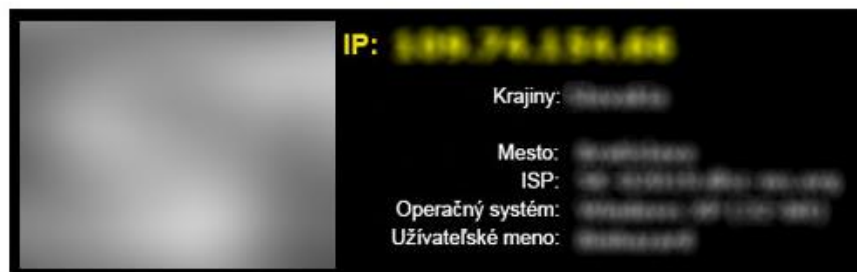
Čerpacie stanice - Ukash je teraz k dispozícii od čerpacích staníc.



ePay - Získajte Ukash z tisícov supermarketov a call obchody, kde ePay znamená.



Zostávajúci čas: 47:56:09



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/zvierackosti atď) Že ste porušil Všeobecnú deklaráciu o boji proti šíreniu detskej pornografie a obvinený z trestného činu podľa článku 161 trestného zákonníka Slovenskej republiky.

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

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 Slovenskej republiky.

Článok 148 trestného zákonníka Slovenskej 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 Slovenskej republiky (ďalej len "zákon neopatrni a nedbalé používanie počítačov (PC)")

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 staniách Agip a OMV, vo vybraných pobočkách stávkovej kancelárie Tipsport, všetkých predajných miestach GG Tabaku a vo CBA.



FileCoder



FileCoder



FileCoder

CryptoLocker

Payment for private key



Private key will be destroyed on
16. 9. 2013
7:53

Time left
5903 : 02 : 03

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](#)

Enter the transaction ID and press «Pay»:

2 BTC


<< Back PAY

Pokec Sniffer

[ÚVOD](#)[AKO TO FUNGUJE](#)[DOWNLOAD](#)[KONTAKT](#)



POKEC SNIFFER



- 100% úspešnosť v odhalení hesla
- jednoduché ovládanie
- grafické rozhranie
- podpora Win 9x/XP/7

Vitajte na stránkach Pokec Snifferu!

Pokec Sniffer je po dlhej dobe konečne program, ktorý úspešne prelomí heslo do každého albumu na Pokec(i). Jeho ovládanie je jednoduché a zvládne ho aj začiatočník. Želáme veľa príjemných chvíľ strávených jeho používaním.

Politika Ochrany osobných údajov

Pokec Sniffer môžete používať len v prípade, že ste naozaj skutočným vlastníkom zistovaného albumu! Bol vyvinutý na testovacie účely a akékoľvek jeho zneužitie je trestné podľa zákona.

Ochrana osobných údajov v Slovenskej republike upravuje zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „zákon č. 428/2002 Z. z.“). Nezávislou národnou dozornou autoritou vykonávajúcou dohľad nad ochranou osobných údajov je Úrad na ochranu osobných údajov SR (ďalej len „úrad“). Osobné údaje v zmysle § 3 zákona č. 428/2002 Z. z. sú údaje týkajúce sa určenej alebo určitej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo

Pokec Sniffer



Pokec DeCrypt

...a heslo nie je problém!

[Úvod](#)[Stiahnite si](#)[Kontakt](#)[Ako to funguje](#)

Dnes je: 15.02.2011



Pokec DeCrypt

AKO TO FUNGUJE

Program je veľmi jednoduchý a na jeho ovládanie nepotrebuje žiadne extra znalosti.

Jednoducho zadáte meno obete a následne na to názov albumu ktorého heslo chcete zistiť

a o všetko ostatné sa už postará program samotný. Vid', obrázok

Pokec DeCrypt [X]

Nick obete:

Názov albumu:

Banking trojany

DEMO

```
0000000005,0xB016A950,0x00000001,0x00000085)
HANDLEp*** Address 8016a950 has base at 80100000

.6.2 irq1:if SYSVER 0xf0000565

Name                               Dll Base DateStmp - Name
ntoskrnl.exe                       80010000 33247f88 - ai.dll
atapi.sys                          80007000 3324804 - SIPORT.
Disk.sys                           801db000 336015a - ASS2.SY
Ntfs.sys                           80237000 344eeb4 - wvid.sy
NTice.sys                          f1f48000 31ec6c8d - lappy.SY
Cdrom.SYS                          f228e000 31ec6c9 - ull.SYS
KSecDD.SYS                         f2290000 335a - .SYS
win32k.sys                         fe0c2000 34 - .dll
Cdfe.SYS                           fdca2000 3 - .sys
nbf.sys                            fdc35000 - .s
netbt.sys                          f1f68000 - .s
afd.sys                            f2008000 - .
Parport.SYS                        fdc14000 - W
netuser.sys                        f1dd0000
```

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.

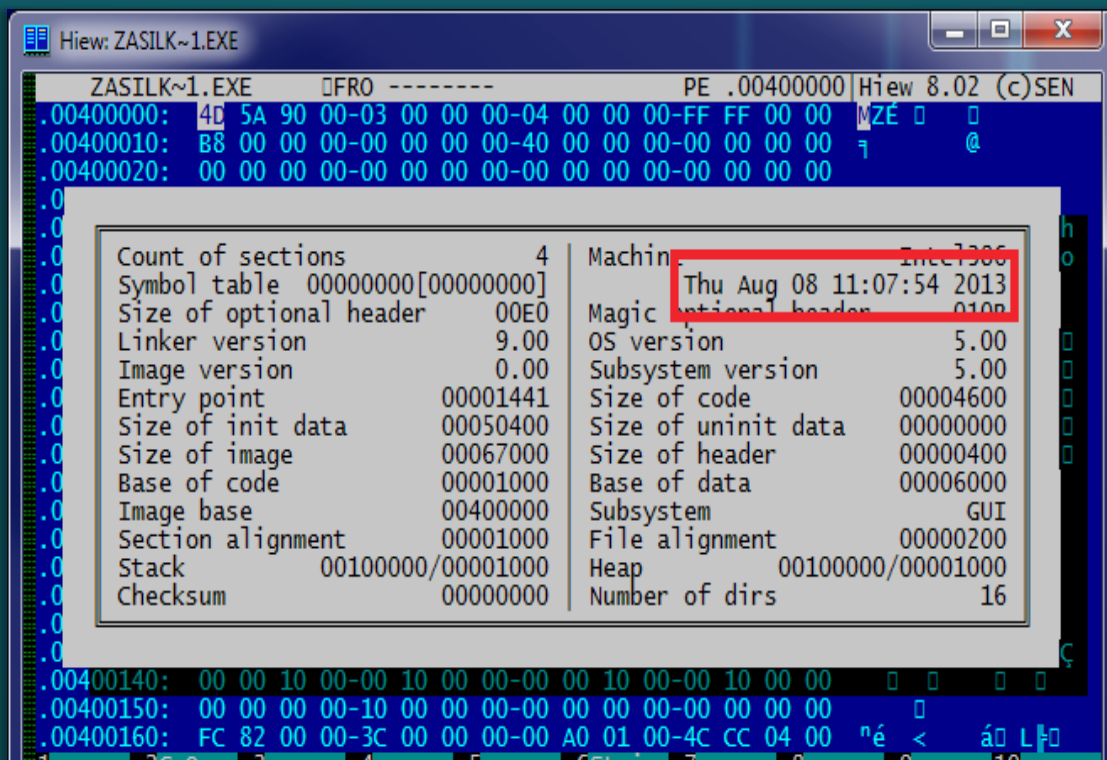
Analysis of the threat revealed that we were dealing with a banking trojan, with similar functionality and identical goals to the infamous Zeus and SpyEye, but significant implementation differences indicated that this is a new malware family, not a variant of a previously known trojan.

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 sophisticated manner.

Šírenie

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

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



Hiew: ZASILK~1.EXE

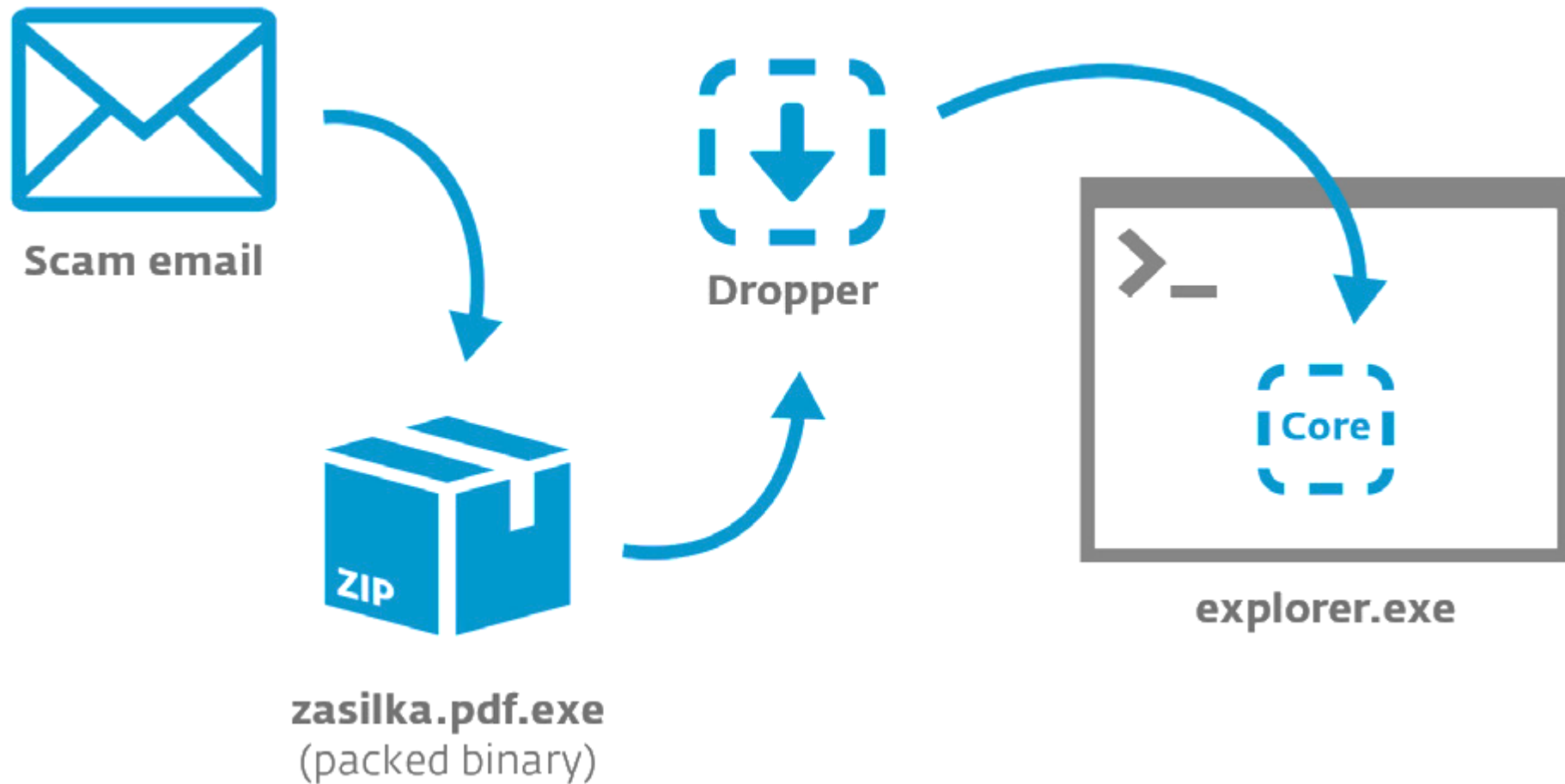
ZASILK~1.EXE PE .00400000 Hiew 8.02 (c)SEN

Count of sections	4	Machine	Intel386
Symbol table	00000000[00000000]	Creation Date	Thu Aug 08 11:07:54 2013
Size of optional header	00E0	Magic	0100
Linker version	9.00	OS version	5.00
Image version	0.00	Subsystem version	5.00
Entry point	00001441	Size of code	00004600
Size of init data	00050400	Size of unit data	00000000
Size of image	00067000	Size of header	00000400
Base of code	00001000	Base of data	00006000
Image base	00400000	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00001000	Heap	00100000/00001000
Checksum	00000000	Number of dirs	16

ceskaposta.net registry whois

Domain Name: CESKAPOSTA.NET
Registrar: ENOM, INC.
Whois Server: whois.enom.com
Referral URL: http://www.enom.com
Name Server: DNS1.REGISTRAR-SERVERS.COM
Name Server: DNS2.REGISTRAR-SERVERS.COM
Name Server: DNS3.REGISTRAR-SERVERS.COM
Name Server: DNS4.REGISTRAR-SERVERS.COM
Name Server: DNS5.REGISTRAR-SERVERS.COM
Status: clientTransferProhibited
Updated Date: 07-aug-2013
Creation Date: 07-aug-2013
Expiration Date: 07-aug-2014

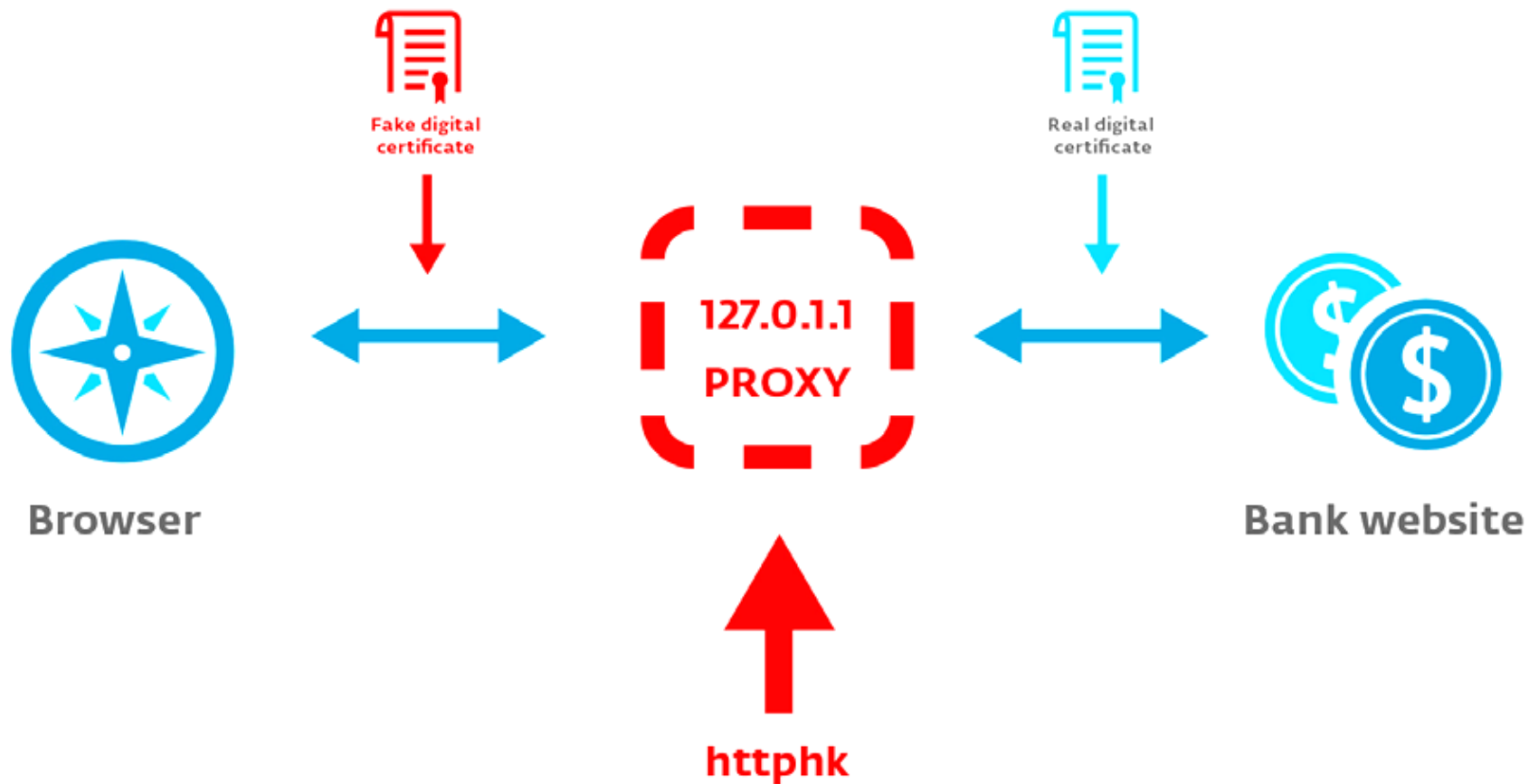
Čo a ako?



Schopnosti

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

Odpočúvanie HTTPS





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**
Have I saved any passwords for this website? **No**

[View Cookies](#)[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 the following purposes:

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 Certificate>
Serial Number	01

Issued By

Common Name (CN)	PolarSSL Test CA
Organization (O)	PolarSSL
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	2/12/2011
Expires On	2/12/2021

Fingerprints

SHA1 Fingerprint	D0:CB:9B:2D:48:0A
MD5 Fingerprint	5E:31:E9:C7:D5:4F

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 Google Workspace

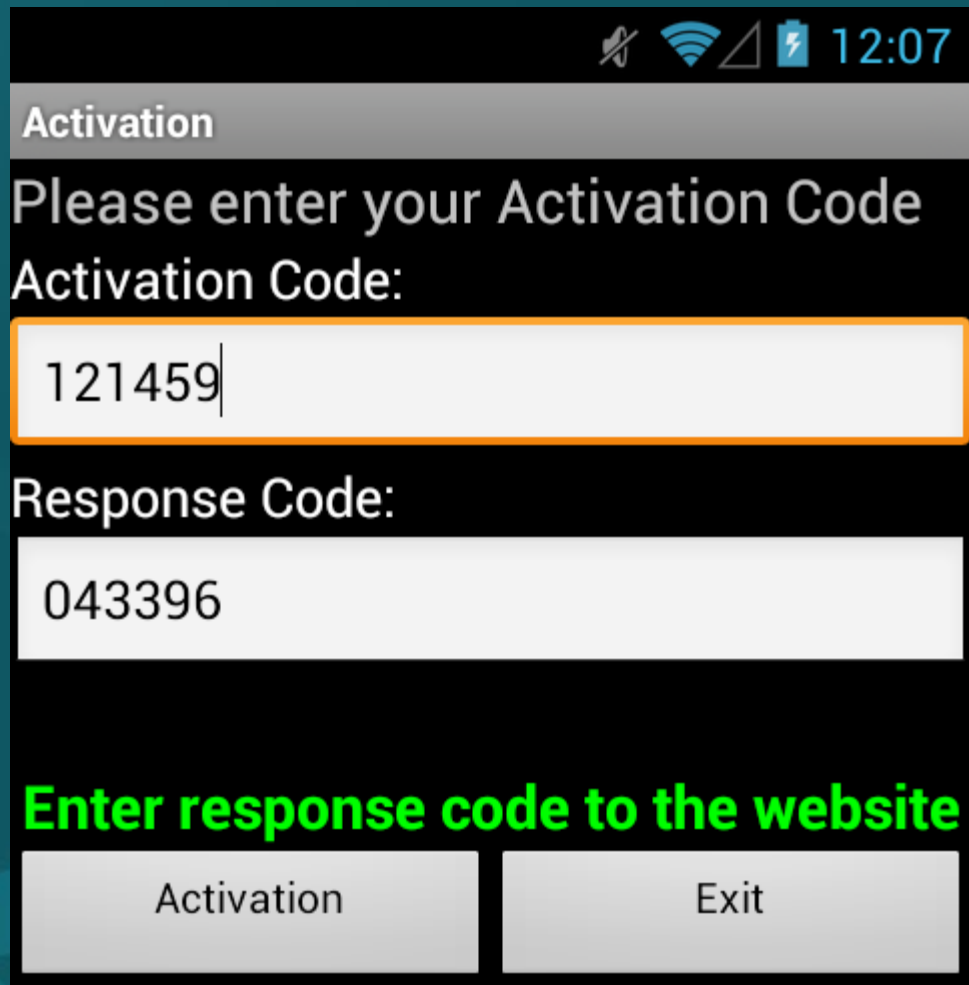
Get the Gmail you love with custom domain, calendar, video meetings & more business. [Learn more](#)

Mobilná komponenta

➤ *Android*

➤ *Symbian*

➤ *Blackberry*



The screenshot shows a mobile application interface for activation. At the top, there is a status bar with icons for signal, Wi-Fi, and battery, and the time 12:07. Below this is a header bar labeled "Activation". The main text reads "Please enter your Activation Code". Below this, the label "Activation Code:" is followed by a text input field containing the number "121459". Below the input field, the label "Response Code:" is followed by another text input field containing the number "043396". At the bottom, there is a green instruction "Enter response code to the website". Below this instruction are two buttons: "Activation" and "Exit".

Activation

Please enter your Activation Code

Activation Code:

121459

Response Code:

043396

Enter response code to the website

Activation Exit

Ďakujeme za pozornosť! Otázky?

