

Evolución de los *bankers*

Autor: Sebastián Bortnik, Analista de Seguridad de ESET para Latinoamérica
Fecha: Lunes 04 de mayo del 2009

Índice

Introducción.....	3
Keyloggers, una técnica primitiva.....	3
Keyloggers modernos	5
Superposición de imágenes.....	6
Phishing.....	7
Falsas aplicaciones bancarias	8
Nuevos mecanismos de autenticación.....	9
Conclusión.....	10
Más información	11

El robo de información personal es uno de los vectores de ataque más frecuentes en el escenario actual del malware. La información bancaria y financiera de los usuarios es uno de los objetivos preferidos de los atacantes, ya que ofrece un canal directo a su fin último: el dinero.

Introducción

Se denomina **troyanos bancarios** (o bankers) a una familia de códigos maliciosos cuyo fin es la obtención de información bancaria de los usuarios. Por lo general, los datos que se desean obtener son las credenciales de autenticación en *home banking*, que luego son enviadas al creador del código por algún medio. De esta forma, el atacante puede ingresar a la cuenta bancaria de la víctima con acceso total para realizar cualquier tipo de operación que esté permitida por la entidad financiera.

Dentro de la familia mencionada, existe una gran cantidad de variantes que difieren en sus métodos y características. Las mismas han ido evolucionando al pasar de los años, en tanto los atacantes se vieron afectados por las contramedidas implementadas por las entidades financieras. Dichas variantes serán descritas a lo largo de este informe, incluyéndose las particularidades más importantes de sus ejemplares más relevantes.

La mayoría de los casos presentados en el presente artículo son detectados por ESET NOD32 como *Win32/Spy.Banker*. Algunas de ellas serán identificadas a modo de ejemplo.

Keyloggers, una técnica primitiva

Las primeras variantes de troyanos bancarios hacían uso de técnicas de keylogging, destinadas a capturar las teclas que el usuario tipea mientras ingresa al home banking, almacenar la información en un archivo temporal y, posteriormente, enviar la información al atacante. Generalmente los datos obtenidos son enviados por correo electrónico, alojados en servidores FTP u otros medios similares.

Un keylogger (acrónimo en inglés de *key* – en español, tecla – y *logger* – registro) es una herramienta que permite capturar las pulsaciones del teclado y almacenarlas para su posterior visualización. Esta funcionalidad no ha sido creada específicamente para el robo de información bancaria, sino que puede ser utilizada tanto para fines benignos como maliciosos.

Los bankers explotan estas aplicaciones de otra forma. Capturar todas las pulsaciones del teclado y registrarlas en un archivo, implicaría un tiempo importante de análisis por parte del atacante en busca de las pulsaciones correspondientes al uso de banca en línea. Es por ello que los troyanos incluyen una

funcionalidad que monitorea la actividad del sistema y activa el registro de pulsaciones cuando es identificado un acceso a este tipo de recursos. Tiempo atrás hubo en Brasil casos reales en los que la variante *Win32/Spy.Banker.SO* comenzó con el registro al detectar que un usuario accedía a un listado de portales de bancos legítimos.

Las primeras variantes de esta amenaza utilizaban estas técnicas. Otros ejemplos son las firmas *Win32/Spy.Banker.I*, *Win32/Spy.BankerUI* o *Win32/Spy.Banker.MT*, entre otras.

Con la proliferación de esta amenaza, los bancos comenzaron a ofrecer una capa de mayor protección en el formulario de autenticación. Para ello, la gran mayoría de los portales agregaron un teclado virtual opcional al momento de ingresar los datos de acceso, permitiendo que se ingresen los caracteres haciendo clic en un teclado que aparece en pantalla y evitando así, que un *keylogger* capture la información sensible.



Imagen 1 – Ejemplo de un teclado virtual en formulario de acceso

En la imagen superior, obtenida de un reconocido banco, se exhibe la utilización del teclado virtual, por medio del cual, a medida que el usuario hace clic sobre el teclado en pantalla, los caracteres van siendo ingresados en el formulario.

Keyloggers modernos

La instalación de teclados virtuales en los portales de banca en línea hizo que la efectividad de los troyanos bancarios se viera afectada, aunque no tan severamente, dado el bajo índice de usuarios que en aquel entonces lo utilizaban. No obstante, los atacantes comenzaron a trabajar en lo que fue la primera evolución de los bankers, la cual consistió en la incorporación de técnicas avanzadas de keylogging en sus códigos a fin de contrarrestar las funcionalidades de los teclados virtuales.

El primer caso se basó en la utilización de las funciones API del sistema operativo y la captura de las coordenadas de los clics del mouse en pantalla. Es decir, si el usuario hace un clic por cada caracter de su contraseña, el código malicioso registra, por cada uno de ellos, las coordenadas de ubicación del mouse en ese momento. Posteriormente, conociendo el teclado virtual del banco y su disposición en pantalla, la resolución de la misma y las coordenadas, el atacante puede rearmar los datos ingresados por el usuario. En estos casos, cuando el código malicioso comienza a capturar las pulsaciones de las teclas, se registran dichas coordenadas en paralelo. Al ser la información enviada al atacante, éste dispone, de una u otra forma, de los datos de acceso del usuario.

Como contramedida, los bancos comenzaron a agregar una nueva funcionalidad a sus teclados virtuales: alterar el orden de las teclas respecto del dispositivo físico. De esta forma, las coordenadas son válidas solo para la distribución de las teclas que fue mostrada al usuario al momento de la autenticación.



Imagen 2 – Teclado virtual con teclas aleatoriamente ordenadas

Sin embargo, nuevamente los atacantes hicieron evolucionar los códigos maliciosos de forma tal de evadir las contramedidas implementadas por los bancos para proteger a sus usuarios.

La siguiente generación de variantes de la familia, incluyó funcionalidades para capturar la información del usuario en los teclados virtuales:

- Captura de imágenes alrededor del mouse ante cada clic: de esta forma, el atacante recibe una secuencia de imágenes que forman los datos de acceso del usuario, ingresados a través del teclado virtual
- Captura de video: el código malicioso comienza una grabación de video al detectar un acceso a *home banking*, que luego es enviada al atacante en formato comprimido

Los primeros ejemplares que capturaban video, fueron [detectados por ESET NOD32](#) hace más de dos años en Brasil, en ese caso las variantes *Win32/Spy.Banker.NOX* y *Win32/Spy.Banker.NOY*.

Superposición de imágenes

Otra técnica utilizada por los troyanos bancarios consiste en el uso de banners para superponer falsas porciones de sitios sobre los originales y lograr así que los usuarios hagan clic en los espacios del atacante. Esta técnica fue detectada durante el 2007 y muchas variantes implementan esta metodología. Algunas de las firmas que identifican a esta amenaza son, por ejemplo, *Win32/Spy.Banker.ABZ*, *Win32/Spy.Banker.ZZ* y *Win32/Spy.Banker.CHC*, entre otras. Esta última, posee código HTML para superponer en bancos legítimos. Para más detalles se puede acceder al [análisis técnico realizado por ESET Latinoamérica](#).

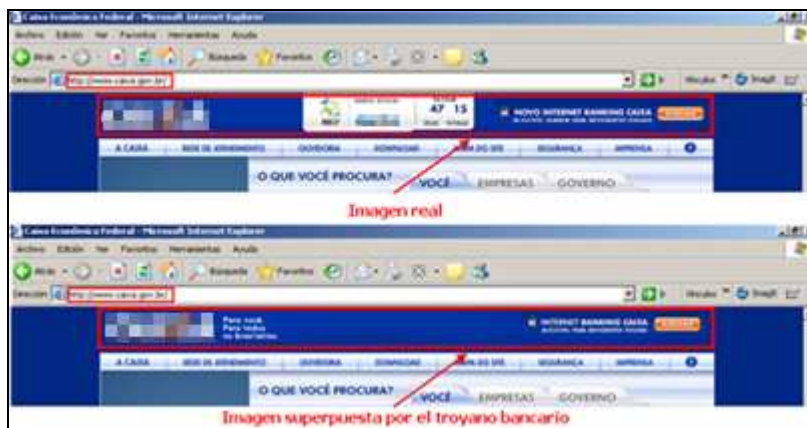


Imagen 3 – Banner de suplantación para un reconocido banco de Brasil

Nótese que, como contramedida para esta técnica, las entidades financieras no pueden realizar prácticamente nada, ya que el usuario no interactúa con el sitio web original. La única capa de protección

es evitar la infección del troyano, a través de una solución antivirus con capacidades proactivas de detección.

Phishing

El [phishing](#) es otra de las técnicas utilizadas para obtener información bancaria de los usuarios. En este caso, la amenaza no refiere a un código malicioso en particular, ni a la familia *Win32/Spy.Banker*, analizada en sus diferentes variantes.

Para el robo de información bancaria, los atacantes crean sitios web similares a los originales, intentando engañar al usuario para que este navegue en ellos pensando que está en el sitio oficial y brinde la información de acceso a sus cuentas. Existen dos técnicas para que la víctima llegue al sitio web:

1. Se envían correos electrónicos simulando ser la entidad bancaria, con enlaces al sitio falso (modalidad bajo la cual no se utilizan códigos maliciosos)
2. A través de un código malicioso, se modifica la configuración de los sistemas, redireccionando a un sitio web falso al usuario que desee ingresar a cierto banco. Esta técnica se denomina [pharming local](#) y los archivos de este tipo son detectados bajo la familia *Win32/Qhost*.

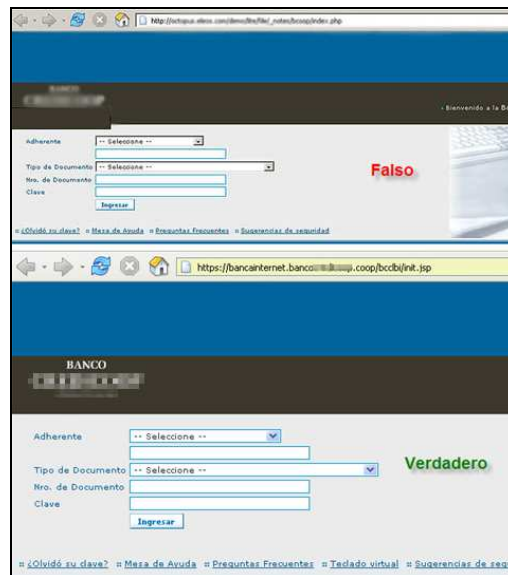


Imagen 4 – Phishing a una banca en línea

En la imagen superior puede observarse el esfuerzo de los atacantes por realizar con la mayor exactitud posible los sitios web falsos.

El ataque también puede ser llevado a cabo con otros medios en lugar de la web, dando lugar a las técnicas conocidas como [vishing y smishing](#), que hacen uso de la telefonía IP y los mensajes de texto de los teléfonos celulares.

Falsas aplicaciones bancarias

La última evolución detectada por la familia de trojanos bancarios, durante el año 2009, utiliza una técnica de phishing particular: la simulación de software legítimo de la entidad financiera.

El ataque consiste en enviar un correo electrónico al usuario simulando provenir del banco que indica la necesidad de descargar una aplicación. Cuando el usuario ejecuta la aplicación, observará una interfaz con aspecto (logo, colores, etc.) del banco que, en algún momento, solicitará al usuario sus credenciales de acceso. Nótese en la imagen siguiente, que incluso se ofrece al usuario un teclado virtual, para ganar su confianza respecto a la legitimidad de la aplicación.



Imagen 5 – Software simulando login bancario

Algunas de las variantes que utilizan estas técnicas son las firmas *Win32/Spy.Banker.QNB* y *Win32/Spy.Banker.QOH*.

En la siguiente imagen puede observarse, con un capturador de tráfico de red, cómo la información ingresada es enviada al atacante por correo electrónico.

```
From: [redacted]@isbt.com.br
Subject: ar
To: [redacted]@isbt.com.br
Date: Mon, 23 Mar 2009 10:19:08 -0300
X-Priority: 3
X-Library: Indy 9.00.10

Tipo de documento: DNI
Numero do documento: 11111111
Clave de Ita. Home Banking: 111111
Clave de la Tarjeta Elect.nica Ita.: 1111
.
250 2.0.0 ok: queued as D4D84F0000A1
QUIT
221 2.0.0 Bye
```

The image shows a network traffic capture of an email. The email header includes fields for From, Subject, To, Date, X-Priority, and X-Library. The body of the email contains sensitive information: 'Tipo de documento: DNI', 'Numero do documento: 11111111', 'Clave de Ita. Home Banking: 111111', and 'Clave de la Tarjeta Elect.nica Ita.: 1111'. An orange arrow points to the document details section.

Imagen 6 – Envío de credenciales de acceso al atacante

Nuevos mecanismos de autenticación

En el vaivén entre ataques y contramedidas que atacantes y entidades financieras vienen sosteniendo hace años, éstas últimas continúan trabajando en la implementación de estrategias alternativas de autenticación y control con el objetivo de brindar mayor protección a sus usuarios. Es decir, anteponen nuevos factores de autenticación, además de un usuario y contraseña de acceso, para poder operar la banca en línea.

Algunas de las principales medidas utilizadas por los bancos son:

- **Tarjetas de coordenadas:** son tarjetas físicas con una tabla de doble entrada que el cliente debe tener en su poder. Al momento de realizar la transacción, el sitio web le indica al usuario las coordenadas de la tabla que corresponden a la clave que debe ingresar. Su seguridad radica en la necesidad de acceso físico y en la variabilidad de utilización de claves. No obstante, debe contemplarse el hecho de que también existen troyanos dedicados al robo de tarjetas de coordenadas.
- **Tokens de seguridad:** son dispositivos que actualizan periódicamente (cada un minuto o menos) una clave única. Esta debe ser utilizada combinada con las claves del usuario para acceder al servicio o para realizar ciertas operaciones. Este tipo de tecnologías trabaja con doble autenticación, en conjunto con los datos de acceso anteriores del usuario: algo que se posee (token) y algo que se conoce (contraseña).

- Dispositivos biométricos: ofrecen un alto índice de seguridad, dada su naturaleza. Aunque en algunos bancos se ha trabajado en su implementación, en Latinoamérica no ha sido aún confirmada dicha tendencia. El principal inconveniente de esta tecnología es la necesidad de hardware de autenticación biométrica para cada usuario que quiera hacer uso de la banca en línea.
- Telefonía celular: a través de los teléfonos móviles, los usuarios tienen la posibilidad de realizar transacciones bancarias. Sin embargo, estos dispositivos también se están empezando a ver afectados por amenazas de este tipo.

Asimismo, los bancos han incrementado en el último tiempo sus medidas de concientización hacia sus clientes, colocando, por ejemplo, información en sus páginas web respecto a los cuidados y recomendaciones básicas de protección.

Conclusión

El robo de información bancaria es un objetivo recurrente de los creadores de códigos maliciosos y atacantes ya que ofrece una vía directa para la obtención de dinero. A pesar del esfuerzo de las entidades financieras, los atacantes han logrado una evolución de las amenazas con el fin de sortear las contramedidas implementadas y es de esperar que esto continúe en el tiempo de forma indeterminada.

Como protección, los usuarios, deberán **contar con una herramienta de seguridad antimalware con capacidades proactivas de detección**, como ESET NOD32 y ESET Smart Security a fin de evitar la infección de sus sistemas por códigos maliciosos de este tipo. Es importante, además, hacer uso de la banca en línea con los cuidados necesarios.

La educación de los usuarios, por la que [ESET Latinoamérica](#) trabaja con constancia, debe ser realizada en conjunto por la comunidad de seguridad informática y, en este caso, las entidades financieras afectadas, a través de la concientización e información al público.

Los delincuentes se esfuerzan para generar nuevos vectores de ataque, ante cada capa de protección que se implemente y todos los actores afectados deben estar preparados para dar respuestas rápidas y así evitar el robo de dinero, que siempre es el fin último de los atacantes.

Más información

ESET Latinoamérica

<http://www.eset-la.com>

Plataforma Educativa de ESET Latinoamérica

<http://edu.eset-la.com>

Blog de Laboratorio de ESET Latinoamérica

<http://blogs.eset-la.com/laboratorio>