

# [ Banking Fraud Evolution ]

New techniques in real fraud cases

Jose Miguel Esparza



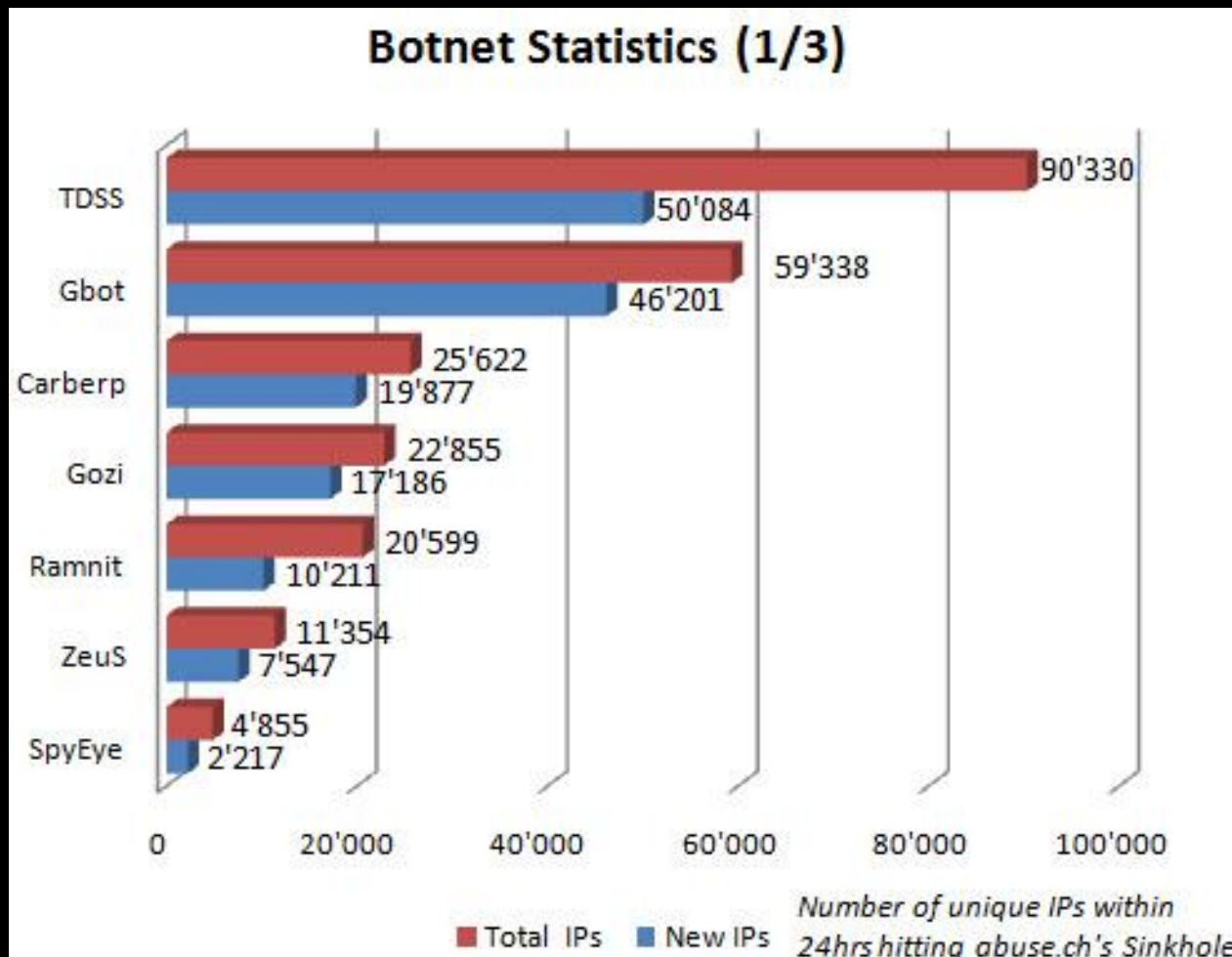
# [ Agenda ]

- Banking trojans
- Tatanga: a new actor emerges
- Anatomy of an e-banking fraud incident
- The eternal game of cat and mouse
- Real e-banking fraud incidents
- Conclusions

# [ Banking trojans ]

- ...
- Zeus
- Sinowal (Torpig)
- Gozi
- SpyEye
- Carberp
- Feodo
- ...

# [ Banking trojans ]



Source: abuse.ch

# [ Banking trojans ]

- Binaries functionalities
  - Bot
  - Configuration update
  - Binary update
  - HTML injection
  - Redirection

# [ Banking trojans ]

- Binaries functionalities
  - Screenshots
  - Capture virtual keyboards
  - Credentials theft
  - Certificates theft
  - System corruption (KillOS)

# [ Banking trojans ]

- Binaries functionalities

- Screenshots

- Ca

- Cr

**Information theft**

- Certificates theft

- System corruption (KillOS)

# [ Tatanga ]

- Discovered by S21sec in February 2011
- **Very low detection**
- *MarioForever* (2008) evolution?
- C++
- No packers
- **Modular design**
- Anti-VM, anti-debugging
- 64bits support












# [ Tatanga ]

- Proxys to distribute binaries
- Weak encrypted communication with C&C
- HTML injection
- Man in the Browser
- Records video!!

# [ Tatanga ]

- Proxys to distribute binaries
- Weak encrypted communication with C&C
- HTML injection
- Man in the Browser
- Records video!!

 1001A028	AVIStreamSetFormat	AVIFIL32
 1001A02C	AVIMakeCompressedStream	AVIFIL32
 1001A030	AVIFileCreateStreamA	AVIFIL32
 1001A034	AVIFileOpenA	AVIFIL32
 1001A038	AVIFileInit	AVIFIL32
 1001A03C	AVIFileExit	AVIFIL32
 1001A040	AVIStreamRelease	AVIFIL32
 1001A044	AVIFileRelease	AVIFIL32
 1001A048	AVIStreamWrite	AVIFIL32

# [ Tatanga ]

- Modules: XOR + BZIP2
  - HTTPTrafficLogger
  - Comm
  - ModDynamicInjection
  - ModEmailGrabber
  - ModAVTrafficBlocker
  - ModCrashGuard

# [ Tatanga ]

- Modules: XOR + BZIP2
  - ModMalwareRemover

```
call    ds>DeleteFileA
test    eax, eax
setnle [ebp+var_D]
cmp     [ebp+var_D], bl
jz      short loc_10002B1E
push    ecx
mov     ecx, esp
mov     [ebp+var_34], esp
push    offset aZeusv2Delete ; "ZeusV2 Delete"
call    ??0CString@@QAE@PBD@Z ; CString::CString(char const *)
push    1
call    sub_10009A13
pop     ecx
pop     ecx
```

# [ Tatanga ]

- Modules: XOR + BZIP2
  - SSL Decrypt
  - FilePatcher
  - IMSender
  - HTTPSender
  - Coredb
  - SmartHTTPDoser

# [ Tatanga ]

- Control panel
  - Statistics: country, browser, OS, AV, injections, honeypots
  - Injections and drops management
  - Storing dumps of banking webpages
  - Classified versions of droppers and modules
  - Dependencies between modules
  - DDoS
  - FTP iframer
  - ...

# [ Tatanga ]

## Short Summary

Total bots	1298 (31 new)	
Alive bots	553	42.6%
Dead bots	745 (39)	57.4%
Online bots	36	2.77%
Recovered bots	18 (0)	2.42%
Down. exe for recover today	0	0%
Malware infected	1068 (14)	82.28%
Zeus infected	1 (0)	0.08%
AV Protected	696 (15)	53.62%
Honey pots	24	1.85%

## Short OS Stats

Windows XP	688	53%
Windows Vista	175	13.48%
Windows Se7en	95	7.32%

## TOP 10 builds

311	880 (0)	67.8%
306	116 (0)	8.94%
301	103 (0)	7.94%
310	72 (0)	5.55%
302	66 (0)	5.08%
307	14 (0)	1.08%
916	12 (0)	0.92%
305	12 (0)	0.92%
312	12 (0)	0.92%
915	6 (0)	0.46%

## TOP 10 builds Alive

311	422	32.51%
306	64	4.93%
302	37	2.85%
312	12	0.92%
305	6	0.46%
915	3	0.23%
916	3	0.23%
307	2	0.15%
310	2	0.15%
777	2	0.15%

## TOP 10 Country Alive

	Spain	467	84.45%
	Germany	14	2.53%
	United States	11	1.99%
	Mexico	9	1.63%
	United Kingdom	8	1.45%

## TOP 10 Country Online

	Spain	33	91.67%
	Luxembourg	1	2.78%
	Israel	1	2.78%
	Brazil	1	2.78%

## TOP 10 Infested Networks

Total Networks		4		
		T	A	O
		33	2	0
		10	5	0
		5	5	0

## TOP 10 Browser Installed

	MSIE	262	39.64%
	Chrome	131	19.82%
	Netscape	126	19.06%
	Mozilla Firefox	110	16.64%

# [ Tatanga ]

Short Summary			Short OS Stats			TOP 10 builds			TOP 10 builds Alive		
Total bots	1298 (31 new)		Windows XP	688	53%	311	880 (0)	67.8%	311	422	32.51%
Alive bots	553	42.6%	Windows Vista	175	13.48%	306	116 (0)	8.94%	306	64	4.93%
Dead bots	745 (39)	57.4%	Windows								
Online bots	36	2.77%									
Recovered bots	18 (0)	2.42%									
Down. exe for recover today	0	0%									
Malware infected	1068 (14)	82.28%									
Zeus infected	1 (0)	0.08%									
AV Protected	696 (15)	53.62%									
Honey pots	24	1.85%									

TOP 10 Country Alive			TOP 10			Total Networks			Browser		
Spain	467	84.45%	Spain	33	91.67%	MSIE	262	39.64%	MSIE	262	39.64%
Germany	14	2.53%	Luxembourg	1	2.78%	Chrome	131	19.82%	Chrome	131	19.82%
United States	11	1.99%	Israel	1	2.78%	Netscape	126	19.06%	Netscape	126	19.06%
Mexico	9	1.63%	Brazil	1	2.78%	Mozilla Firefox	110	16.64%	Mozilla Firefox	110	16.64%
United Kingdom	8	1.45%									











  

Malware infected			Zeus infected			AV Protected			Honey pots		
1068	(14)	82.28%	1	(0)	0.08%	696	(15)	53.62%	24		1.85%











# [ Tatanga ]

## TOP 10 Country Dead

	Spain	619 (34)	83.09%
	Namibia	31 (1)	4.16%
	Germany	23 (0)	3.09%
	United Kingdom	22 (2)	2.95%
	United States	9 (0)	1.21%
	Brazil	7 (0)	0.94%
	Luxembourg	4 (0)	0.54%
	Costa Rica	4 (0)	0.54%
	Mexico	4 (0)	0.54%
	France	3 (1)	0.4%









## TOP 10 Software Dead

	Windows Defender	166 (12)	22.28%
	Avast	111 (9)	14.9%
	Panda	71 (3)	9.53%
	Antivir	38 (9)	5.1%
	NOD32	33 (2)	4.43%
	McAfee	30 (1)	4.03%
	Kaspersky Antivirus	22 (1)	2.95%
	VMWare	21 (1)	2.82%
	McAfee Antispyware	19 (1)	2.55%
	VMWare Tools	16 (1)	2.15%

## TOP 10 Software Installed

	Windows Defender	273 (0)	24.91%
	Avast	257 (0)	23.45%
	Panda	126 (0)	11.5%
	Antivir	74 (1)	6.75%
	NOD32	67 (0)	6.11%
	McAfee	60 (0)	5.47%
	Kaspersky Antivirus	47 (0)	4.29%
	McAfee Antispyware	43 (0)	3.92%
	VMWare	41 (8)	3.74%
	VMWare Tools	34 (8)	3.1%





















## TOP 10 AV locked

	Avast	37 (0)	2.85%
	Panda	17 (0)	1.31%
	NOD32	13 (0)	1%
	AVG	11 (0)	0.85%
	Kaspersky Anti-Virus	6 (0)	0.46%
	McAfee	3 (0)	0.23%
	Kaspersky Internet Security	3 (0)	0.23%
	Trusteer	1 (1)	0.08%
	Spyware Doctor	1 (0)	0.08%

# [ Tatanga ]

	Build	Country	Executed	Modules	Action
<input checked="" type="checkbox"/>	301		102817	DB (id:25 ver:1.0) SSL Decrypt (id:19 ver:1.22) HTTPFixerPlus (id:17 ver:1.36) WebLogs (id:18 ver:1.22) ModStaticInject (id:22 ver:3.56) ModRemoteControl (id:23 ver:1.35) ModEmailGrabber (id:13 ver:1.11) FTP+Email (id:3 ver:1.6) PEInfector (id:33 ver:1.45) MalwareRemover (id:2 ver:1.24) Web Sender (id:14 ver:1.22)	✗
<input checked="" type="checkbox"/>	300		715	DB (id:25 ver:1.0) SSL Decrypt (id:19 ver:1.22) HTTPFixerPlus (id:17 ver:1.36) WebLogs (id:18 ver:1.22) ModStaticInject (id:22 ver:3.56) ModRemoteControl (id:23 ver:1.35) ModEmailGrabber (id:13 ver:1.11) FTP+Email (id:3 ver:1.6) PEInfector (id:33 ver:1.45) MalwareRemover (id:2 ver:1.24) Web Sender (id:14 ver:1.22)	✗

# [ Tatanga ]

Id	Module	Version	Comment	Dependence	Action
18	Web Logger	1.22		HTTPFixerPlus (17) SSL Decrypt (19) DB (25)	 
19	SSL Decrypt	1.26		Intercept (20)	 
20	Interceptor	0			 
21	SmartHTTPDoser	0		DB (25)	 
22	ModStaticInject	0		WebLogs (18)	 
23	RemoteControl	0			 
25	Core DB	1.1			 
30	ModBlockAVTraffic	1.22			 
33	PEInfector	0			 
61	AT Control	1.51		DB (25) SSL Decrypt (19) HTTPFixerPlus (17) WebLogs (18)	 

# [ Tatanga ]

---

**AT Control**

**Maintenan**

**List Drops**



**Inject options**

**Inject requests**

**Page Dumper**

**Inject dumps**

**Inject stats**

**Config**



# [ Tatanga ]

Recipient	
Country	[DE] Germany
Account Name	
Account #	
Routing/BSB#	
Bank name	
Bank address	
Currency	EUR
Payment type	internal
Transfer Mode	Automatic
Status	used





















Comment

Save

# [ Tatanga ]

[Add new server](#)

Current domen for recover:

ID	IP	Domen	Speed	Scripts	FTP Access	Action
1	<input type="text"/>	<input type="text"/>	0.00 Kb/s	<span style="color: red;">●</span>	<span style="color: green;">●</span>	 
3	<input type="text"/>	<input type="text"/>	12609.76 Kb/s	<span style="color: red;">●</span>	<span style="color: green;">●</span>	 
4	<input type="text"/>	<input type="text"/>	0.00 Kb/s	<span style="color: red;">●</span>	<span style="color: red;">●</span>	 
5	<input type="text"/>	<input type="text"/>	3602.79 Kb/s	<span style="color: green;">●</span>	<span style="color: red;">●</span>	 
6	<input type="text"/>	<input type="text"/>	0.00 Kb/s	<span style="color: green;">●</span>	<span style="color: red;">●</span>	 
7	<input type="text"/>	<input type="text"/>	2521.95 Kb/s	<span style="color: green;">●</span>	<span style="color: green;">●</span>	 
8	<input type="text"/>	<input type="text"/>	8406.51 Kb/s	<span style="color: green;">●</span>	<span style="color: green;">●</span>	 
9	<input type="text"/>	<input type="text"/>	8406.51 Kb/s	<span style="color: green;">●</span>	<span style="color: green;">●</span>	 
10	<input type="text"/>	<input type="text"/>	3152.44 Kb/s	<span style="color: green;">●</span>	<span style="color: green;">●</span>	 
11	<input type="text"/>	<input type="text"/>	12609.76 Kb/s	<span style="color: green;">●</span>	<span style="color: green;">●</span>	 

# [ Tatanga ]

Smart DDoS

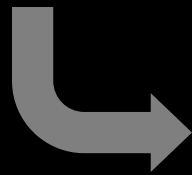
Smart DDoS Stats

Script	Base.js ▾
Profile	test2 ▾
Host	http://[redacted] ▾
Type	<input type="radio"/> Online <input checked="" type="radio"/> 3 Hour <input type="radio"/> 6 Hour <input type="radio"/> 12 Hour <input type="radio"/> Day
Date	<input type="text"/>
Time	00 <input type="text"/> hour

Filter

# [ Anatomy of an e-fraud incident ]

- Infection
- Configuration file update/download
- Interaction with the user



**Social engineering!!**



HTML injection, Mit(B|M|Mo), Pharming, Phishing...

- Banking credentials theft



# [ Anatomy of an e-fraud incident ]

- Account spying
  - Manual / Automatic
  - Getting **balance** to choose the victim
- Fraudulent transaction
  - Manual → **Mules**
  - Automatic → **Man in the Browser (MitB)**
- Money laundering

# [ The game of cat and mouse ]

ID + Password

Virtual keyboard

2FA

OTP

Code card

Token

SMS : mTAN



# [ The game of cat and mouse ]

## 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...

# [ The game of cat and mouse ]

## 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 se 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...

# [ The game of cat and mouse ]

Token

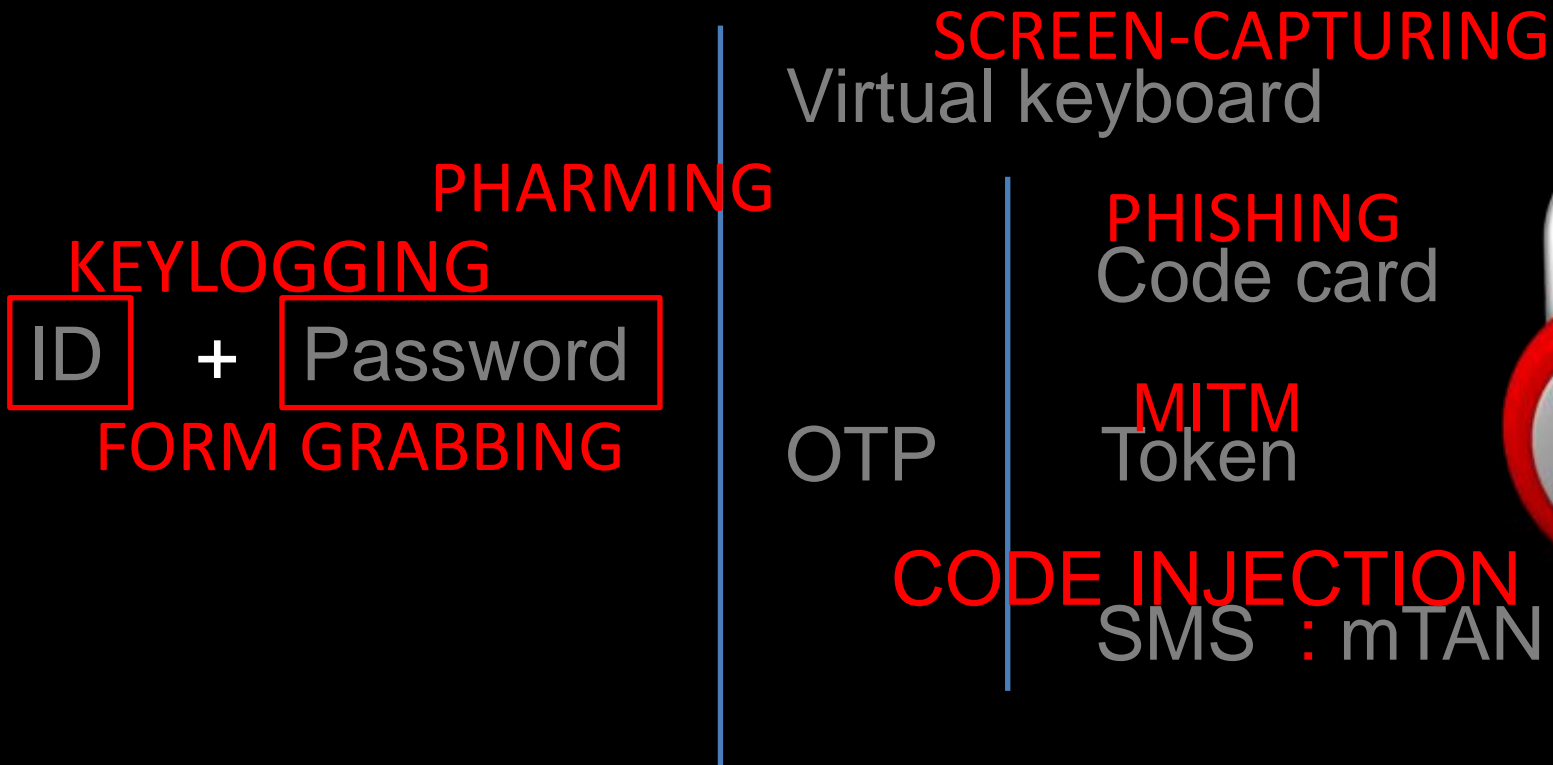


mTAN



...MITM, code injection

# [ The game of cat and mouse ]



# [ Real e-banking fraud incidents ]

- **SpyEye** MitB, October 2010
- Automatic fraudulent transfer
  - Session of the legit user
  - Balance request
  - Account selection based on balance
  - Getting mules from the server
  - Social engineering  $\longrightarrow$  password request
  - Automatic transaction
  - Modification of balance and operations

# [ Real e-banking fraud incidents ]

- **Tatanga** MitB, February 2011
- Automatic fraudulent transfer **using OTP**
  - **Session of the legit user**
  - Balance request
  - **Account selection based on balance**
  - **Getting mules from the server**
  - Social engineering  $\longrightarrow$  password request
  - Social engineering  $\longrightarrow$  **OTP request**
  - **Automatic transaction**
  - **Modification of balance and operations**



# [ Real e-banking fraud incidents ]

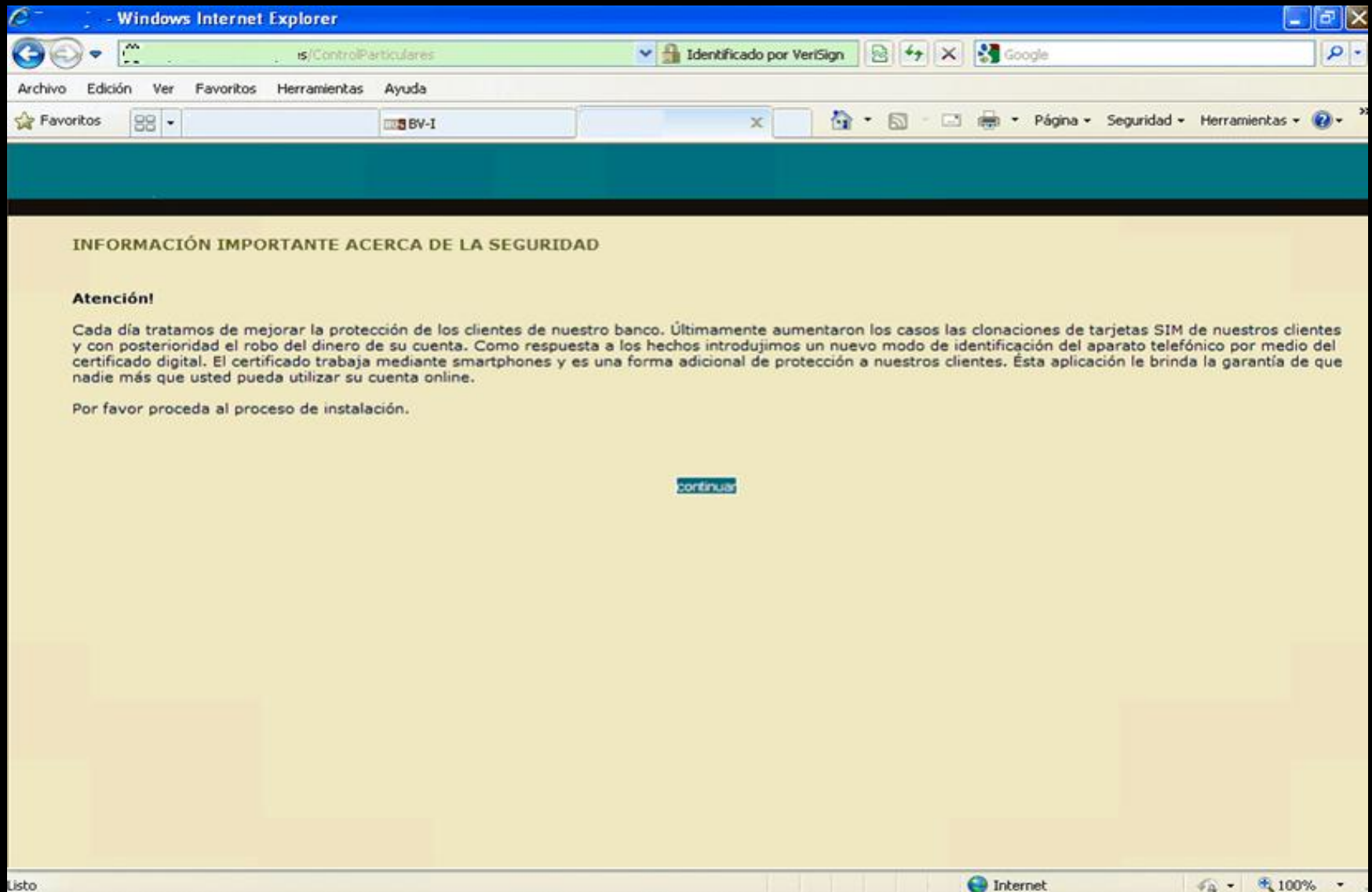
- **Tatanga MitB, February 2011**

```
</div>
<div id="step2" class="logoutWarning" style="display:none;">
  <h2>Security measures - Step 2 of 2</h2>
  <div class="logoutMsg" style="overflow:hidden;">
    <p><strong>As an additional security measure, we spend obligatory
of a correctness of your phone number entered in a profile and that that you it is
nstead of the malefactor who has got access to your account.<br>
    Now to you the test call will be made and the demo transfer from
is initialized, thus we confirm that you are a genuine account owner.</strong></p>
    <div class="primary"><div class="subPanel authPanel" style="margi
our authentication number is</p><p class="authNumber" style="font-size: 4em;" id="s
p><p>(we'll ask you for this number when we call)</p></div></div>
    <div class="inner authResponse1"><h3>Your authentication is in pr
>Contacting you on Mobile: <span id="step2_phone"></span></p></div>
    <div class="inner dash"><h3>Once your phone authentication has be
...</h3><p>Click 'Continue' to complete the process.</p></div>
    <p><strong>Pay attention, transfer is just a demo. No real means
count. The given procedure is obligatory and without its performance you can't get
r account. Your safety - our primary goal.</strong></p>
  </div>
  <ul class="actions">
```

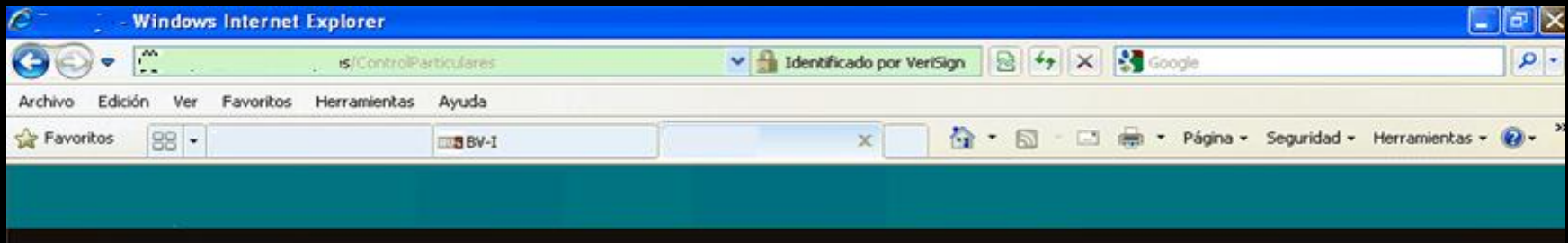
# [ Real e-banking fraud incidents ]

- **ZeuS** Man in the Mobile (MitMo)
  - September 2010, Spain
  - February 2011, Poland

# [ Zeus Man in the Mobile ]



# [ ZeuS Man in the Mobile ]



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

# [ Zeus Man in the Mobile ]

Ustawienia | Bezpieczeństwo | Regulacje | Pomoc | Drukuj | Odśwież

→ Wyjście

Strona główna | Przelewy | Rachunki | Oszczędności | Karty | Kredyty | Kontakt | Wnioski | bankujesz-kupujesz.pl

Zalogowany użytkownik:

Ostatnie logowanie: 2011-02-09 16:29 Adres IP: 127.0.0.1  
Nieudane logowanie: 2011-02-09 16:28 Adres IP:

### Ważna informacja dotycząca bezpieczeństwa

#### Uwaga

Z każdym dniem staramy się poprawiać ochronę dla klientów naszego banku. Dany certyfikat funkcjonuje **na smartfonach** i jest dodatkowym środkiem ochronnym klientów naszego banku.

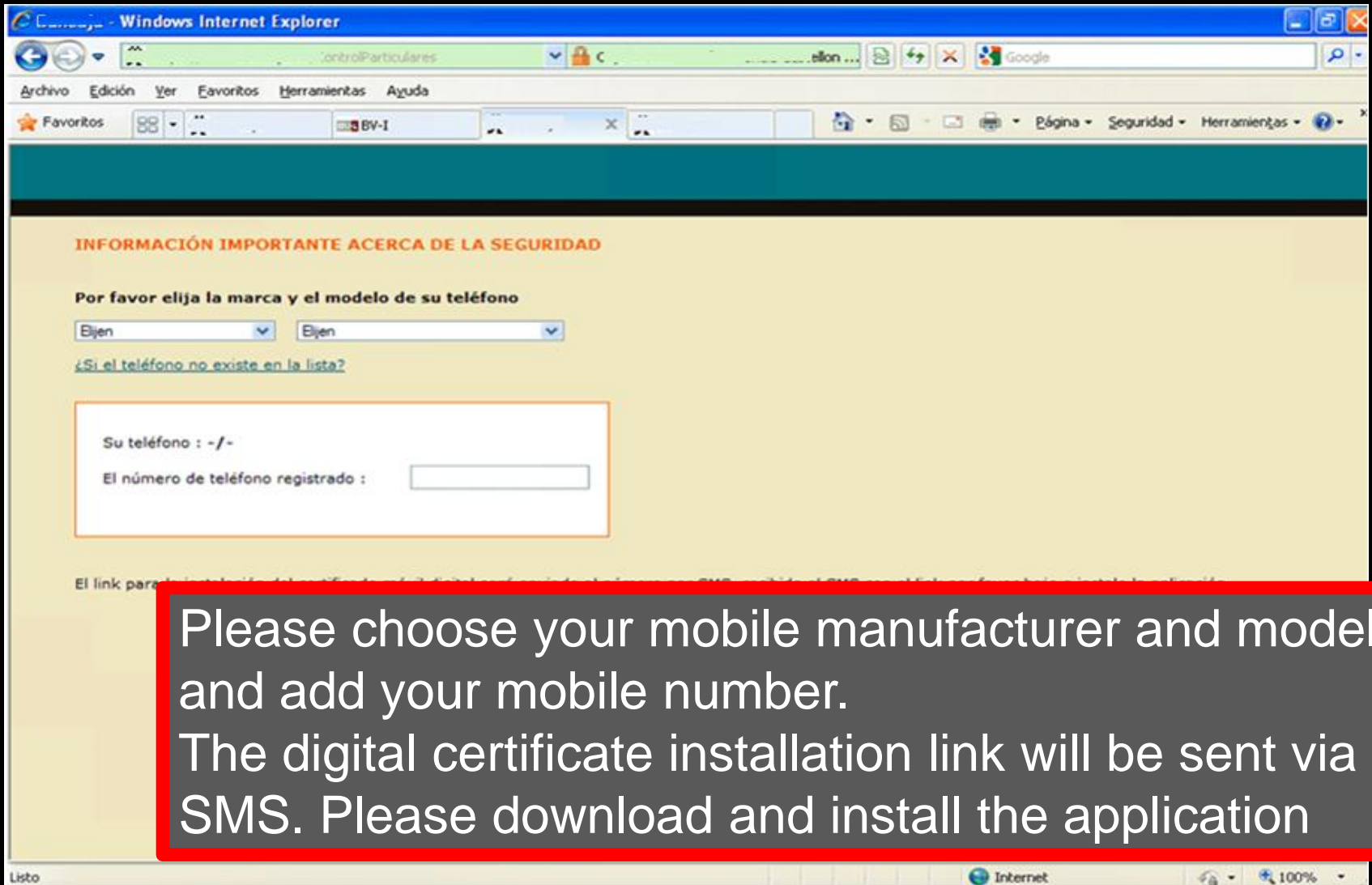
Ten załącznik gwarantuje, że właśnie PAŃSTWO, i nikt inny nie będzie mógł skorzystać z Państwa rachunku on-line.

Proszę zainstalować aplikację.

[Dalej >>](#)

Source: <http://niebezpiecznik.pl/post/zeus-straszy-polskie-banki/>

# [ ZeuS Man in the Mobile ]



**INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD**

Por favor elija la marca y el modelo de su teléfono

Eijon Eijon

[¿Si el teléfono no existe en la lista?](#)

Su teléfono : -/-

El número de teléfono registrado :

El link para...

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 Man in the Mobile ]

Ustawienia | Bezpieczeństwo | Regulacje | Pomoc | Drukuj | Odśwież

→ Wyjście

Strona główna | Przelewy | Rachunki | Oszczędności | Karty | Kredyty | Kontakt | Wnioski | bankujesz-kupujesz.pl

Zalogowany użytkownik:

Ostatnie logowanie: 2011-02-09 16:29 Adres IP: 127.0.0.1  
Nieudane logowanie: 2011-02-09 16:28 Adres IP:

### Ważna informacja dotycząca bezpieczeństwa

Proszę wybrać markę i model telefonu

Co robić, jeśli mojego telefonu nie ma na liście?

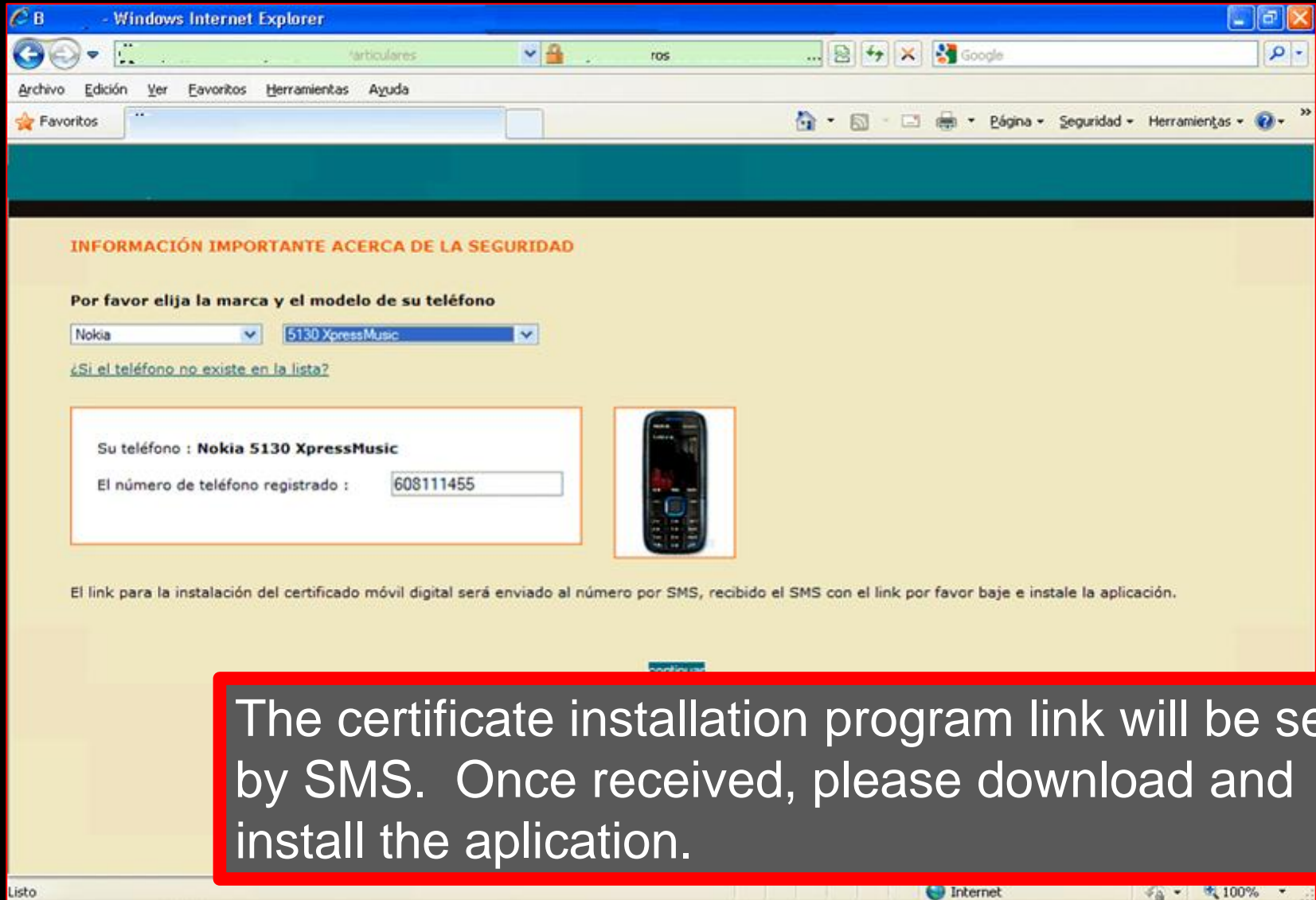
Wybrany telefon komórkowy : -/-

**Telefon komórkowy :**

Link do zainstalowania mobilnego cyfrowego certyfikatu zostanie wysłany na numer za pomocą sms, po otrzymaniu sms z linkiem należy go pobrać i zainstalować załącznik

[Dalej >>](#)

# [ ZeuS Man in the Mobile ]



The screenshot shows a Windows Internet Explorer browser window. The address bar contains the URL "http://www.arbitrales.com/". The page title is "Información importante acerca de la seguridad". The main content area has a yellow background and contains the following text:

**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



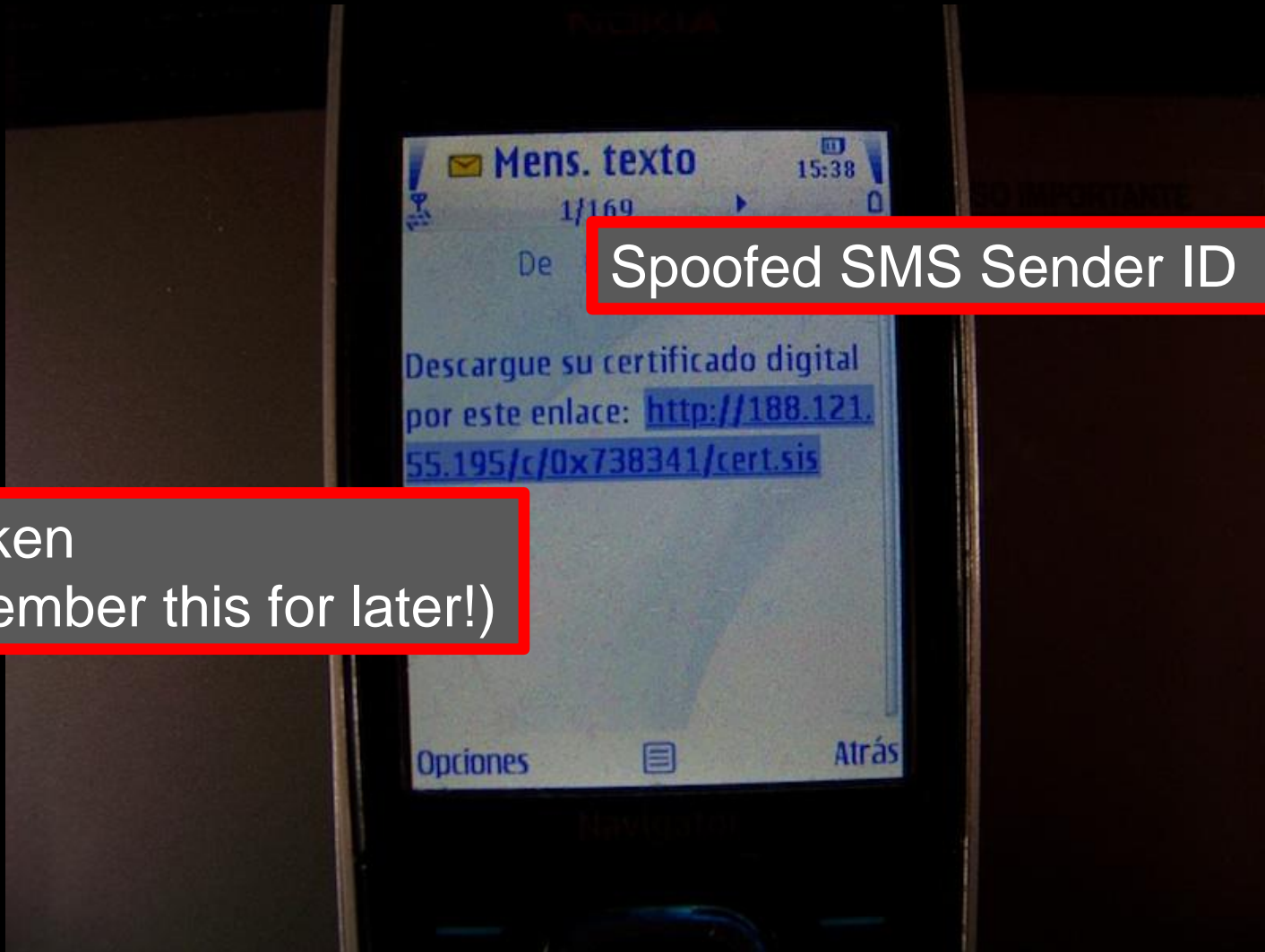
El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

At the bottom of the browser window, the status bar shows "Listo" on the left and "Internet" and "100%" on the right.

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



# [ ZeuS Man in the Mobile ]



Spooferd SMS Sender ID

ID Token  
(remember this for later!)

# [ ZeuS Man in the Mobile ]

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 signing. The main area displays the package path 'E:\Nokia\Data\download\cert.sis' and the package name 'Nokia update'. Below this, there are two columns of fields for package metadata and target device information.

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]		

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

# [ ZeuS Man in the Mobile ]



**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.

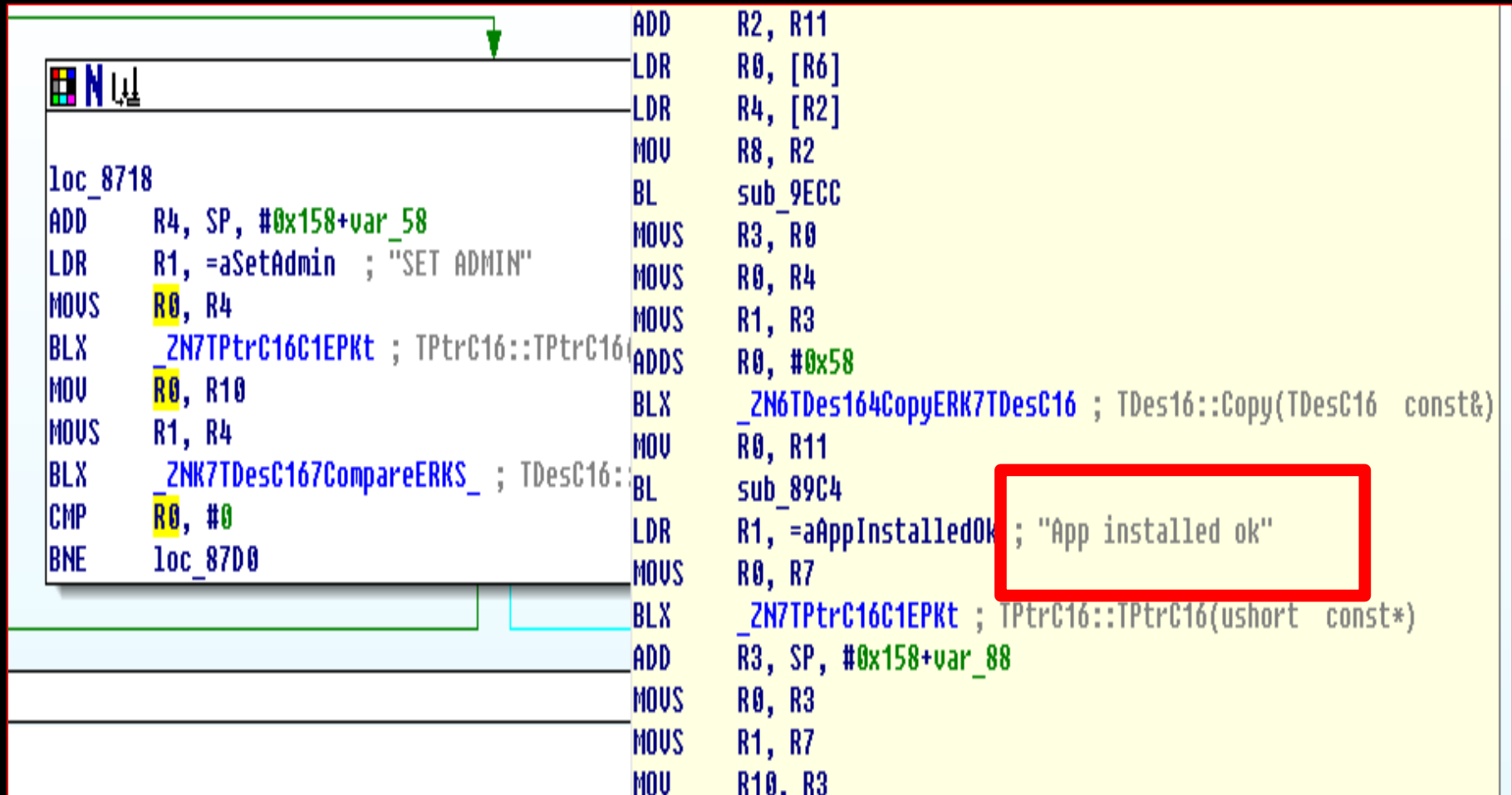
**WARNING!** This application is intended to be used only for private and legal purposes. It cannot be used for violating anyone's rights, spying or other illegal purposes. User of SMS Monitor takes all responsibility for using this application in any illegal use cases.

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

Buy

[http://dtarasov.ru/smsmonitor\\_lite.html](http://dtarasov.ru/smsmonitor_lite.html)

# [ ZeuS Man in the Mobile ]



```
loc_8718
ADD R4, SP, #0x158+var_58
LDR R1, =aSetAdmin ; "SET ADMIN"
MOVS R0, R4
BLX _ZN7TPtrC16C1EPkt ; TPtrC16::TPtrC16
MOV R0, R10
MOVS R1, R4
BLX _ZNK7TDesC167CompareERKS_ ; TDesC16:
CMP R0, #0
BNE loc_87D0

ADD R2, R11
LDR R0, [R6]
LDR R4, [R2]
MOV R8, R2
BL sub_9ECC
MOVS R3, R0
MOVS R0, R4
MOVS R1, R3
ADDS R0, #0x58
BLX _ZN6TDes164CopyERK7TDesC16 ; TDes16::Copy(TDesC16 const&)
MOV 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
MOV R10, R3
```

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

# [ ZeuS Man in the Mobile ]

ON / OFF  
SET ADMIN  
ADD  
REM  
SET

SENDER | ALL

```
.text:791B22A0 var_10= -0x10
.text:791B22A0 oIdR11= -0xC
.text:791B22A0 oIdSP= -8
.text:791B22A0 oIdLR= -4
.text:791B22A0
Program control flow
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]
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:791B22E8
```

UNKNOWN | 791B22A0: esremitentechungoo

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	.)a.....
00612AF8	03 03 03 03 03 03 03 03 03 03 03 03 03 03 03	.....(1.y...
00612B08	03 03 03 03 60 00 00 00 28 31 1D 79 00 00 00 00	.....+4.4.7.
00612B18	0D 00 00 30 20 00 00 00 2B 00 34 00 34 00 37 00	7.8.1 [REDACTED]
00612B28	37 00 38 00 31 00 [REDACTED] 00	5.....
00612B38	35 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00612B48	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	.....
00612B68	70 2B 61 00 28 00 00 00 70 93 1D 79 B8 40 61 00	p+a.(...p0.y+@a.

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

# [ ZeuS Man in the Mobile ]

**CP :: Summary statistics**

Information:  
Current user: 8frcvvh8  
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:  
> Installed  
bi o.pers (2)  
bi o.corp (2)

si der.corp (2)  
bt l)  
bi s.pers (4)  
bi s.corp (2)  
ca r (2)  
ca iarias (2)  
ca (3)  
di it (5)  
ur (4)

Terminado

**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		

# [ ZeuS Man in the Mobile ]

The screenshot shows a Mozilla Firefox browser window displaying a web page titled "CP :: Summary statistics". The browser's address bar shows the URL "http://.../jag/cpz.php?m=stats\_main". The page content is organized into several sections:

- Information:** Current user: 8frcvh8, 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:** > Installed
  - bi o.pers (2)
  - bi o.corp (2)
  - sa der.pers (3)
  - sa der.corp (2)

A red rectangular box highlights the "Banks" and "SMS" sections. A red arrow points from the "Banks" section in the left sidebar to the "Banks" section in the main content area. The status bar at the bottom of the browser window shows "Terminado" and "TW".

# [ ZeuS Man in the Mobile ]

```
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)
```

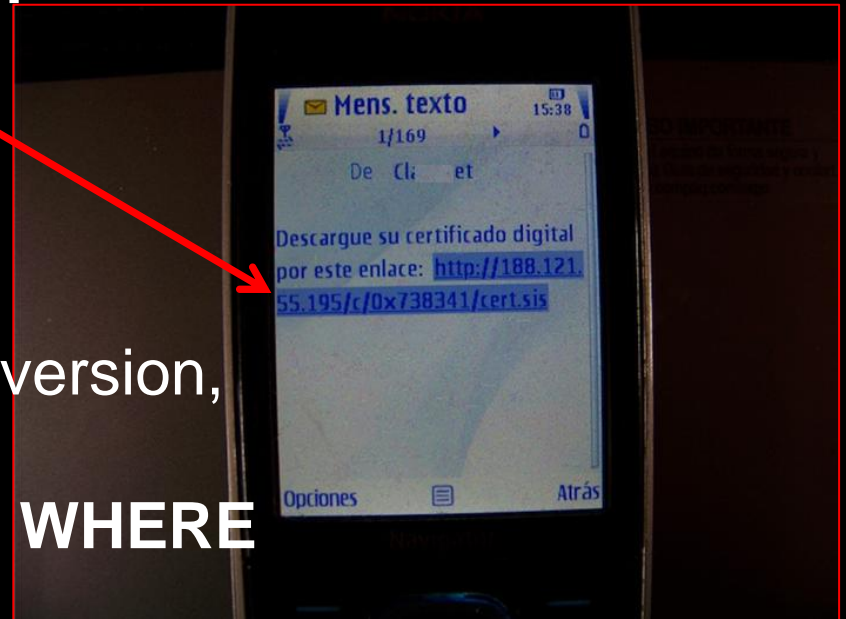




# [ ZeuS Man in the Mobile ]

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'");
```



# [ ZeuS Man in the Mobile ]



ZeuS infected



# [ ZeuS Man in the Mobile ]



ZeuS infected



# [ ZeuS Man in the Mobile ]

ID + PASSWORD



ZeuS infected



# [ ZeuS Man in the Mobile ]

ID + PASSWORD



ZeuS infected



Mitmo Infected



# [ ZeuS Man in the Mobile ]

ID + PASSWORD



ZeuS infected



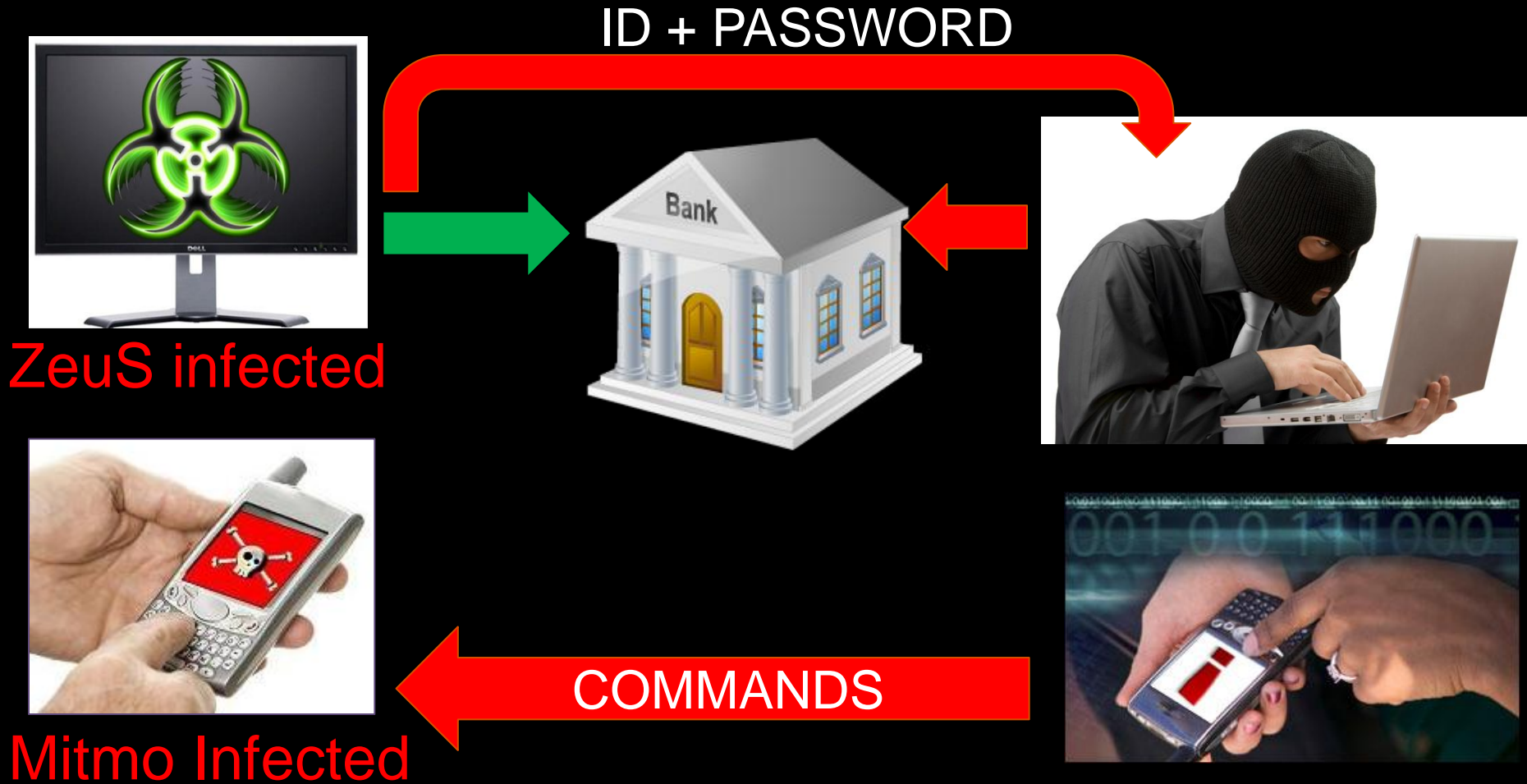
Mitmo Infected



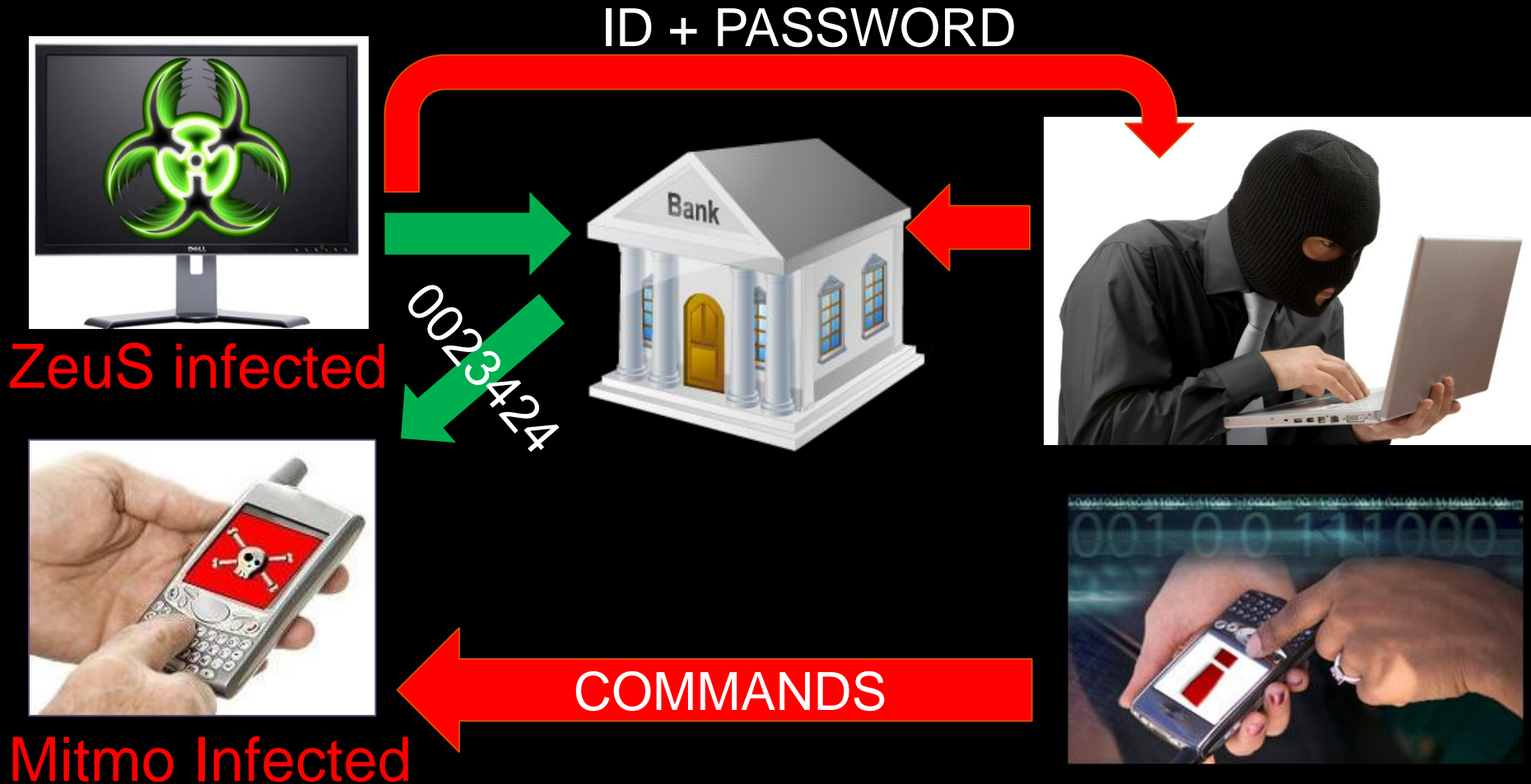
COMMANDS



# [ ZeuS Man in the Mobile ]

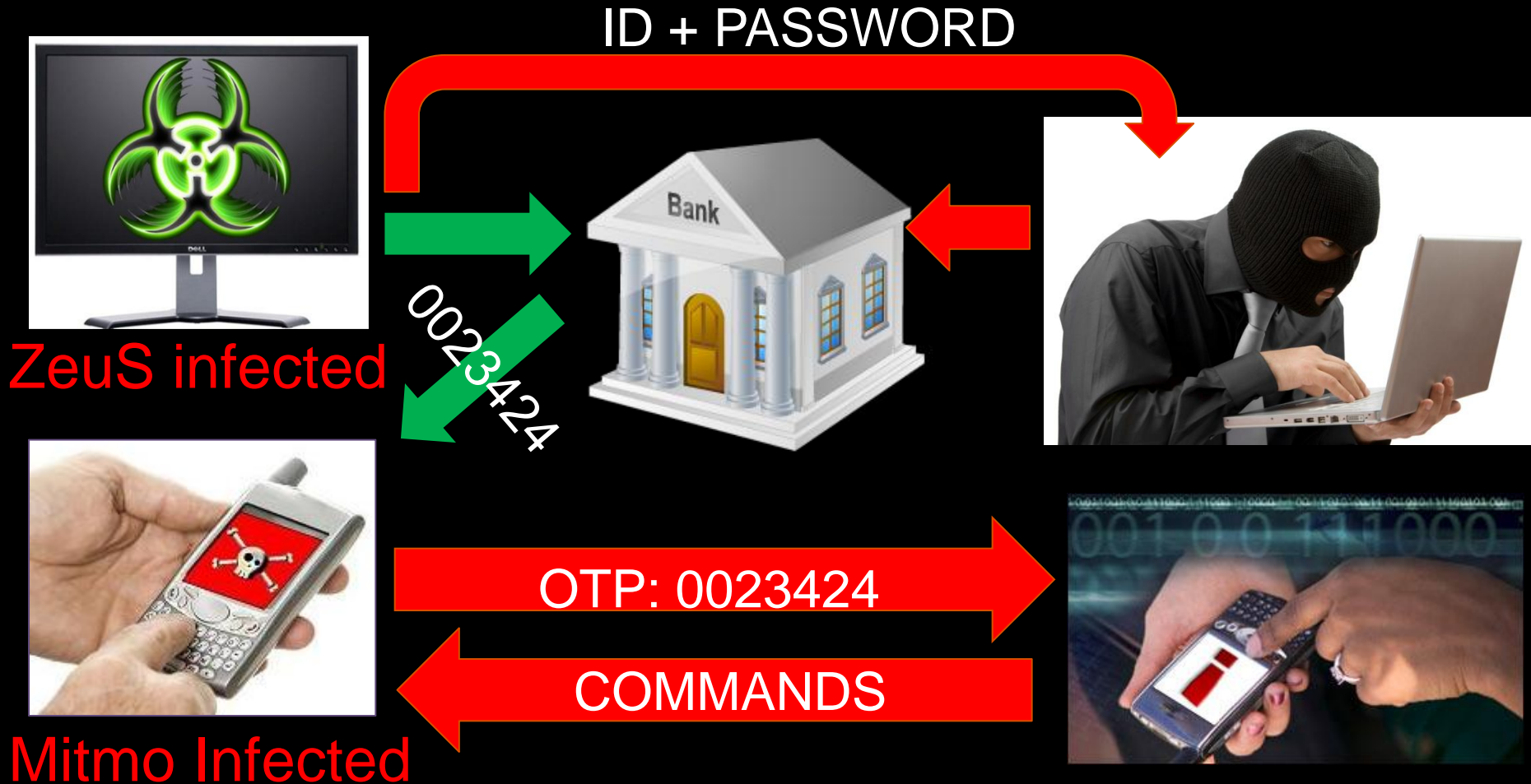


# [ ZeuS Man in the Mobile ]





# [ ZeuS Man in the Mobile ]



# [ ZeuS Man in the Mobile ]

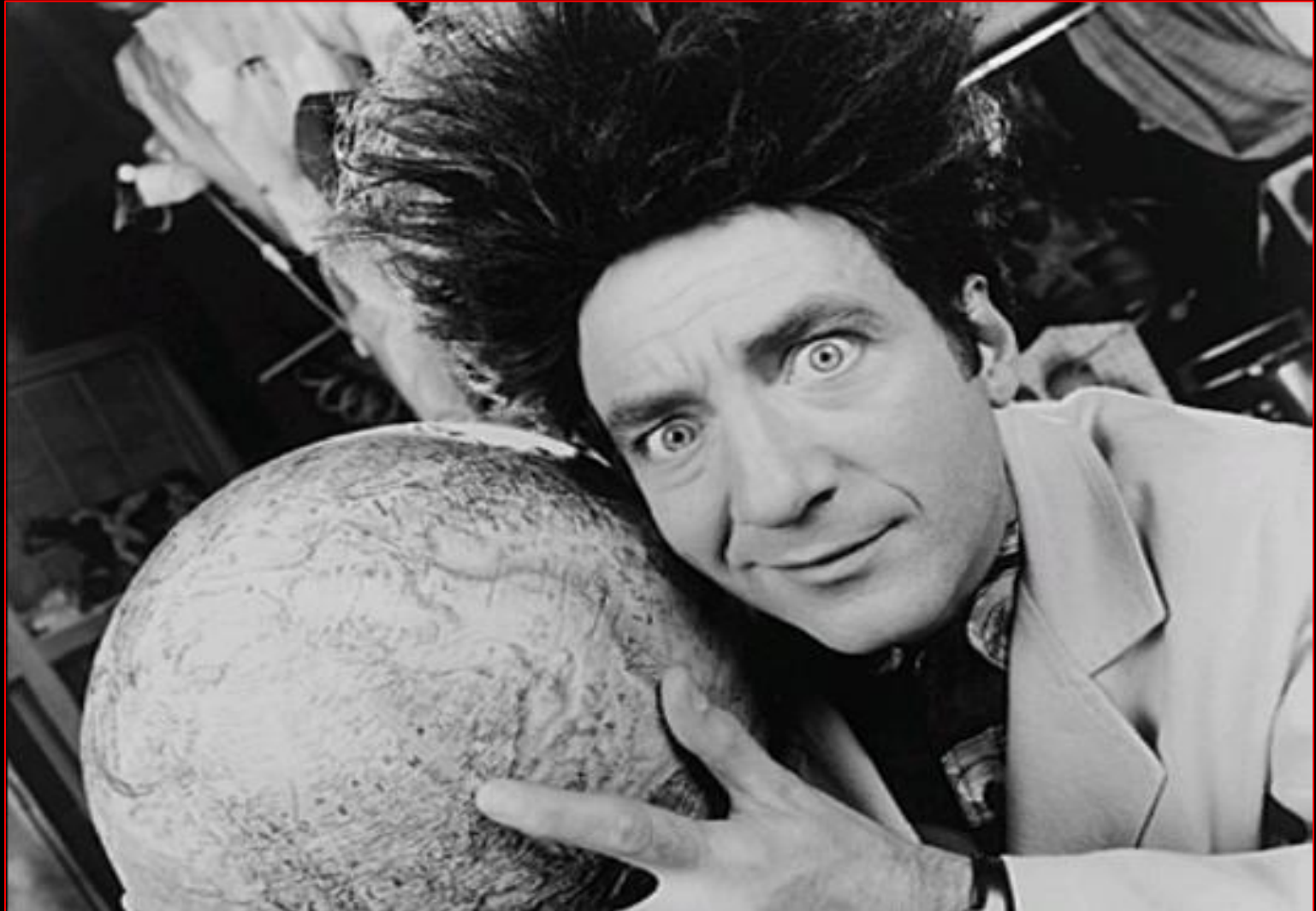


[ DEMO TIME!! ]

# [ Conclusions ]

- Successful attacks: not binary dependent
- Social engineering
  - HTML injections + extras
    - Innovation
    - Underground market
  - User dependent
- Monitoring injections
- Sharing information

[ Questions? ]



# [ Thank You!! ]

Jose Miguel Esparza

jesparza s21sec.com

@eternaltodo

