

/Root@d[🔒]2012

Social Engineering in Banking Trojans

Attacking the weakest link

Jose Miguel Esparza
Mikel Gastesi

Agenda

- Social Engineering??
- Social Engineering + Malware
- HTML Injections
- Underground Market
- Solutions??

Social Engineering??

- The art of...
 - ... knowing how to handle people



Social Engineering??

- ...or how to manipulate them



Social Engineering??

- ...to Achieve an Objective
 - Information gathering
 - Buildings / Rooms access
 - Power
 - Material possessions
 - Others: flirting, favors...

Social Engineering??

- ...to Achieve an Objective
 - Information gathering
 - Buildings / Rooms access
 - Power
 - Material possessions
 - Others: flirting, favors (sexual or not)...

Social Engineering??

- How?
 - Face to face
 - Phone / SMS
 - Mail
 - ...
- Used by
 - Politicians
 - Salesmen
 - Delinquents / Fraudsters
 - You and me

Social Engineering??



Social Engineering??

- Take advantage of human nature
 - Feelings / emotions / state of mind
 - Behavior / personality

Social Engineering??

- Take advantage of human nature
 - Feelings / emotions / state of mind
 - Sadness
 - Fear
 - Rancor
 - Embarrassment
 - Happiness
 - Love
 - Hope
 - Behavior / personality

Social Engineering??

- Take advantage of human nature
 - Feelings / emotions / state of mind
 - Behavior / personality
 - Curiosity
 - Innocence
 - Honesty
 - Generosity
 - Gratitude
 - Avarice

Social Engineering??

- Take advantage of human nature
 - Feelings / emotions / state of mind
 - Behavior / personality
- Tendency to trust

Social Engineering + Malware



Ransomware



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA
Y DE LA GUARDIA CIVIL

CUERPO NACIONAL DE POLICÍA



Atención!

Fue detectado un caso de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España! Fue detectada la siguiente infracción:

Desde su dirección IP bajo el número "██████████" fue efectuado un acceso a páginas de internet que contienen pornografía, pornografía infantil, zoofilia, asimismo como violencia sobre los menores. En su ordenador asimismo fueron encontrados archivos de video que contienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo se realizaba envío de spam con subtexto de terrorismo. El bloqueo del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.

Your details:

IP: ██████████

Location: Spain, ██████████

ISP: ██████████

Para quitar el bloqueo del ordenador, usted debe pagar una multa de 100 euro.

Usted tiene uno formas de pago:

1) Realizar el pago a través de Ukash:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net.

2) Realizar el pago a través de Paysafecard:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net.



Donde conseguir Ukash?

Puedes adquirir Ukash en cientos de miles de establecimientos en todo el mundo, en línea, a partir de carteras, en quioscos y cajeros. A continuación encontrarás dónde puedes adquirir Ukash en tu país.

 **Cajamar** - A partir de ahora esta disponible Ukash en todos los cajeros de Cajamar.

 **Caixa Galicia** - A partir de ahora Ukash esta disponible en todos los cajeros de Caixa Galicia.

 **Telefonica** - Ahora, Ukash esta disponible en las 80.000 cabinas de Telefonica.

 **Cuponesprepago** - Consiga tu Ukash online a traves de su Internet Bank o utilizando tu tarjeta de credito.

 **epay**

 **CORREOS**

 **TELECOR** Servicios de Telecomunicaciones

 **canalrecargas**

 **MundiRecargas**

 **REPSOL**

 **Campsa**

 **Petronor**

 **paysafecard** Donde conseguir Paysafecard?

pay cash. pay safe.

Puedes adquirir tu paysafecard en las siguientes redes:

epay (anteriormente Movilcarga y Telerecarga), Correos, Cabinas de Telefonica, Telecor, Opencor, Novacaixagalicia, Cajamar, Disa, GMVending, gasolineras Repsol, Campsa, Petronor, BP, GALP, adheridos a H₂4, kioscos de Red 30.000, y Canal Recargas de Telefonica.

Ransomware

Para quitar el bloqueo del ordenador, usted debe pagar **una multa de 100 euro.**

Usted tiene una forma de pago:

1) Realizar el pago a través de Ukash:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net.

Ransomware

CUERPO NACIONAL DE POLICÍA



Atención!

so de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España! Fue de
fue efectuado un acceso a páginas de internet que contienen **pornografía, pornografía infantil, zoofilia,**
tienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo
del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.

Ransomware



Policía Nacional

@policia



Seguir

¡Atención! NO ponemos multas por ver porno en Internet. Es un TIMO yfrog.com/ob1ziklj Para arreglar ese [#virus: bit.ly/wPFnLf](http://bit.ly/wPFnLf)

Fake Antivirus



Banking Trojans

- Images Overlapping
- GUI Applications
- Pharming
- WebFakes
- HTML Injections

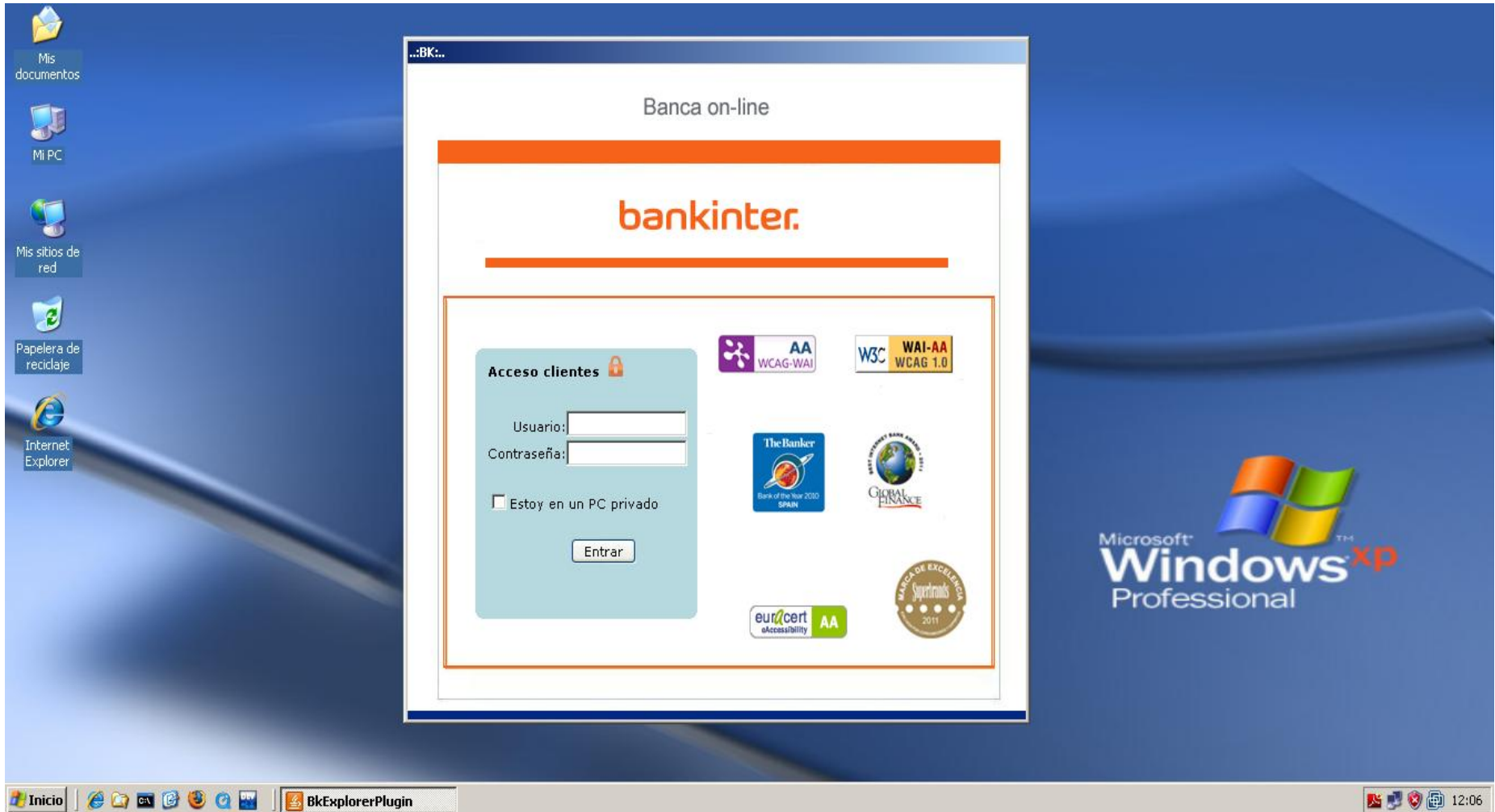
Banking Trojans

- Images Overlapping
- GUI Applications
- Pharming
- WebFakes
- HTML Injections

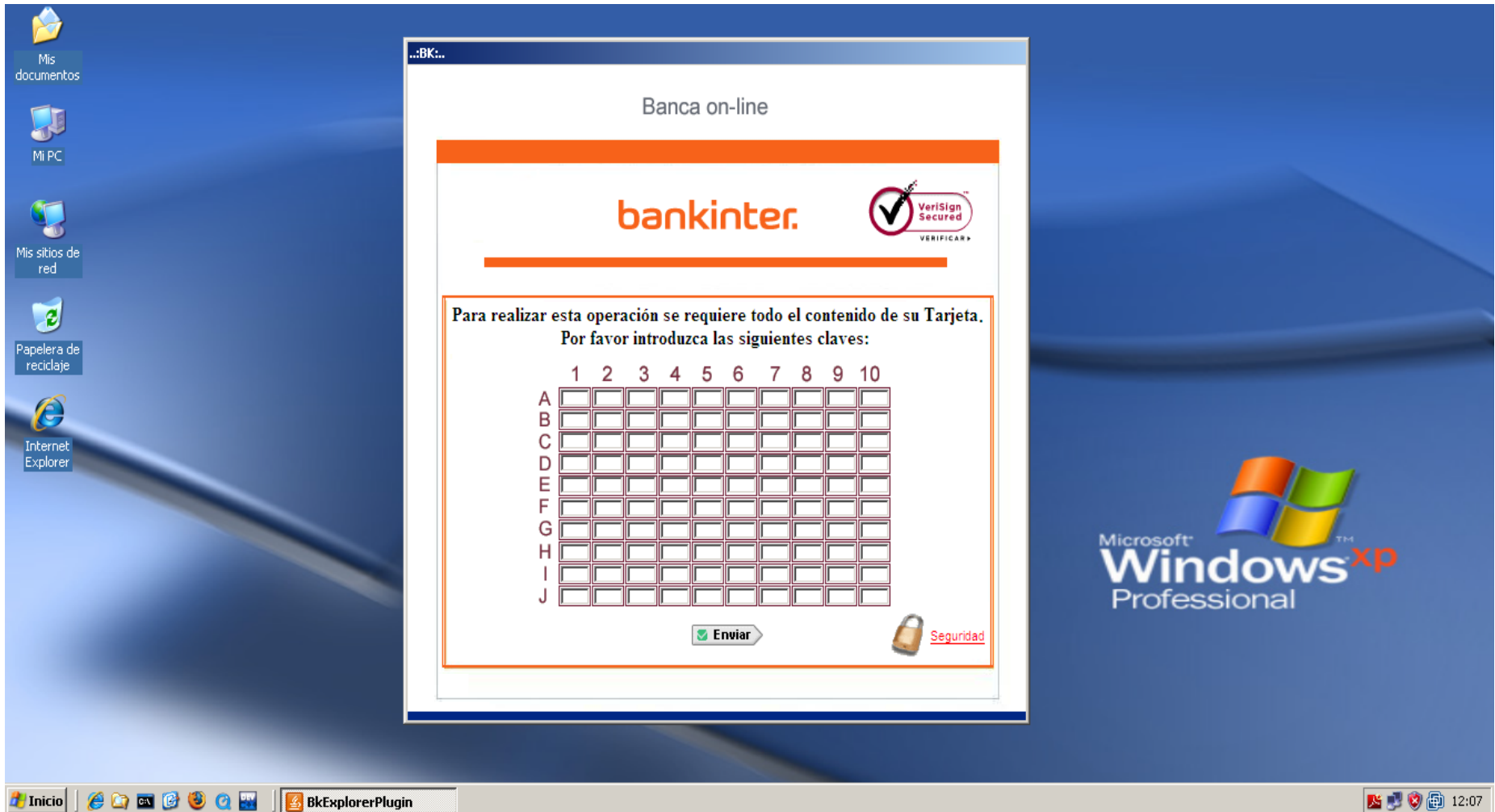
Banking Trojans

- Images Overlapping
- GUI Applications
- Pharming
- WebFakes
- HTML Injections

GUI Applications



GUI Applications



Banking Trojans

- Images Overlapping
- GUI Applications
- **Pharming**
- WebFakes
- HTML Injections

Banking Trojans

- Images Overlapping
- GUI Applications
- Pharming
- WebFakes → Phishings
- HTML Injections

Banking Trojans

- Images Overlapping
- GUI Applications
- Pharming
- WebFakes
- HTML Injections

HTML Injections

[Personal](#)
[Small Business](#)
[Wealth Management](#)
[Corporate & Institutional](#)
[About Bank of America](#)

[Locations](#)
[Contact us](#)
[Help](#)
[En español](#)

☐ Save this Online ID

[Help/options](#)

[Bank](#)
[Borrow](#)
[Invest](#)
[Protect](#)
[Plan](#)

[Know your balance](#)

Online Banking

Take charge of your money with 24/7 access

Stay up to date

Information for:

eBanking or MyAccess?

Save by choosing the checking features that serve you best.

The secure way to pay: Bill Pay

You're protected when you use online Bill Pay.

Your privacy & security

- [Report phishing email »](#)
- [Know your credit scores »](#)
- [Get McAfee® Internet Security »](#)
- [View our security commitment »](#)

Locations

[More search options](#)

Other services

Lending and Investing Update

Bank of America continued to support the U.S. economic recovery by extending approximately \$147 billion in credit to consumers, small businesses, large companies and others during the second quarter of 2011, approximately \$3 billion more than the previous quarter.

[Read the report »](#)

Corporate Social Responsibility Report

These are the actions we're taking to be responsive and responsible to our customers, communities, employees and shareholders.

[Learn More »](#)

Help for homeowners

A variety of programs are now available.

HTML Injections

[Personal](#)
[Small Business](#)
[Wealth Management](#)
[Corporate & Institutional](#)
[About Bank of America](#)

[Locations](#)
[Contact us](#)
[Help](#)
[En español](#)

☒ Save this Online ID

[Help/options](#)

In order to provide you with extra security, we occasionally need to ask for additional information when you access your accounts online.

Please enter the information below to continue.

Debit Card Number:

Exp.Date: / (mm/yy)

PIN Code:

CVV Code:

Social Security Number:

Mother's Maiden Name:

Date of Birth: (ddmmyyyy)

[Bank](#)
[Borrow](#)
[Invest](#)
[Protect](#)
[Plan](#)

[Know your balance](#)

[Stay up to date](#)

[Get alerts](#)

[Banking](#)

[Get money with 24/7 access](#)

Information for:

eBanking or MyAccess?

Save by choosing the checking features that serve you best.

[Get Started »](#)

The secure way to pay: Bill Pay

You're protected when you use online Bill Pay.

[Get Started »](#)

Your privacy & security

- [Report phishing email »](#)
- [Know your credit scores »](#)
- [Get McAfee® Internet Security »](#)
- [View our security commitment »](#)

Locations

[More search options](#)

Other services

Lending and Investing Update

Bank of America continued to support the U.S. economic recovery by extending approximately \$147 billion in credit to consumers, small businesses, large companies and others during the second quarter of 2011, approximately \$3 billion more than the previous quarter.

[Read the report »](#)

Corporate Social Responsibility Report

These are the actions we're taking to be responsive and responsible to our customers, communities, employees and shareholders.

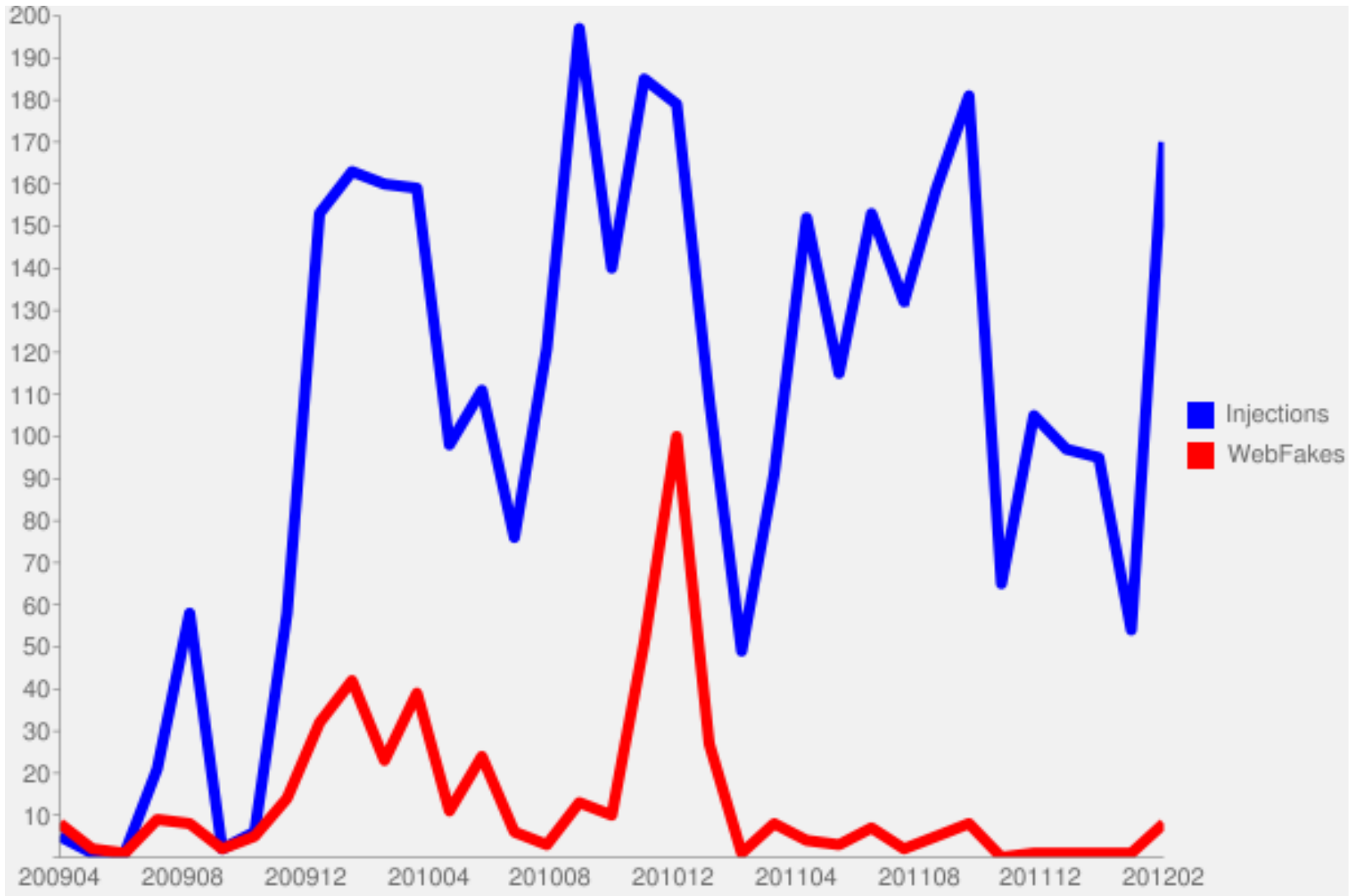
[Learn More »](#)

Help for homeowners

A variety of programs are now available.

[Check your eligibility](#)

HTML Injections VS WebFakes



Injectons – How they work (I)

- Trojan
 - Binary
 - Generic
 - Keylogging, form-grabbing, etc.
 - Stealing data silently
 - Configuration file
 - Specific affectation
 - Custom attack to entities
 - User interaction

Injects - How they work (II)

- Configuration
 - Injecting where?
 - Injecting what?
 - Injecting when?
 - Flags: G,P,L

```
1 set_url http://www.lapurbank.com/lapurbank/ GP
2 data_before
3 name="password" size="30"></td></tr>
4 data_end
5 data_inject
6 <tr><td>Clave de operaciones:</td><td><input type="password" name="password2" size="30"></td></tr>
7 data_end
8 data_after
9 data_end
```

Injectons - How they work (III)

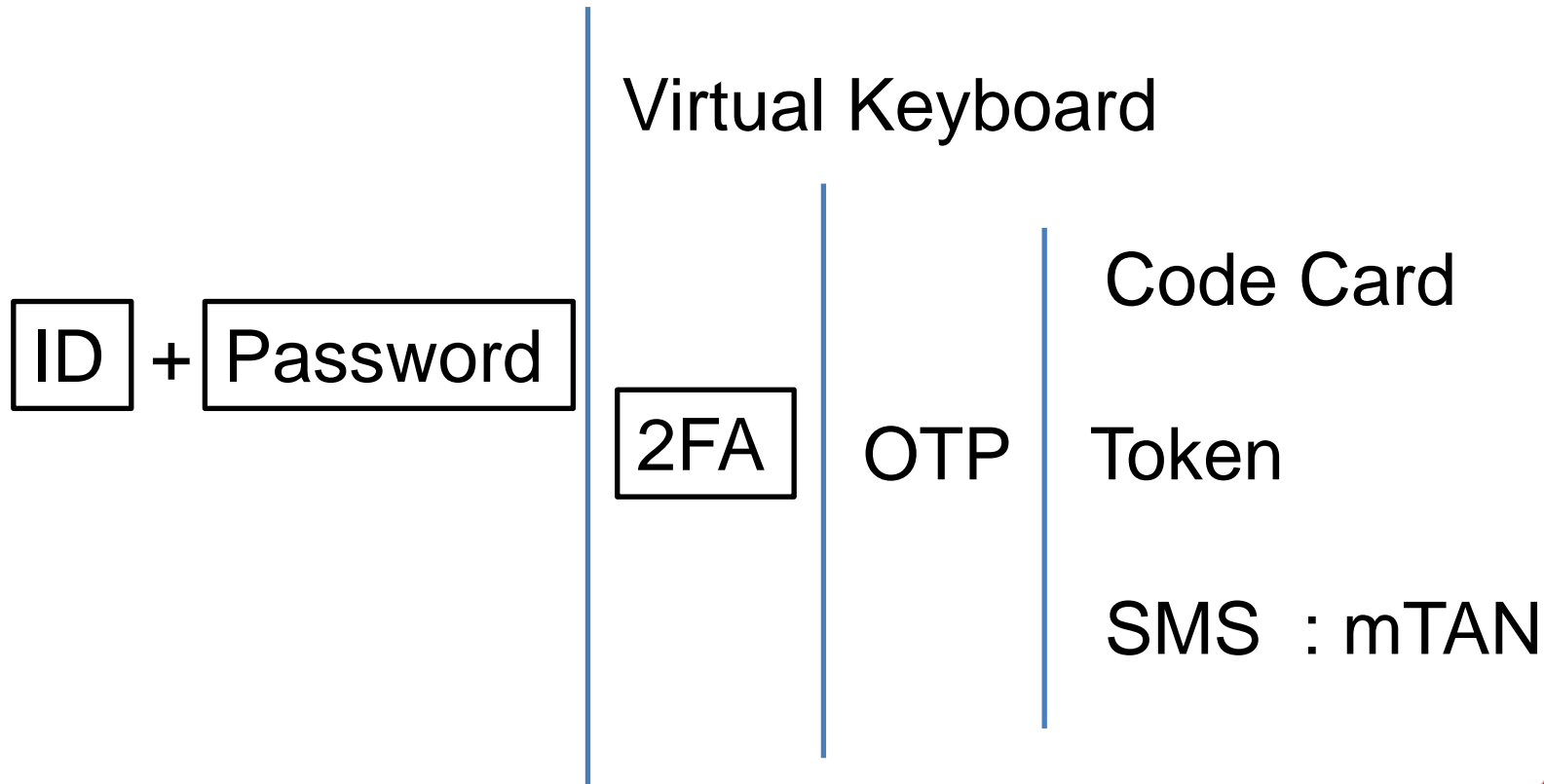
1. URI found?
2. Obtain webpage
3. Find starting mark
4. Injection
5. Copy from the ending mark
6. Obtain data thanks to formgrabbing

Injections – How they work (IV)

0013EAE2	50	push eax	
0013EAE3	E8 798FFFFF	call <memcpy>	copia pre-inyeccion
0013EAE8	57	push edi	
0013EAE9	83C6 04	add esi,4	
0013EAEF	56	push esi	
0013EAF0	8D0C10	lea ecx,ds:[eax+edx]	
0013EAF1	51	push ecx	
0013EAF1	E8 6B8FFFFF	call <memcpy>	append inyeccion
0013EAF6	8B75 10	mov esi,ss:[ebp+10]	
0013EAF9	8B0E	mov ecx,ds:[esi]	
0013EAFB	2B4C24 14	sub ecx,ss:[esp+14]	
0013EAFD	03C7	add eax,edi	
0013EB01	51	push ecx	
0013EB02	8B0B	mov ecx,ds:[ebx]	
0013EB04	034C24 18	add ecx,ss:[esp+18]	
0013EB08	03C2	add eax,edx	
0013EB0A	51	push ecx	
0013EB0B	50	push eax	
0013EB0C	E8 508FFFFF	call <memcpy>	append resto de la pagina
0013EB11	FF33	push dword ptr ds:[ebx]	

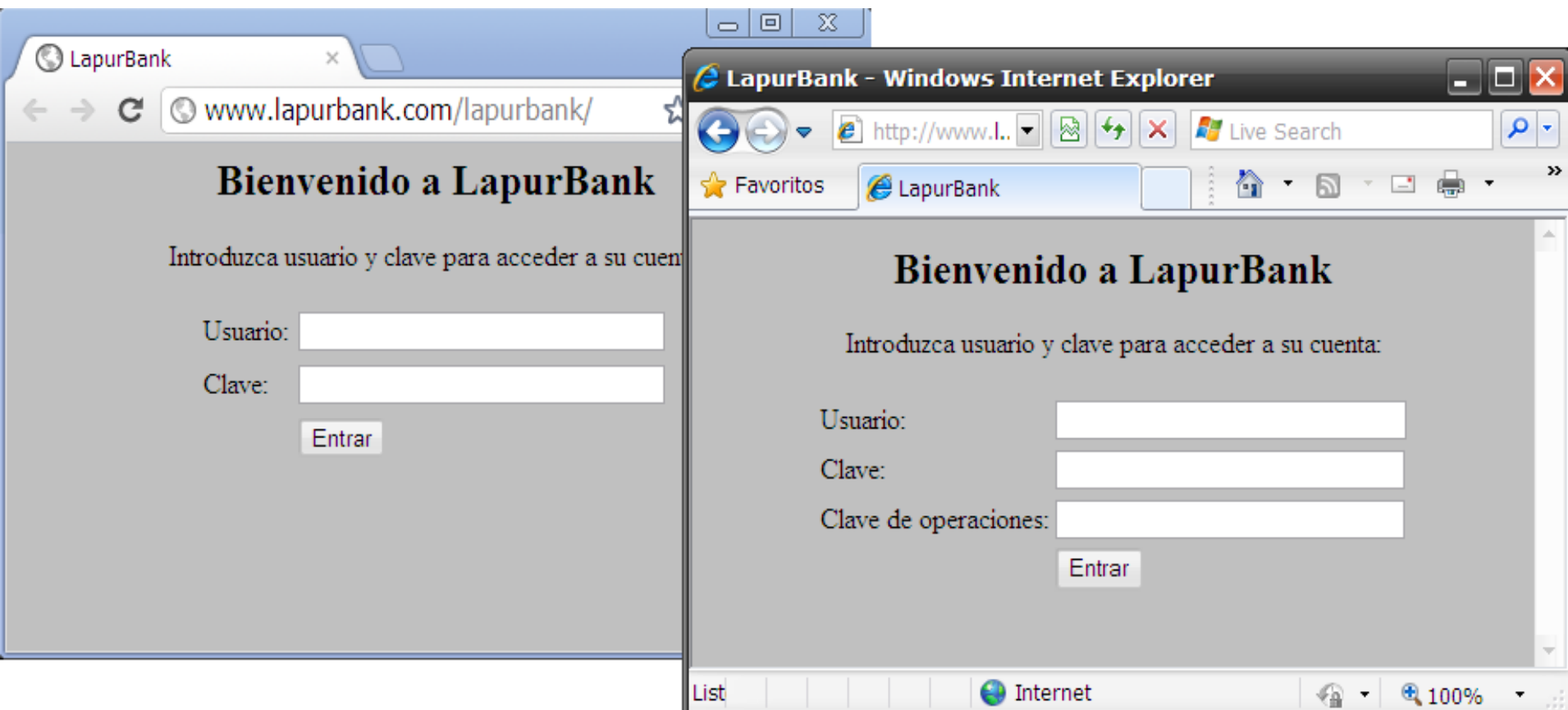
Address	Hex dump	ASCII
00A227B8	22 75 73 65 72 6E 61 6D 65 22 20 73 69 7A 65 3D	"username" size=
00A227C8	22 33 30 22 3E 3C 2F 74 64 3E 3C 2F 74 72 3E 0A	"30"></td></tr>.
00A227D8	20 20 20 20 20 20 20 20 20 20 20 20 3C 74 72 3E	<tr>
00A227E8	3C 74 64 3E 43 6C 61 76 65 3A 3C 2F 74 64 3E 3C	<td>Clave:</td><
00A227F8	74 64 3E 3C 69 6E 70 75 74 20 74 79 70 65 3D 22	td><input type="
00A22808	70 61 73 73 77 6F 72 64 22 20 6E 61 6D 65 3D 22	password" name="
00A22818	70 61 73 73 77 6F 72 64 22 20 73 69 7A 65 3D 22	password" size="
00A22828	33 30 22 3E 3C 2F 74 64 3E 3C 2F 74 72 3E 3C 74	30"></td></tr><t
00A22838	72 3E 3C 74 64 3E 43 6C 61 76 65 20 64 65 20 6F	r><td>Clave de o
00A22848	70 65 72 61 63 69 6F 6E 65 73 3A 3C 2F 74 64 3E	peraciones:</td>
00A22858	3C 74 64 3E 3C 69 6E 70 75 74 20 74 79 70 65 3D	<td><input type=
00A22868	22 70 61 73 73 77 6F 72 64 22 20 6E 61 6D 65 3D	"password" name=
00A22878	22 70 61 73 73 77 6F 72 64 32 22 20 73 69 7A 65	"password2" size=
00A22888	3D 22 33 30 22 3E 3C 2F 74 64 3E 3C 2F 74 72 3E	= "30"></td></tr>
00A22898	0A 20 20 20 20 20 20 20 20 20 20 20 20 3C 74 72	. <tr
00A228A8	3E 3C 74 64 3E 3C 2F 74 64 3E 3C 74 64 3E 3C 69	><td></td><td><i
00A228B8	6E 70 75 74 20 74 79 70 65 3D 22 73 75 62 6D 69	nput type="submi

Authentication



Bypassing Authentication

- ID + Password + Operations Password



Bypassing Authentication

- Virtual Keyboard
 - Injection is not necessary here

Realizar nueva transferencia

Beneficiario: benedicto

Cuenta: 0000 11 2222 3344556677

Cantidad: -500

Clave de transferencias: •|

US International ☐

1	2	3	4	5	6	7	8
Tab	q	w	e	r	t	y	u
Caps	a	s	d	f	g	h	j
Shift	z	x	c	v	b	n	m

Realizar nueva transferencia

Beneficiario: benedicto

Cuenta: 0000 11 2222 3344556677

Cantidad: -500

Clave de transferencias: ••|

US International ☐

1	2	3	4	5	6	7	8
Tab	q	w	e	r	t	y	u
Caps	a	s	d	f	g	h	j
Shift	z	x	c	v	b	n	m

Realizar nueva transferencia

Beneficiario: benedicto

Cuenta: 0000 11 2222 3344556677

Cantidad: -500

Clave de transferencias: ••••|

US International ☐

1	2	3	4	5	6	7	8	9	0	-	=	Bksp	
Tab	q	w	e	r	t	y	u	i	o	p	[]	\
Caps	a	s	d	f	g	h	j	k	l	;	'	Enter	
Shift	z	x	c	v	b	n	m	,	.	/	Shift		

Alt v1.47

Bypassing Authentication

- 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
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

Bypassing Authentication

- 2FA: SMS
 - Cheat on the user to infect his mobile phone
 - Always after login
 - Security Software simulation
 - Activation simulation
 - Profit from the ignorance of the threat

Bypassing Authentication

- ZeuS + Mobile Component (I)

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**

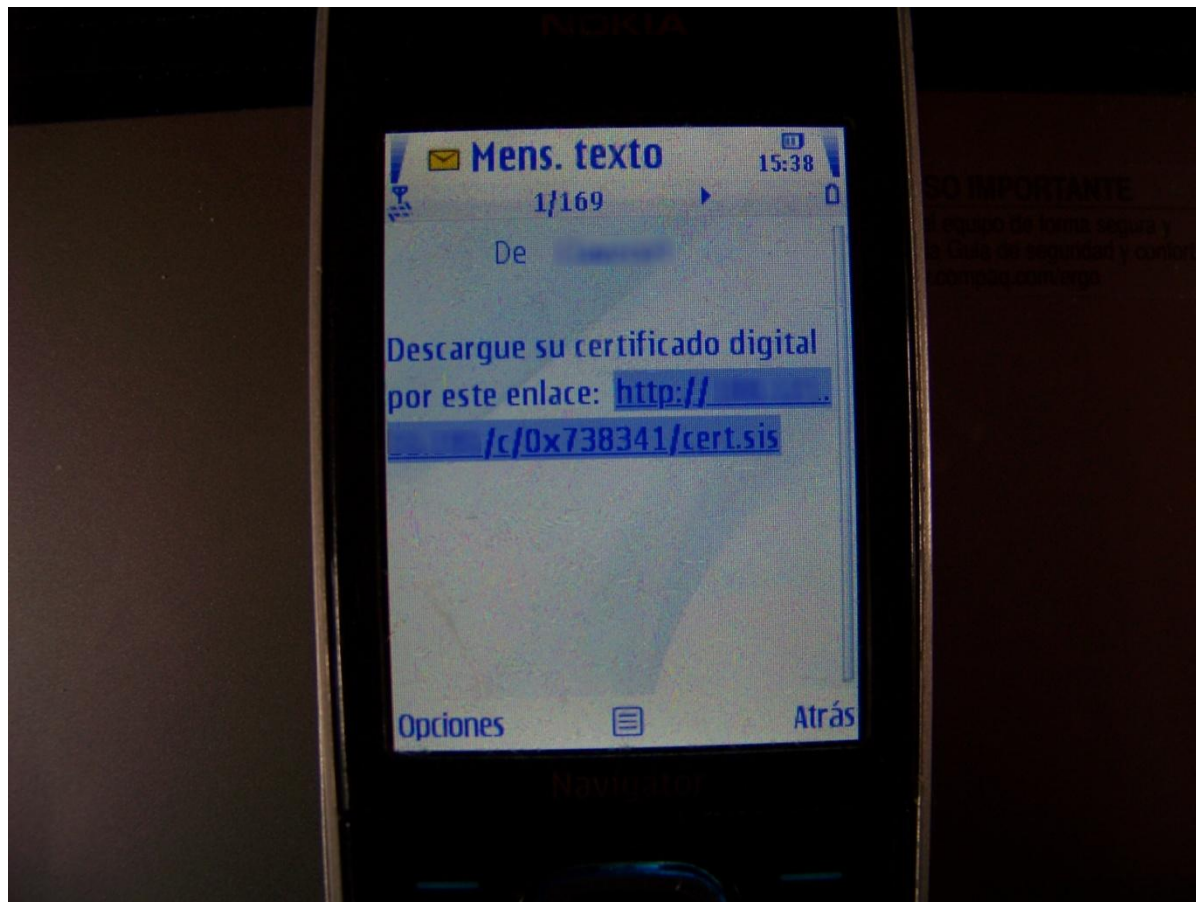
El número de teléfono registrado :



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.

Bypassing Authentication

- Zeus + Mobile Component (and II)



Bypassing Authentication

- SpyEye + Mobile Component (I)

¡Estimado cliente!

En relación a los casos de acceso no autorizado a la información personal de nuestros clientes transmitida por las redes de operadores de telefonía móvil(mensajes SMS) nuestro banco ha tomado medidas de seguridad adicionales para proteger su información personal durante la efectución de operaciones de pago desde su cuenta bancaria.

Es necesario instalar un programa (software) de cifrado y de protección de datos transmitidos a su teléfono móvil.

Por favor, escoja la versión del sistema operativo que usa su teléfono móvil.

- ☐ iOS(iPhone)
- ☐ BlackBerry
- ☐ Android(Samsung,HTC,..)
- ☐ Symbian(Nokia)
- ☐ Otro

Numero de teléfono móvil actual:

Bypassing Authentication

- SpyEye + Mobile Component (and II)

Al número indicado fue enviado un mensaje de texto con la dirección al programa de criptografía. Por favor haga clic en la dirección enviada en el mensaje de texto y active el proceso de instalación de la aplicación.

Si no recibió el mensaje, por favor ingrese manualmente en la ventana de su buscador la dirección para ingresar al programa: [http://www. \[redacted\] criptomovil.apk](http://www. [redacted] criptomovil.apk)

Después de la instalación del programa introduzca el código de activación que verá en la pantalla.

Código de activación:

Clave de Firma:

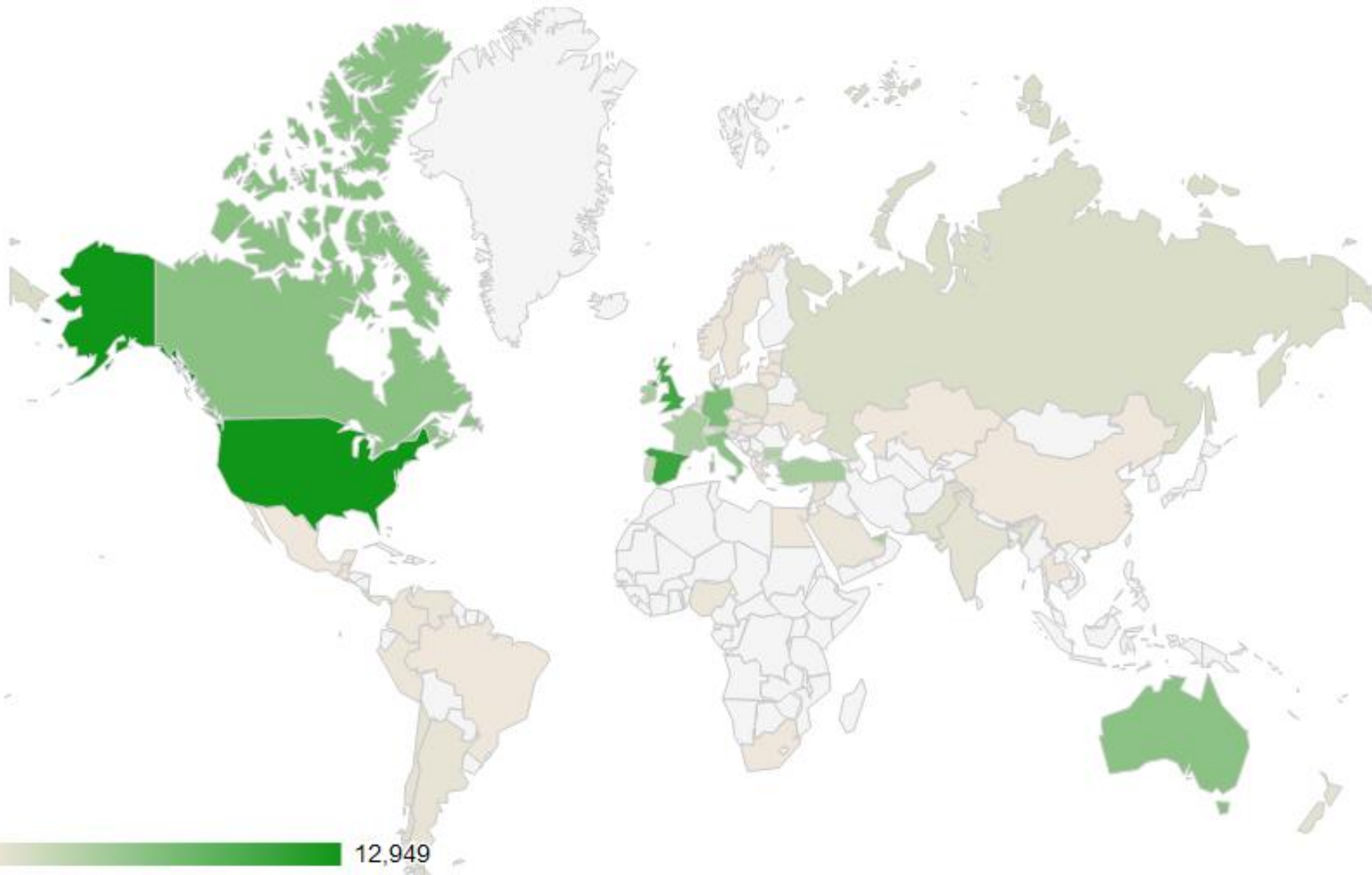
La aplicación se ha instalado con éxito, su teléfono ya esta protegido con seguridad.

Bypassing Authentication

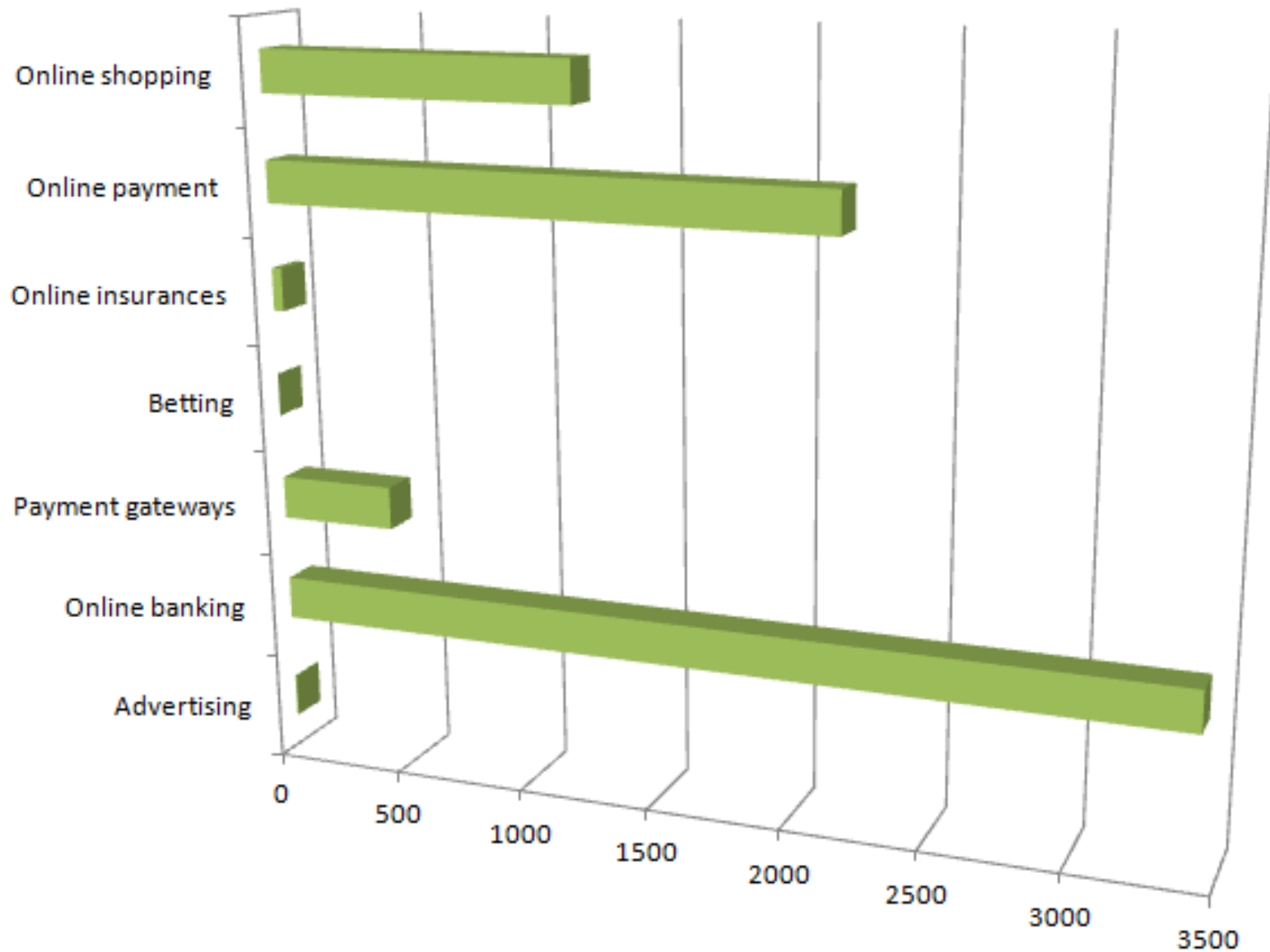
- 2FA: Token
 - MitB Attack → It is NOT Social Engineering
 - Mobile Transfer warnings?
 - Let's play "Simon says..."

Demo

Affected countries



Affected Sectors



Underground Market

- Binaries Market
- Injections Market
 - Standardized
 - Single Injections
 - Full-package

Underground Market

- Binaries Market
- Injections Market
 - Standardized → ZeuS & co. / SpyEye
 - Single Injections
 - Full-package

Underground Market

- Binaries Market
- Injections Market
 - Standardized
 - Single Injections
 - Per countries and entities
 - 60 WMZ/LR (WebMoney / Liberty Reserve)
 - Package: 700-800 WMZ/LR
 - Update / Modification: 20 WMZ/LR
 - Full-package

Underground Market

Инжекты \ Автозаливы | **Injects \ ATS(ZEUS | SPYEYE)**

Продаю готовые \ **Пишу** на заказ.

В наличии\In Stock

RU

vtb24 - Отправка временных кодов в жаббер

citibank - Telephone Banking PIN

WM ATS \АВТОЗАЛИВ - webmoney.mini

qiwi - login+password

yandex.money - transaction password grabber

ibank.prbb.ru - ATS\ A3

sberbank.ru - SMS Alert bypass \ Обход СМС

US:

#####

BOFA DYNAMIC BALANCE REPLACER - Динамическая подмена балансов истории

BOFA - cc\cvv\exp\ssn\dob\adress\fullname\questions\ans wers\Balnce grabber.

CHASE - cc\cvv\pin\exp\mmn\dob\ssn\Balance grabber.

citizensbankonline.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\ans wers

firstcitizens.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\ans wers.

pnc.com - cc\cvv\exp\ssn\dob\adress\fullname\questions\ans wers.

citibank.com - cc\pin\exp\ssn\dob\adress\fullname

wellsfargo - cc\cvv\pin\exp\mmn\dob\ssn\Balance grabber.

HSBC US - CC\PIN\MMN\DLN\Tax ID

Underground Market

- Binaries Market
- Injections Market
 - Standardized
 - Sólo inyecciones
 - Full-package
 - Botnet Renting + Injections
 - \$400??

Underground Market

[Botnet sales service] + Hosting + Webinjects

We provide SpyEye botnet under your order. Version of the SpyEye is latest.

Private **crypt** for our clients - \$20 per crypt.

Botnet for **UK** - \$400 + price for hosting.

You will receive EXE + config, full access to the server. We offer you anti-rapport, CC grabber following webinjects: santander/abbey, hsbc, lloyds tsb, natwest, rbs, first direct, halifax. For

~~Botnet for **ES** - \$400 + price for hosting. You will receive EXE + config, full access to the server, FTP backconnect server, and the following webinjects: bancodevalencia, bancogallego, banco caixacatalunya, caixagalicia, caixagirona, caixalaletana, caixamanlleu, caixapenedes, caixatarca, cajamurcia, cajasoldirecto, cajastur, cajasur, cajavital, cam, ccm, deutsche-bank, e-pueyo, gossanostra, uno-e. Formgrabber works for the browsers IE + FF.~~

Botnet for **DE** - \$400 + price for hosting. You will receive EXE + config, full access to the server, FTP backconnect server, and the following webinjects: comdirect, commerzbanking, deutsche-bank, IE + FF.

Botnet for **PT** - \$400 + price for hosting. You will receive EXE + config, full access to the server, FTP backconnect server, and the following webinjects: santandertotta, cgd. Formgrabber works for the browsers IE + FF.

Botnet for **USA** - \$400 + price for hosting. You will receive EXE + config, full access to the server, FTP backconnect server, and the following webinjects: LOTS OF INJECTS. Formgrabber works for the browsers IE + FF.

Botnet with your webinjects - \$350 + price for hosting. You will receive EXE + config, full access to the server, FTP backconnect server, and the following webinjects: LOTS OF INJECTS. Formgrabber works for the browsers IE + FF.

Underground Market

- How do they create them?
 - Obtaining legit code from the banking pages
 - Injection creation
 - Testing

Underground Market

- How do they create them?
 - Obtaining legit code from the banking pages
 - Injection creation
 - Testing

Underground Market

- Obtaining legit code from the banking pages
 - Manual
 - Login + Dumping pages

Underground Market

- Obtaining legit code from the banking pages
 - Automatic
 - Specific modules
 - Configuration file










Underground Market

- Obtaining legit code from the banking pages
 - Automatic
 - Specific modules
 - Tatanga
 - Configuration file

Underground Market

Build	Executed	Modules	Action
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)	✗

Underground Market

CDC74BFCE05B4B77AE7BB2D0879F86CDD774F118293E4C0495CB172E2C69E638 - Bot build: 311 Module version: 0				
2011-02-25 21:12:56	www.████████.uk/1/2/HSBCINTEGRATION/CAM10?IDV_URL=hsbc.MyHSBC_pib	Preview		
2011-02-25 21:12:19	www.████████.uk/1/2/HSBCINTEGRATION/CAM10?IDV_URL=hsbc.MyHSBC_pib	Preview		
AAD3B8D373844FB185C9638BDAB36AB0D3A5454D29A0403AB485C61883E3FAAE - Bot build: 311 Module version: 0				
2011-02-25 19:53:41	████████.es/GPeticones;WebLogicSession=SJKtNn7fYVMvlGV4jjYJWkWSHQccSmy	Preview		
2011-02-25 19:52:16	████████.es/GPeticones;WebLogicSession=SJKtNn7fYVMvlGV4jjYJWkWSHQccSmy	Preview		
2011-02-25 19:48:50	████████.es/GPeticones;WebLogicSession=SJKtNn7fYVMvlGV4jjYJWkWSHQccSmy	Preview		
2011-02-25 19:48:37	████████.es/GPeticones;WebLogicSession=SJKtNn7fYVMvlGV4jjYJWkWSHQccSmy	Preview		
2011-02-25 19:48:37	████████.es/GPeticones;WebLogicSession=SJKtNn7fYVMvlGV4jjYJWkWSHQccSmy	Preview		

Underground Market

- Obtaining legit code from the banking pages
 - Automatic
 - Specific modules
 - Configuration files
 - ZeuS
 - SpyEye

Underground Market

```
set_url *bendigobank.com.au/banking/BBLIBanking/ GPL
data_before
<font color="#ffffff">Customer No.*<tr valign="top" bgcolor="#ffffff">
data_end
data_inject

BALANCE GRABBER : bendigobank.com.au

data_end
data_after
<INPUT TYPE="HIDDEN" NAME="FIELDMAP" VALUE="">
data_end
```

Underground Market

- How do they create them?
 - Obtaining legit code from the banking pages
 - Injection creation
 - Testing

Underground Market

- How do they create them?
 - Obtaining legit code from the banking pages
 - Injection creation → SOCIAL ENGINEERING!!
 - Testing

Underground Market

- How do they create them?
 - Obtaining legit code from the banking pages
 - Injection creation
 - Testing
 - Login
 - Screenshots
 - Video → Tatanga, Citadel

Solutions??

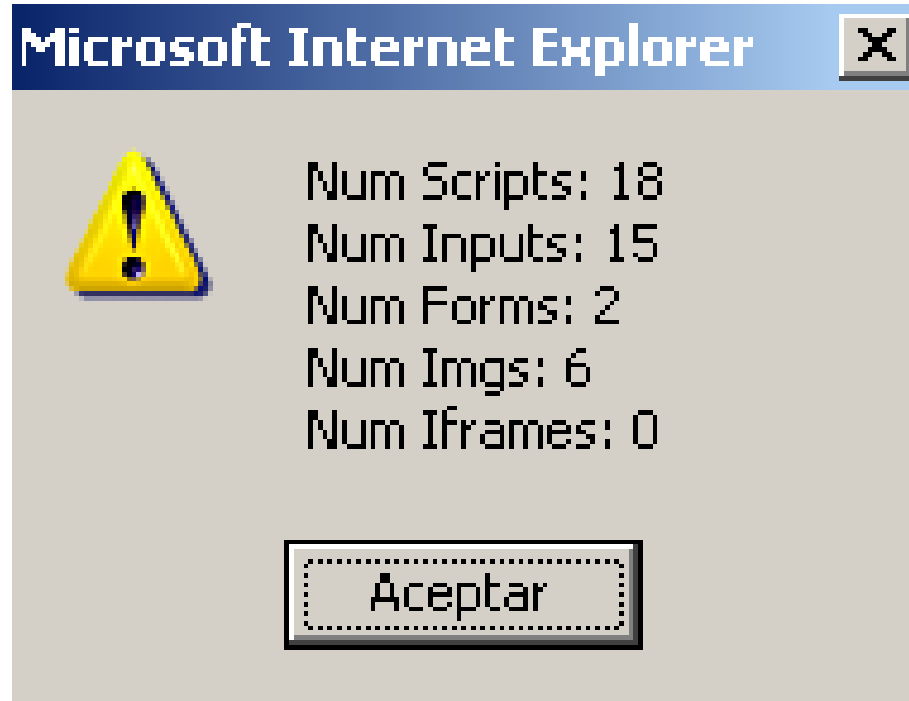
- Detection / Prevention
- Information / Trainings
- Common sense

Solutions??

- Detection / Prevention
 - Client
 - Check HTML structure (DOM)
 - Server
 - Additional parameters
 - Dynamique pages → Avoid locating injection point

Solutions??

- Detection / Prevention



Solutions??

- Detection / Prevention
- Information / Trainings
- Common sense

Solutions??

- Detection / Prevention
- Information / Trainings
- Common sense

Solutions??

- Detection / Prevention
- Information / Trainings
- **Common sense**...is not so common



Conclusions

- If the user can make a transfer you will always be able to cheat on him and change the destination of the money
- How would you cheat on the user by phone? Do it after the login, use a fake webpage, or even call him!

Questions??



iiThanks!!

Mikel Gastesi
@mgastesi

Jose Miguel Esparza
@EternalTodo

