

Robo de Información personal online



Autores: Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica
Cristian Borghello, Technical & Educational Manager de ESET para
Latinoamérica

Fecha: Martes 26 de junio del 2008

El presente documento tiene como objetivo presentar la evolución de las técnicas para obtener información confidencial o privada en Internet, ya sea a través de sitios web o a través de programas dañinos. Además, se presentan los consejos básicos para reconocer y evitar este tipo de ataques tanto en un ambiente hogareño como en uno corporativo.

Desde el nacimiento del comercio electrónico, los servicios ofrecidos a través de Internet cambiaron radicalmente la manera de hacer negocios ampliando significativamente su horizonte al establecer nuevos modelos de mercado.

Uno de los servicios más representativos surgidos de este nuevo modelo de negocio, es el que brindan las entidades financieras y bancarias al facilitar la realización de operaciones de cualquier tipo, requiriendo para ello tan sólo una conexión a Internet. Esto posibilita una manera cómoda y eficiente de interactuar con las organizaciones, desde la tranquilidad del hogar y sin la necesidad de trasladarse hasta el lugar físico de la misma.

Paralelamente al surgimiento de este modelo de negocio online, fueron apareciendo nuevos y cada vez más complejos ataques informáticos que buscan obtener información confidencial de los usuarios, dando lugar a una nueva modalidad delictiva, encuadrada dentro del marco de las estafas.

Las estafas y fraudes (físicos) no son delitos nuevos y están regulados por leyes en la mayoría de los países del mundo. Sin embargo, el robo de información confidencial a través de medios virtuales, aprovechando las ventajas y facilidades que ofrece Internet, es un nuevo desafío para las jurisprudencias internacionales.

Dependiendo de la legislación de cada país, estos fraudes muchas veces no son ilegales debido a que las leyes no los consideran, destacándose una falta importante de acciones en este sentido.

Las técnicas de ataque son utilizadas con fines de lucro, aprovechando las nuevas tecnologías y su evolución constante. Actualmente, las personas que realizan estas acciones se apoyan fundamentalmente en el empleo de sitios web falsos y de códigos maliciosos, que poseen la capacidad de registrar la información ingresada por el usuario.

En los últimos años se ha registrado un mayor incremento de estas modalidades delictivas, convirtiéndose en la principal y más peligrosa amenaza para los usuarios que hacen uso de servicios online.

Metodologías

A continuación, se exponen dos de los principales métodos actuales para obtener información personal de usuarios. El primero de ellos, el phishing, hace referencia a la obtención de información confidencial en sitios web, y el segundo, los troyanos bancarios (bankers) refieren a la utilización de códigos maliciosos para el mismo fin.

El Phishing

El phishing es una modalidad de obtención de información llevada a cabo a través de Internet que intenta obtener, de manera completamente involuntaria y fraudulenta, datos personales o sensibles que posibiliten realizar una estafa, utilizando metodologías de Ingeniería Social [1].

Los primeros casos de phishing a entidades bancarias fueron reportados en Estados Unidos durante el 2003 y desde entonces, esta modalidad delictiva se ha ido diseminando a lo largo del planeta, constituyendo en la actualidad una de las principales amenazas para cualquier sitio que maneje información confidencial.

La mayoría de los casos de ataques de phishing se presentan ante los usuarios en forma de correo electrónico masivo (spam) invitándolo a ingresar a un sitio web similar al de la entidad financiera para solicitarle información confidencial (usuario, contraseña, PIN, número de tarjeta de crédito, etc).

Los Códigos Maliciosos

A continuación, se exponen aquellos tipos de ataques de malware más representativos de la actualidad haciendo referencia a su línea evolutiva a largo del tiempo.

Backdoor

A finales de los '90, las aplicaciones backdoor, como Sub7 o BackOrifice [2], dieron origen al robo de información de forma remota. Dichas aplicaciones poseían componentes que permitían interceptar cualquier tipo de información y enviarla al atacante a través de la red.

En ese momento, la información relacionada a tarjetas de crédito podía ser parte de los objetivos de las personas malintencionadas que utilizaban estas aplicaciones, para luego usar esos datos para adquirir

distintos servicios y/o productos en forma fraudulenta, perjudicando directamente al dueño real de la tarjeta.

Keylogger

Estas aplicaciones son troyanos y se caracterizan por poseer la capacidad de capturar y monitorear, de manera oculta, todo aquello que se escribe a través del teclado e incluso con el clic del mouse. Además, existen dispositivos físicos que se acoplan a modo de adaptadores al equipo y cuyas funcionalidades son similares a las de un keylogger de software.

Un atacante busca instalar keyloggers en el sistema de la víctima y configurarlo para que le envíe toda la información que haya capturado y almacenado, incluyendo las contraseñas de acceso a diferentes servicios, como por ejemplo el Home Banking.

Troyanos bancarios (bankers)

La evolución de los códigos maliciosos fue dando origen a nuevas estrategias de engaño que permiten obtener información particular de las computadoras comprometidas a través de troyanos.

Debido a sus características singulares, algunos de estos códigos maliciosos, reciben el nombre genérico de troyanos bancarios, ya que su objetivo general es obtener información bancaria de los usuarios.

Tipos de ataques

Una vez descritas algunas de las herramientas utilizadas por los delincuentes, es necesario estudiar las diversas metodologías y tipos de ataques posibles que buscan robar información confidencial del usuario para utilizarla fraudulentamente para adquirir productos o servicios:

Ataques de phishing basados en suplantación

En estos casos, la metodología consiste en suplantar la dirección verdadera de un sitio web por una dirección falsa. Entre las técnicas que se utilizan para llevar a cabo ataques de phishing por suplantación, los más utilizados son los siguientes:

- **Nombres de dominios erróneos:** consiste en registrar dominios similares a los utilizados por las entidades bancarias. Fue una de las primeras formas explotadas y si bien los sitios pueden ser fácilmente rastreados e inhabilitados, sigue siendo utilizado en la actualidad. Ejemplo:

`www.bancoenlinea.com` → `www.bancoenlineas.com`.

Es decir, para la primera dirección verdadera, *www.bancoenlinea.com*, el phisher registra una dirección similar *www.bancoenlineas.com*.

El truco radica en registrar un nombre similar al original, por lo general agregando o cambiando alguna de los caracteres del dominio original. Con esto, se logra que el usuario ingrese al sitio falso cuando comete el error de tipear la URL o cuando ingresa desde un enlace sin notar la diferencia en el nombre del dominio.

En esta metodología, conocida como **typosquatting**¹, el atacante puede “jugar” con los caracteres y registrar una dirección web que a simple vista parece la original, como por ejemplo:

`www.banc0enlinea.com`

Donde la letra “o” se ha remplazado por el número “0”.

- **Ofuscación de URL:** se crea un sitio web falso ocultando, o evitando la fácil lectura, de la dirección o URL a la que el usuario ingresa. Esta técnica es denominada ofuscación² de URL.

En este caso, el phisher busca dificultar la lectura de la URL a través de diferentes trucos que básicamente consisten en ocultar la dirección web codificando la dirección IP de distintas maneras. Como resultado, lo que el usuario visualiza en la barra de navegación podría ser algo similar a lo siguiente:

- Visualización de la dirección en sistema decimal:
`http://201.60.31.236/`
- Visualización de la dirección en sistema hexadecimal:
`http://0xc9.0x3c.0x1f.0xec/`
- Visualización de la dirección en sistema octal:
`http://0311.0074.0037.354/`

Para más información al respecto, se sugiere la lectura del curso “Seguridad en las transacciones comerciales en línea” disponible en la Plataforma Educativa de ESET Latinoamérica.

¹ **Typosquatting:** <http://en.wikipedia.org/wiki/Typosquatting>

² **Ofuscación:** técnica que consiste en dificultar la lectura del texto

- Clonación de páginas web:** consiste en hostear o alojar una página web falsa, muy similar a la original de la entidad atacada, en un servidor controlado por el atacante. Actualmente, esta técnica es la más común y la más explotada para realizar ataques de phishing. A continuación, se presenta una página web de una entidad bancaria, que ha sido copiada, pero presenta algunas alteraciones con respecto a la original:



Imagen 1-Ejemplo de clonación de página web

Al contrario de lo que se puede suponer, cualquier persona puede realizar un ataque de phishing sin poseer conocimientos avanzados del tema, debido a que existen aplicaciones que permiten “automatizar” el desarrollo de estos ataques.

Los denominados *kits de phishing*, si bien tuvieron su mayor auge y popularidad a mediados del 2007, aún permiten llevar a cabo este tipo de fraudes con sólo modificar una plantilla preestablecida sobre cada entidad.

Estos kits son comercializados a través de sitios web y foros, con lo que el atacante sólo necesita un servidor web para concretar los ataques y obtener la información bancaria y financiera de los clientes de una determinada institución en cuestión de horas.

Utilización de troyanos bancarios

A diferencia de los keyloggers convencionales, los troyanos bancarios están diseñados para detectar patrones de cadenas como por ejemplo “password” o “contraseña” cada vez que el usuario ingresa a la zona de registro de la entidad atacada. En ese momento, se activa la captura de información específica, obteniendo los datos de registro del usuario.

Ante esta problemática, las entidades comenzaron a implementar contramedidas como los teclados virtuales con el ánimo de minimizar el impacto causado por las acciones de estos ataques.

Esta medida de seguridad permite ingresar la información solicitada mediante la utilización del mouse y a través de un teclado que se despliega en pantalla, posibilitando que el usuario ingrese sus datos sin presionar ninguna tecla en el teclado físico.



Imagen 2- Diferentes tipos de teclados virtuales

Posteriormente, los atacantes comenzaron a implementar, en estos troyanos, un módulo que permite no sólo el registro de lo que se escribe con el teclado, sino que también permite realizar capturas de pantalla (imágenes) cada vez que el usuario accede al sitio web y realiza un clic sobre el teclado virtual. De esta manera, los creadores de códigos maliciosos lograron saltar las restricciones provistas por esta contramedida.

Del mismo modo, muchos de estos troyanos bancarios basados en componentes keylogger, también poseen la capacidad de grabar videos. Estos videos capturan parte de la pantalla del usuario tomando como referencia el cursor del mouse, precisamente en la zona donde se ubica el teclado virtual, permitiendo que el atacante logre obtener, de igual forma, la información que busca.

Para más información al respecto se sugiere la lectura del curso “Seguridad en las transacciones comerciales en línea” disponible en la Plataforma Educativa de ESET Latinoamérica.

Los primeros casos donde se utilizaban capturas de video fueron reportados en Brasil, y si bien esta modalidad no es una estrategia ampliamente difundida mediante troyanos bancarios, no significa que no sea utilizada por los atacantes. Ejemplos de bankers con estas características son la familia de troyanos que ESET NOD32 detecta como *Win32/Spy.Banker*.

Aunque para muchos troyanos bancarios los teclados virtuales no constituyan obstáculo alguno, es recomendable su utilización en los sitios web de aquellas entidades que dispongan de ellos.

Para los clientes de entidades que no dispongan de teclado virtual, se puede recurrir al incorporado en la mayoría de los sistemas operativos. En el caso de plataformas Windows, este recurso puede ser activado como sigue:

Inicio → Ejecutar → osk



Imagen 3 – Ejemplo del teclado virtual de sistemas Windows

Redireccionamiento Web

Otra de las técnicas utilizadas por los troyanos bancarios es la denominada *DNS Poisoning* (envenenamiento de DNS), consistente en modificar los DNS³ para redireccionar el dominio real hacia una dirección IP falsa creada por el atacante.

De esta manera, cada vez que el usuario ingrese a una determinada dirección, como por ejemplo *www.bancoenlinea.com* o a una dirección IP como *201.60.31.236*, será redireccionado hacia la página web previamente creada por el atacante con el fin de engañar a la víctima.

³ **DNS:** Domain Name Server – Sistema de Nombres de Dominio. Consiste en un sistema que permite la traducción de los nombres de dominio por direcciones IP y viceversa.

La técnica más utilizada por los troyanos bancarios es la denominada **Pharming Local**. En este caso, cuando el troyano bancario compromete un equipo, lo que modifica es un archivo llamado "hosts" que puede ser encontrado en cualquier sistema operativo.

Este es un archivo de texto que funciona a modo de caché interno permitiendo resolver, de manera local, nombres de dominio contra direcciones IP, de manera tal que la relación entre los nombres de los sitios web configurados en tal archivo, identifican de manera unívoca las direcciones IP, establecidas en el archivo en cuestión.

Para más información al respecto, se sugiere la lectura del curso "Seguridad en las transacciones comerciales en línea" disponible en la Plataforma Educativa de ESET Latinoamérica.

La familia de troyanos bancarios identificados por ESET NOD32 como *Win32/Qhost* constituyen ejemplos concretos de troyanos basados en esta técnica [3].

Superposición de imágenes

La técnica se basa en la superposición de una imagen en la zona de acceso del sitio web. Se utiliza otra variante de troyano bancario para controlar el momento en que el usuario ingresa al sitio web de la entidad elegida. Cuando esto sucede, el troyano muestra una imagen que se superpone a la del sitio web, en la zona de acceso del login de usuario.

Es decir que el usuario ingresa a la página real de la entidad bancaria, sin percatarse de que en la zona de acceso se superpuso una imagen falsa. Cuando el usuario hace clic sobre la imagen desplegada por el código malicioso, y no sobre la verdadera zona de acceso, ingresa al sitio web falso donde sus datos serán grabados por el troyano y enviados al atacante.

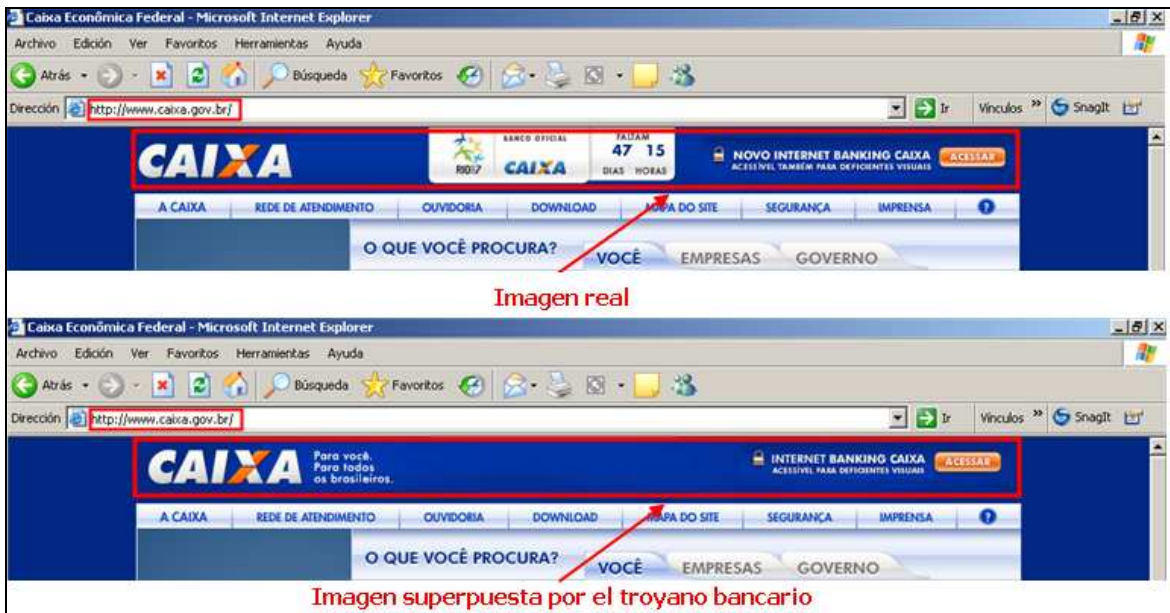


Imagem 4 - Comparación entre la página verdadera y la falsa

Una problemática mundial

Lamentablemente, los ataques descritos son cada vez mayores y se encuentran en crecimiento a nivel mundial. Según el APWG [4], sólo durante enero del 2008 se reportaron alrededor de 30.000 casos de ataques de phishing, siendo Estados Unidos el país con mayor tasa de hospedaje de sitios web falsos con casi el 37,25%, seguido por Rusia, China y Alemania con el 11,66%, 10,3% y 5,64% respectivamente.

En Latinoamérica, esta problemática también alcanzó tasas de propagación realmente preocupantes registrándose una gran actividad de ataques en muchos países de la zona. Por su lado, Brasil se encuentra entre los países de América Latina que realizan mayor cantidad de ataques de phishing.

Medidas para prevenir el robo de información

Además de enfatizar que las entidades financieras y bancarias jamás solicitan claves, cambios de ellas o información personal de los clientes a través del correo electrónico, es sumamente importante que los usuarios incorporen hábitos de navegación que permitan minimizar el impacto que provoca ser víctima de los ataques descritos.

A continuación, se presenta una serie de consejos que ayudan a contrarrestar estas acciones maliciosas [5]:

- **Mantener el sistema operativo, el navegador y el antivirus con las últimas actualizaciones de seguridad disponibles.** Esto ayuda a mantener el sistema libre de todo tipo de códigos maliciosos, sobre todo, aquellos que aprovechan técnicas de inyección de código HTML y vulnerabilidades *0-Day* (de día cero).
- **Instalar un antivirus con capacidades de detección proactiva.** Debido a la gran variedad de malware, las técnicas de detección utilizadas por las mejores soluciones antivirus están basadas en la detección proactiva de los códigos maliciosos. De esta manera, a través de un análisis en tiempo real, el antivirus puede indicar que determinado archivo es potencialmente peligroso, incluso sin que el mismo cuente aún con una firma que lo identifique.
- **Hacer caso omiso a correos electrónicos de origen desconocido o a nombre de entidades financieras o bancarias.** Por lo general, los correos electrónicos con estas características suelen ser no deseados (spam) y esconden potenciales ataques de phishing buscando propagar malware como los descritos. Del mismo modo, es conveniente no atender a mensajes escritos en idiomas que no son el nativo de quien los recibe.
- **Evitar introducir datos personales y/o financieros en sitios desconocidos.** De esta manera, se minimiza la posibilidad de recibir correo electrónico no deseado, una de las principales vías por las que se diseminan los ataques de phishing y malware.
- **Escribir con el teclado, la dirección de la entidad en la barra de navegación.** Es recomendable no acceder a sitios web por medio de enlaces incrustados en correos electrónicos, sino que es conveniente acceder a dichos sitios escribiendo directamente la dirección en la barra de navegación del navegador que se utilice.

- **No operar desde ambientes públicos.** En lo posible, se debe evitar acceder a sitios de transacciones comerciales desde sistemas que se encuentren en lugares de acceso público como cibercafés, locutorios, aeropuertos, hoteles, etc. ya que, al ser utilizadas por cualquier persona, pueden conllevar a potenciales riesgos de robo de datos.
- **Verificar las medidas de seguridad del sitio web.** Otro buen hábito es verificar la existencia de un candado en el navegador utilizado, que permita visualizar el certificado digital del sitio al que se accede. Asimismo, verificar que la dirección web de la página de la institución financiera comience con “https”⁴. Esto indica que se está navegando bajo un protocolo seguro.
- **Utilizar claves fuertes.** Una de las medidas de seguridad implementada por las entidades es que la contraseña de acceso debe cumplir con determinados requisitos impuestos por la entidad en cuestión. Por ello, al momento de elegir la contraseña, es conveniente que sea fácil de recordar pero que además sea lo suficientemente robusta como para dificultar su descubrimiento por parte de usuarios malintencionados.

Para más información al respecto se sugiere la lectura del curso “Seguridad en las transacciones comerciales en línea” disponibles en la Plataforma Educativa de ESET Latinoamérica.

Bajo este escenario, las organizaciones o empresas de cualquier tipo no están exentas de ser víctimas de ataques de phishing o malware; por lo tanto, además de las pautas mencionadas, es necesario extremar las medidas de seguridad teniendo en cuenta aspectos como:

- **Elaboración de políticas de seguridad claras.** Las mismas deben involucrar medidas que ayuden a combatir códigos maliciosos.
- **Ejecución de planes de seguridad.** Los que deben incorporar medidas en materia de concientización de usuarios.
- **Implementación de soluciones antimalware.** Implementar soluciones de seguridad antimalware con sistemas de detección proactiva que ayuden a prevenir la proliferación de códigos maliciosos que puedan afectar los activos de la compañía.

⁴ **HTTPS:** Protocolo seguro de transferencia de hipertexto (Hypertext Transfer Protocol Secure). Protocolo de comunicación que permite la transferencia de información de manera segura.

Denunciar casos de phishing

Un tema muy importante que surge luego de la exposición a problemas de ataques de phishing y que muchos usuarios demandan, radica en cómo denunciar estos casos de estafas en línea.

Si un usuario detecta un caso de phishing que afecte particularmente a clientes de alguna entidad de su país, una de las principales acciones que debería adoptar es denunciar el caso a la organización involucrada, para lo cual es aconsejable proveer la mayor cantidad de información posible relacionada al engaño.

También existen comunidades que se encargan de facilitar esta labor poniendo a disposición de los usuarios diversos medios de denuncia. Uno de los ejemplos más representativos es el Anti-Phishing Working Group donde se pueden reportar casos de phishing a través del correo electrónico. Otro caso lo representa PhishTank que permite denunciar estos casos a través de su sitio web [6].

Por otro lado, muchos países cuentan con grupos de respuestas ante incidentes denominados CERT. Estas organizaciones se encargan de atender los problemas relacionados con incidentes informáticos llevados a cabo en ambientes gubernamentales.

Los CERTs, al recibir denuncias por casos de phishing, realizan un reporte del incidente, contactan a las entidades involucradas e informan a los responsables de las ISP que hostean los sitios maliciosos, dando de baja a la página falsa.

Además, la mayoría de los navegadores de Internet han incorporado, entre sus funcionalidades, la posibilidad de denunciar páginas web maliciosas como medida de seguridad anti-fraude [7].

Conclusiones

La cantidad de troyanos y de sitios falsos encontrados cada día, confirma que las personas que se dedican a esta actividad ganan mucho dinero en el proceso, del cual el usuario forma parte involuntariamente, siendo la víctima en todos los casos.

Las metodologías actuales para robar información confidencial son muchas y mutan continuamente en el tiempo, por lo que estar informados sobre ellas se ha vuelto fundamental, así como también la utilización de soluciones de seguridad con capacidades proactivas, como ESET NOD32 Antivirus o ESET Smart

Security, capaces de prevenir cualquier tipo de ataque de códigos maliciosos, incluso aquellos desconocidos.

La combinación entre un usuario educado en términos de seguridad informática y software de seguridad de última generación logran la mejor forma de prevención contra cualquier amenaza actual.

Más información:

[1] El arma infalible: La Ingeniería Social

<http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social>

[2] Cronología de los virus informáticos

<http://www.eset-la.com/threat-center/1600-cronologia-virus-informaticos>

[3] Nuevo ataque de phishing a Banamex

<http://blogs.eset-la.com/laboratorio/2008/05/20/nuevo-ataque-phishing-banamex/>

[4] Sitio de Anti-Phishing Working Group APWG

<http://www.antiphishing.org/>

[5] Consejos contra el malware III

[http://www.eset-la.com/threat-center/1535--consejos-contr-malware-\(iii\)](http://www.eset-la.com/threat-center/1535--consejos-contr-malware-(iii))

[6] Sitio de PhishTank

<http://www.phishtank.com/>

[7] Denunciar Phishing

<http://blogs.eset-la.com/laboratorio/2008/04/01/denunciar-phishing/>

Plataforma Educativa de ESET Latinoamérica

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

Blog de Laboratorio de ESET Latinoamérica

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