

## Nuevo troyano bancario dirigido a entidades españolas y latinas

*Combina la captura del teclado físico con una técnica optimizada para los teclados virtuales.*

*El troyano realiza una serie de pequeñas capturas de pantalla, alrededor del cursor, cada vez que el usuario pincha con el ratón en una tecla virtual. Además marca con una señal roja el punto exacto donde el usuario pinchó, de forma que el atacante puede observar con claridad que tecla fue seleccionada.*

*Está específicamente diseñado contra diversas entidades financieras de Argentina, Bolivia, Brasil, Cabo Verde, España, Estados Unidos, Paraguay, Portugal, Uruguay y Venezuela.*

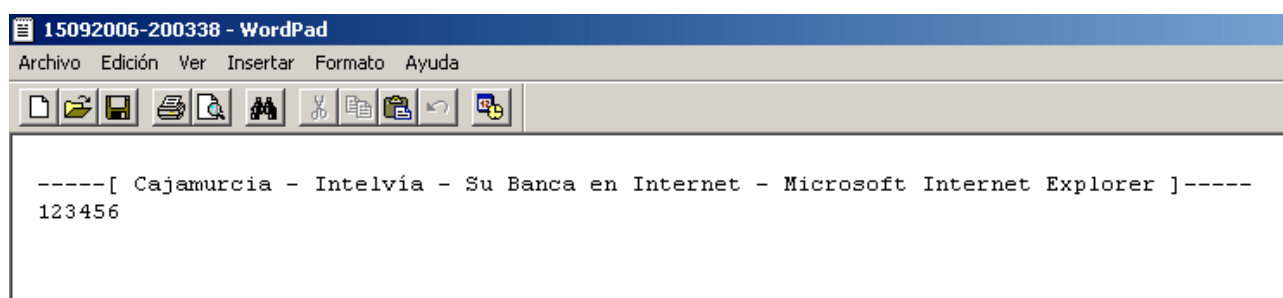
### Introducción

Como ya hemos comentado en análisis anteriores, cada vez son más los sitios webs, especialmente de entidades financieras, que implantan teclados virtuales en un intento de eludir la captura de contraseñas por parte de los troyanos tipo keyloggers ([http://www.hispasec.com/laboratorio/troyano\\_bancario\\_captura\\_video.pdf](http://www.hispasec.com/laboratorio/troyano_bancario_captura_video.pdf)).

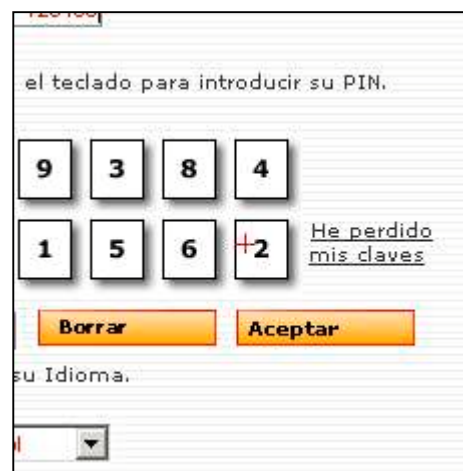
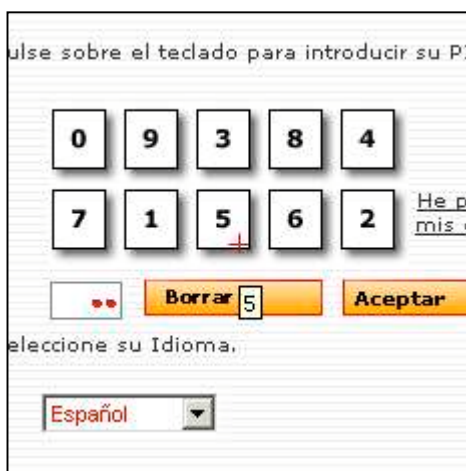
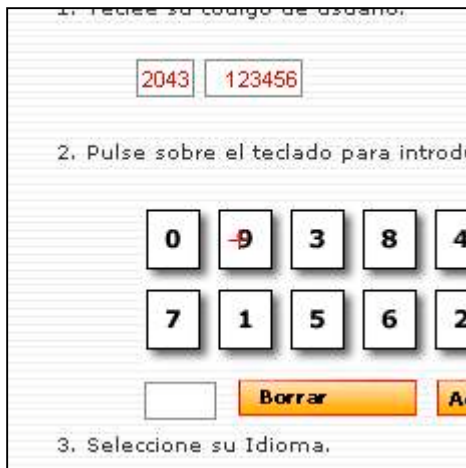
En esta ocasión vamos a analizar un nuevo troyano en activo que combina con efectividad la técnica de keylogger, o captura del teclado físico, con otra técnica especialmente diseñada para la captura de datos introducidos a través de los teclados virtuales. Esta combinación le permite atacar a una gran variedad de páginas de autenticación y acceso a la banca electrónica, de manera independiente a si utilizan o no teclados virtuales.

El método que utiliza contra los teclados virtuales consiste en realizar una pequeña captura de un área de pantalla, alrededor del cursor del ratón, en el momento que el usuario hace click en la tecla virtual. Adicionalmente, y para que el atacante no tenga la menor duda, el troyano incluye en la imagen capturada una señal en color rojo que indica el punto exacto donde el usuario pinchó con el ratón.

Aquí podemos apreciar el log del keylogger y la secuencia de imágenes que captura el troyano en un caso concreto:



Detalle del log del keylogger donde ha capturado el código de usuario (123456) introducido por el usuario a través del teclado físico.



Detalle de las 4 imágenes JPG que recibe el atacante donde puede apreciar las teclas pulsadas por el usuario en el teclado virtual para introducir su PIN. Obsérvese como en cada imagen aparece marcada una tecla por una cruz roja. Siguiendo la secuencia de las imágenes, de izquierda a derecha, el PIN introducido por el usuario es 9452.

A diferencia de otras técnicas, como la del vídeo, este método permite optimizar tanto los recursos consumidos por el troyano en el sistema como el ancho de banda que requiere enviar este tipo de datos gráficos. Mientras que en el caso del vídeo los archivos a enviar al atacante podían ser de varios cientos de KB (lo que a día de hoy tampoco supone mayor problema por la implantación de la banda ancha), este nuevo troyano envía unos archivos JPG de apenas 10 KB.

Para que pueda apreciarse mejor como trabaja el troyano, en el laboratorio de Hispasec hemos preparado unos vídeos/flash que recogen la actividad real del troyano en algunos casos concretos:

Caso Banesto, donde no existe teclado virtual en la autenticación de acceso a la banca:  
[http://www.hispasec.com/laboratorio/troyano\\_captura\\_banesto.htm](http://www.hispasec.com/laboratorio/troyano_captura_banesto.htm)

Caso CajaMurcia, donde si existe teclado virtual:  
[http://www.hispasec.com/laboratorio/troyano\\_captura\\_cajamurcia.htm](http://www.hispasec.com/laboratorio/troyano_captura_cajamurcia.htm)

## Análisis técnico

Dentro del análisis de este tipo de trojanos hay 4 preguntas fundamentales que deben quedar resueltas.

- ¿Qué entidades monitoriza?
- ¿Cómo las monitoriza?
- ¿Qué información obtiene?
- ¿Cómo envía esa información al autor del malware?

Contestando estas preguntas adecuadamente tendremos una idea específica de la peligrosidad del trojano bancario. Veámoslo en la práctica.

### ¿Qué entidades monitoriza?

Un análisis a simple vista de las cadenas contenidas dentro del ejecutable, una vez desempaquetado y reconstruido adecuadamente, no muestra ninguna que se pueda considerar significativa o típica.

Sin embargo, observando más exhaustivamente nos encontramos con cadenas un tanto "extrañas", tipo:

```
'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
```

Obviamente, las cadenas están cifradas de alguna manera, con el fin de evitar posibles análisis heurísticos de los antivirus.

La cadena resaltada en rojo nos da la clave para resolver el problema. Como podemos ver, pese a que la cadena no tiene sentido, la estructura del primer grupo de caracteres ("jjj.oox.rf") nos recuerda inmediatamente a una sintaxis de una URL o dirección web: **www.aaa.bb**

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

### Realizando un pequeño criptoanálisis de la cadena

En primer lugar vemos que la longitud de la cadena original respecto a la cifrada no varía. Además, caracteres no propios del alfabeto, como "/" o "." aparecen sin cifrar. De esta manera llegamos a la conclusión que el cifrado usado está basado en alfabetos.

El más antiguo y sencillo método de cifrado de este tipo es el llamado "Cesar", debido a que fue el propio emperador el primero en ponerlo en práctica. Éste método se basa en la correspondencia entre una letra con otra del mismo alfabeto, pero desplazada  $n$  veces.

Fijándonos en nuestra cadena cifrada "jjj.oox.rf", vamos a calcular el desplazamiento.

**jjj** debería corresponder a **www**

j='6A' (Código Hexadecimal del Ascii correspondiente)  
w='77' (Código Hexadecimal del Ascii correspondiente)

77h-6Ah= 0Dh = 13 decimal

Nos encontramos ante una variación estándar y muy usada del cifrado Cesar: **rot13**.

Este método usa un desplazamiento de 13 posiciones para el alfabeto, el mismo código puede ser usado tanto para cifrar, como para descifrar.

Nuestra misteriosa cadena, una vez descifrada quedaría de esta manera:

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

Operando de la misma manera para las otras cadenas cifradas obtenemos que monitoriza los siguientes sitios webs:

Aviso: Las entradas que aparecen con asteriscos (\*\*\*\*\*) corresponden a entidades que, previamente a la publicación del informe, solicitaron no se hicieran públicos sus casos concretos.

#### 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))

## BRASIL

- 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))

## CABO VERDE

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

## ESPAÑA

- 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))
- 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.bancogui.es](http://www.bancogui.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))
- \*\*\*\*\* ([\\*\\*\\*\\*\\*](http://*****))
- Caja Castilla La Mancha ([www.ccm.es](http://www.ccm.es))
- Caja de Extremadura ([www.cajaextremadura.es](http://www.cajaextremadura.es))
- \*\*\*\*\* ([\\*\\*\\*\\*\\*](http://*****))
- 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))

## ESTADOS UNIDOS

- 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))

## ¿Cómo las monitoriza?

El troyano se vale de la API FindWindowA. Ésta toma como uno de los parámetros el título de la ventana a encontrar. De esta manera, cuando el usuario esté visitando, por ejemplo, la página del bbk, el título de la ventana del Internet Explorer tendrá el siguiente aspecto:

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

Nos suena, ¿verdad?

Otros casos:

**Cajamurcia online - Microsoft Internet Explorer**

**Caixa de Girona - Microsoft Internet Explorer**

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

En algunos casos también contempla la posibilidad de que el usuario utilice otro navegador, en concreto Firefox. Por ejemplo:

**Internet Banking CAIXA - Microsoft Internet Explorer**  
**Internet Banking CAIXA - Mozilla Firefox**

Así es como lo implementa el troyano:

```
mov     esi, esp
lea     eax, [ebp+WindowName] ; array con los títulos de entidades que monitoriza
push   eax                    ; lpWindowName
push   0                     ; lpClassName
call   FindWindowA
```

### ¿Qué información obtiene?

El troyano empieza a realizar capturas de un área determinada en torno al puntero del ratón, siempre y cuando detecte que el usuario haya visitado una de las páginas que monitoriza. Estas capturas se guardan en formato JPG en el directorio C:\WINDOWS\SYSTEM\systray\

El nombre de las imágenes, lo genera según la fecha del sistema, con el formato: *díamesaño-horamínutossegundos.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      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
```

En el caso de que ese directorio no exista, el troyano falla en sus capturas.

Así mismo, también tiene capacidad de keylogger y extrae certificados y claves de seguridad. Todo ello lo guarda en el mismo directorio.

Este código es parte de la rutina del keylogger, el cual activa mediante un hook al sistema.

```
.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

```

## ¿Cómo envía esa información al autor del malware?

El troyano envía todos los ficheros contenidos en el directorio anterior, mediante ftp.

```

.text:00416F9B      call   InternetConnectA ; Abre una conexión
.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      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

```

Lo que hace es acceder a un servidor ftp en un ordenador con IP de Brasil, direccionado por un DNS dinámico, gratuito y relativamente anónimo a través del servicio [www.no-ip.com](http://www.no-ip.com).

Una vez dentro crea un directorio dentro del directorio "/REINADO\_LUCIFER/" con el nombre del ordenador, y procede a depositar allí todos los ficheros capturados en los sistemas infectados.

## Curiosidades y Conclusiones

Entre los títulos que monitoriza se encuentra uno que deliberadamente no hemos puesto en el listado de entidades afectadas, ya que a día de hoy no sería funcional. En concreto se trata de la cadena:

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

Como se puede apreciar aparece una errata en el nombre, al incluir dos "i" en vez de una que sería lo correcto: "ebankinter". Caben varias interpretaciones:

- que efectivamente se trate de una errata del atacante al introducir el nombre
- que se haya confundido con un ataque phishing que fue realizado en septiembre de 2005 bajo el dominio de ebankiinter.com (con dos "i")
- que deliberadamente hubiera incluido esa cadena para interceptar los datos que los usuarios pudieran introducir en las páginas de phishing. Posibilidad esta última bastante remota, o al menos equivocada por parte del atacante, ya que esa web no se encuentra disponible.

El troyano no incluye técnicas rootkits para ocultarse en el sistema, usando el nombre systray.com con el fin de intentar pasar desapercibido entre los ejecutables y procesos.

El método utilizado por este troyano para capturar los datos introducidos en teclados virtuales es claramente más óptimo que la captura de vídeo ([http://www.hispasec.com/laboratorio/troyano\\_bancario\\_captura\\_video.pdf](http://www.hispasec.com/laboratorio/troyano_bancario_captura_video.pdf)). El capturar una pequeña área alrededor del cursor del ratón requiere menos recursos del sistema, el tamaño de los archivos a enviar es mucho menor, y además obtiene unas imágenes donde se señala justo donde ha pinchado el usuario.

Al almacenar el atacante los diferentes archivos en carpetas separadas por ordenador infectado y las imágenes con el formato *díamesaño-horamínutossegundos.jpg*, le permite conocer exactamente la sucesión de teclas pulsadas por cada usuario y, por tanto, las contraseñas introducidas.

De manera independiente a las técnicas utilizadas (existen otras distintas actuando a día de hoy), queda patente que la implantación generalizada de los teclados virtuales por parte de las entidades financieras está provocando que cada vez más troyanos los tengan en cuenta a la hora de realizar las capturas de datos.

A juzgar por el tipo de troyano, por las entidades a las que se dirige, y el destino a donde van a parar los datos capturados, el origen se sitúa en Brasil. Si este caso puntual se confirma como una tendencia, podría ser un dato preocupante para el resto de países y entidades afectadas.

Debemos tener en cuenta que Brasil es, con diferencia, el mayor productor de troyanos bancarios a nivel mundial, si bien hasta la fecha tenía un enfoque claramente autóctono dirigido a las entidades brasileñas.

## Comentarios e información adicional



Laboratorio Hispasec / VirusTotal

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

Hispasec Sistemas

<http://www.hispasec.com>

VirusTotal

<http://www.virustotal.com>