Boletines PandaLabs:

Datos bancarios al descubierto

www.pandasecurity.com/homeusers/security_info | www.pandalabs.com

Índice

1.- Introducción

Los troyanos bancarios siguen suponiendo una gran amenaza para los usuarios y es que, a pesar de que las entidades bancarias han ido aumentando las medidas de seguridad de sus páginas web, también los troyanos bancarios se han ido sofisticando e incluyendo nuevas funcionalidades.

Una de las mayores preocupaciones de los usuarios en cuanto a los riesgos de Internet es el robo de información confidencial, como contraseñas y más aún si se trata de datos bancarios. Esto convierte a los troyanos bancarios en uno de los tipos de malware más peligrosos para los usuarios, ya que están diseñados precisamente para robar ese tipo de información.

Los troyanos bancarios juntos con los falsos programas antivirus parecen haberse proclamado como las categorías más rentables para los ciberdelincuentes.

La ingeniería social sigue siendo uno de los métodos más utilizados por los ciberdelincuentes para introducir este tipo de malware en los ordenadores de los usuarios. Aunque no siempre es imprescindible la intervención del usuario, ya que otra manera habitual de introducir malware en los ordenadores es a través de páginas web con kits de instalación de malware mediante exploits.

Una vez instalado en el ordenador, el principal objetivo de estos troyanos es conseguir los datos bancarios de los usuarios afectados. Normalmente, los troyanos se quedan residentes en memoria y solo se activan cuando el usuario accede a la página web de ciertas entidades bancarias. Para ello, los troyanos cuentan con una lista de bancos a los que atacar.

Para los ciberdelincuentes es relativamente sencillo obtener estos programas maliciosos, ya que existe todo un mercado de venta de troyanos diseñados a la carta y de los denominados kits bancarios, que permiten no solo crear troyanos con múltiples funcionalidades, sino controlarlos y enviarles nuevas instrucciones.

Entre otras cosas, en este boletín resumiremos las principales familias de troyanos bancarios, explicaremos cuáles son las vías de entrada habituales, cómo suelen robar la información, y analizaremos el complejo entramado que hay detrás de este negocio tan lucrativo. Asimismo, ofreceremos una serie de recomendaciones para mantenerse protegido frente a estas amenazas.

2.- Principales familias

A pesar de que existen diversas familias de troyanos bancarios, a continuación destacamos los tres tipos donde se pueden englobar las familias más activas:

1) Troyanos bancarios brasileños (Banbra, Bancos)

Estos troyanos están diseñados principalmente para robar contraseñas de entidades bancarias brasileñas y portuguesas, aunque también es posible encontrar entidades españolas en variantes de la familia "Bancos". Suelen enviar la información obtenida a través de correo electrónico o por FTP.

La diferencia entre ambas familias reside en su lenguaje de programación. Las variantes de la familia Banbra están programadas en Delphi, mientras que las de la familia Bancos en Visual Basic.

A diferencia de otras familias, no se crean con kits generadores de troyanos sino que son programados desde cero.

2) Troyanos bancarios rusos 1.0 (Cimuz, Goldun…)

Existen numerosas variantes de estas familias, ya que se suelen diseñar a través de herramientas de creación de troyanos. Sin embargo, las variantes creadas con estas herramientas presentan diferencias mínimas entre ellas, ya que se trata de kits que no se han actualizado durante los últimos años.

A consecuencia de ello, las nuevas variantes de estas familias de troyanos no implementan nuevas funcionalidades y su detección es relativamente sencilla desde el punto de vista del programa antivirus.

3) Troyanos bancarios rusos 2.0 (Sinowal, Torpig, Bankolimb)

Actualmente algunas de estas familias son las más activas y por lo tanto las más peligrosas, ya que cambian y se actualizan constantemente. Esto dificulta bastante su detección, además van añadiendo nuevas funcionalidades para robar credenciales de diferentes entidades.

Todos ellos tienen una forma común de funcionamiento: la lista de entidades a monitorizar para robar las credenciales la obtienen de un fichero de configuración, que puede estar bien junto al troyano o en un servidor aparte controlado por el ciberdelincuente, de tal forma que no tienen que modificar el troyano para añadir una nueva entidad. También utilizan diferentes técnicas de ocultamiento y polimorfismo que complican su detección y eliminación.

Como se puede observar en la siguiente gráfica, las familias más activas de troyanos bancarios son Sinowal, que representa un 46% del total de las familias diseñadas para robar datos bancarios, seguida de Banker con un 25% y Banbra con un 11%. El 18% restante corresponde a las demás familias de troyanos bancarios:

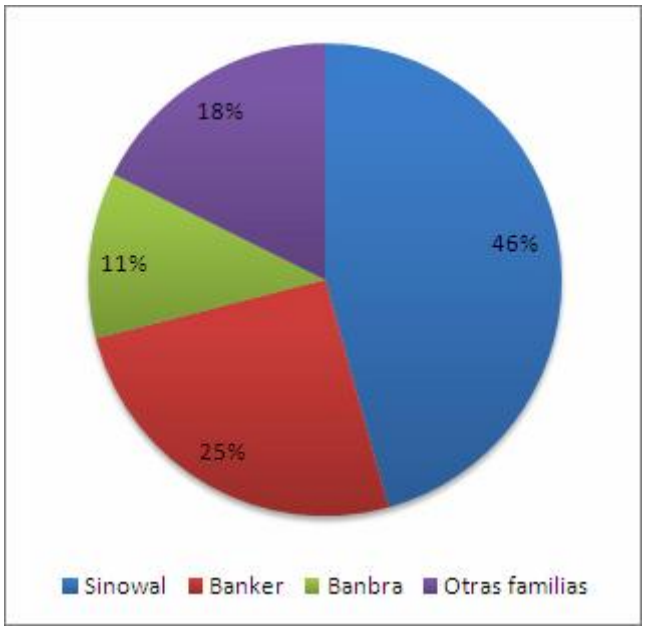

Fig.1 Distribución de familias de troyanos bancarios durante 2008

3.- Vías de infección

La ingeniería social sigue siendo la técnica más habitual para introducir este tipo de amenazas en los ordenadores de los usuarios. Para ello, se suelen distribuir en mensajes de spam que pueden ser de dos tipos:

1. Spam con un archivo adjunto. Normalmente se trata de archivos adjuntos comprimidos, con extensión zip, que contienen un archivo ejecutable. Sin embargo, para engañar a los usuarios y hacerles pensar que se trata de archivos inofensivos, utilizan las siguientes técnicas:

- Icono inofensivo: Presenta un icono relacionado con el tipo de archivo que pretende ser, es decir, si se trata de una imagen tendrá el siguiente icono:

Fig.2 Icono de una imagen

- Doble extensión: Normalmente, el archivo ejecutable tiene doble extensión, en primer lugar tiene la extensión del archivo por el que se hace pasar, por ejemplo en este caso que se trata de una imagen, la extensión sería jpg y después la extensión exe. Es habitual que entre la primera extensión y la segunda haya espacios libres para que el usuario no se percate de que la extensión real es exe.
  Aunque no siempre es necesario añadir una extensión "inofensiva". Si el archivo tiene un icono aparentemente inofensivo para el usuario, puede que la extensión del archivo pase desapercibida para el usuario.

Lo más habitual en estos casos es que el archivo que ejecuta el usuario se trate de un troyano de tipo Downloader. Estos archivos son de pequeño tamaño y su única función es conectarse a una página web para descargar el troyano bancario.

2. Spam que contiene enlaces a una página web.

Se trata de mensajes de correo electrónico que contienen un enlace a una página web. Normalmente, se suele utilizar como cebo un video. Cuando el usuario pulsa el enlace para ver el video, solicita la instalación de algo, puede tratarse de un códec o de una actualización flash, etc.

Una vez descargado el supuesto códec o actualización, hay ocasiones en las que el usuario es redirigido a una página web en la que puede ver un video para evitar que sospeche o no muestra ningún video, lo que podría alertar al usuario.

En el apartado de los ejemplares más destacados de troyanos bancarios, veremos ejemplos de mensajes de spam en los que se distribuyen.

Sin embargo, no hay que olvidar una técnica que se empezó a utilizar a comienzos de este año: la infección de páginas web legales. Para ello, se inserta en dichas páginas una llamada a un servidor malicioso con el objetivo de conseguir información sobre el sistema, como versión del sistema operativo, navegador y actualizaciones instaladas, para introducir malware, que pueden ser troyanos bancarios, intentando explotar alguna vulnerabilidad existente en el sistema.

4.- ¿Cómo roban la información?

Son varias las técnicas que utilizan para robar las contraseñas, y van desde la captura de datos a través de un simple keylogger hasta técnicas tan sofisticadas como la captura de datos al vuelo.

El grado de éxito de un keylogger depende de cómo esté configurado y sobre todo de su capacidad de filtrado de información. Un keylogger que se limita a registrar todas las pulsaciones de teclado introducidas por el usuario generaría una gran cantidad de datos inservibles para los ciberdelincuentes.

Por ello, es importante que el keylogger solo registre la información que le interesa al ciberdelincuente, es decir, los datos bancarios del usuario.

Por esta razón, es necesario que haya un filtrado de esa información y normalmente ese filtrado se hace en función de las páginas web que visita el usuario. Es decir, el troyano permanece controlando la navegación del usuario y se activa únicamente cuando el usuario accede a la página web de ciertos bancos.

Para centrarse en ciertas páginas web, los troyanos bancarios cuentan o descargan una lista con diversas cadenas, que pueden ser partes de una dirección web o cadenas de texto de un cuadro de diálogo, o del título de ventana relacionadas con entidades bancarias. El troyano monitoriza la actividad del sistema y se activa cuando detecta alguna de las cadenas de filtro.

Para monitorizar la navegación del usuario suelen utilizar varias técnicas:

- Registrarse como BHO (Browser Helper Object), que se trata de una funcionalidad de Internet Explorer que se ejecuta cuando se accede al navegador.

- Búsqueda de título de ventanas. Para ello utiliza una función de la API denominada *FindWindow*, que le permite localizar las ventanas que tengan un determinado título. Así un ciberdelincuente podría realizar búsquedas de títulos de ventanas activas que contengan nombre de entidades bancarias.

- Búsqueda de direcciones web en el navegador. El troyano cuenta con un listado de direcciones web pertenecientes a diferentes entidades bancarias. Cuando el usuario teclea en su navegador una dirección web que coincida con alguna de las del listado, el troyano se activa.

Una vez que han detectado que el usuario está accediendo a una página web bancaria, intenta obtener los datos bancarios del usuario a través de las siguientes técnicas:

- Captura de formularios: cuando el troyano detecta un formulario en alguna página web registra la información que el usuario introduzca en los formularios.

- Keylogging: registro de las pulsaciones de teclado introducidas por el usuario en las páginas web.

- Páginas falsas: el troyano crea una página web falsa que imita a la original. Cuando el usuario va a acceder a la página legítima de la entidad bancaria, el troyano ejecuta una aplicación que muestra la página web falsa en vez de la original.

- Formularios falsos: esta técnica consiste que en vez de crear una página web falsa, lo que hace es superponer una ventana que contiene un formulario sobre el formulario real, para que el usuario rellene el formulario falso.

- Campos extras en los formularios: inyecta código HTML en los formularios de las páginas web para solicitar más información.

- Pharming: Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa.

- Ataques "man-in-the-middle": los ciberdelincuentes hacen de intermediarios pudiendo leer, insertar y modificar mensajes entre el cliente y su banco sin que ninguna de las partes sea consciente de que la conexión entre ellas está comprometida.

5.- Sofisticación de los troyanos bancarios

Las entidades bancarias han reaccionado ante la amenaza que suponen los troyanos bancarios para la privacidad y confidencialidad del usuario y han mejorado la seguridad y la autenticación de los clientes. Como consecuencia de ello, se ha producido una sofisticación de los troyanos bancarios.

Las técnicas que utilizan para robar la información han ido mejorando a medida que los bancos, conscientes de la amenaza que suponen estos troyanos, han aumentado las medidas de seguridad en sus páginas web. Por ejemplo, la implantación de los teclados virtuales para el registro de los usuarios, supuso un importante avance en la seguridad de estas páginas web. De esta manera, un keylogger no podría capturar los datos introducidos por el usuario.

Sin embargo, los creadores de malware desarrollaron nuevas funcionalidades para los troyanos bancarios, haciéndoles capaces de registrar los movimientos realizados con el ratón e incluso realizar capturas de pantalla o de vídeo, como es el caso de Trj/Banbra.DCY.

Algunos ejemplares como los pertenecientes a la familia BankoLimb tienen un archivo con una lista de URLs de bancos objetivo. Cuando el usuario infectado con un BankoLimb accede a alguna página web cuya dirección coincida con la de su lista, el troyano se activará e inyectará código html extra en la página del banco.

Esto implica que, además de los campos habituales que tiene que rellenar el usuario para registrarse, tendrá que proporcionar información adicional. El usuario está en la página legítima, pero ligeramente modificada. Por eso es importante que si un usuario está navegando y accede a la página de su banco y le solicitan más información de la habitual, no confíe y no introduzca ningún dato en dicha página, porque posiblemente su ordenador esté infectado con algún troyano bancario y toda la información que introduzca será capturada.

Otras veces, los troyanos superponen la página falsa sobre la original para que el usuario no se de cuenta o directamente redirigen al usuario a una página falsa que imita a la original. Una vez que el usuario se registre en dicha página falsa puede mostrar una página de error o incluso podría redirigir al usuario de nuevo a la página original del banco para evitar que el usuario sospeche.

Algunas variantes de la familia del Sinowal son realmente sofisticadas, ya que son capaces de modificar datos "on the fly", es decir, al vuelo. Por ejemplo, si un usuario está realizando una transferencia a través de la página web de su banco, estas variantes pueden modificar los datos del receptor de dicha transferencia una vez enviada la petición. Además el resultado que se le devuelve al usuario sería con los datos originales, por lo que el usuario no se daría cuenta de la estafa.

Otras variantes consultan al servidor para saber si deben realizar alguna acción en función de las páginas que el usuario está visitando. De esta forma no depende de un fichero de configuración y el ciberdelincuente puede ampliar o modificar la lista de sitios web de las que quiere robar información, inyectar código, etc.

Una vez que roban la información, suele enviarla a través de correo electrónico o se sube a un servidor FTP.

6.- Crimen organizado

En contra de lo que se puede pensar que el ciberdelincuente que crea el troyano bancario es el que roba la información confidencial de los usuarios para posteriormente robarles el dinero, la realidad es bien distinta y el entramado que hay detrás de este negocio es bastante complejo.

El siguiente gráfico ilustra de forma esquemática el proceso más habitual que hay detrás de este negocio tan lucrativo:

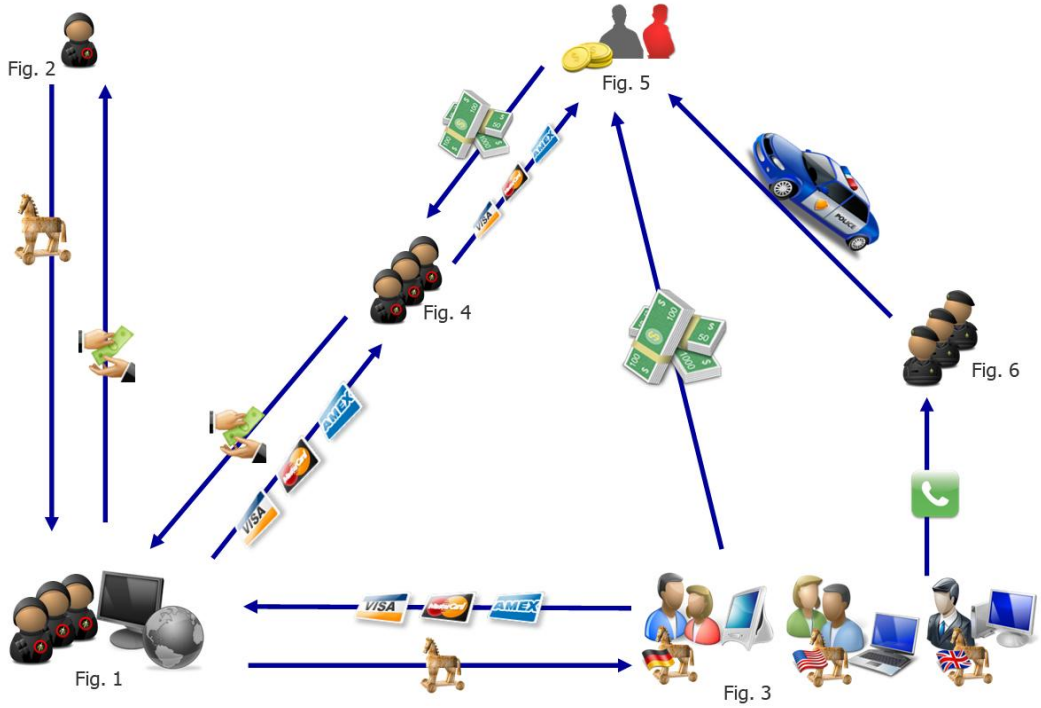

Fig.3 Representación del crimen organizado

Como se puede observar, no se trata de una única persona la que distribuye un troyano bancario para conseguir los datos bancarios de los usuarios y así robarles el dinero. Es mucho más complejo que todo eso y hay todo un negocio detrás de ello.

Vamos a explicar en qué consiste este entramado.

En primer lugar, un grupo de ciberdelincuentes (figura 1) solicita oencarga en foros especializados o en el propio mercado del malware (figura 2) un troyano diseñado a la carta con determinadas características e incluso también podría alquilar toda la infraestructura necesaria para distribuir ese troyano, bien mediante spam o mediante servidores de malware que infectan por el método conocido como drive-by-download. Esta técnica permite la descarga automática de un fichero sin conocimiento del usuario aprovechando posibles vulnerabilidades en el ordenador.

Una vez que tienen el troyano, lo distribuyen a los usuarios con el objetivo de conseguir sus datos bancarios (figura 3). Para ello, los métodos más habituales de distribución de los troyanos son los mensajes de spam o bien infectando páginas web.

Esta técnica de infección de páginas web legítimas consiste en modificar el código fuente de dichas páginas web, añadiendo una referencia de tipo iframe que apunta a un servidor malicioso. Ver anexo (páginas web legales en jaque)

Estos ciberdelincuentes no roban directamente el dinero a los usuarios sino que les roban los datos bancarios y se ponen en contacto con otros ciberdelincuentes (figura 4) a los que les ofrecen los datos a cambio de dinero. De esta manera, hacen negocio pero evitan que les puedan seguir el rastro.

Todos los datos robados se venden en el mercado del malware. Sin embargo, tampoco los que compran los datos bancarios robados son los que roban el dinero a las víctimas. Para evitar que se pueda seguir la pista de los ciberdelincuentes, contratan otras personas como intermediarios, se trata de los muleros (figura 5). Estas personas son contratadas bajo el pretexto de ofertas de trabajo desde casa.

El dinero robado se transfiere a las cuentas de los muleros, ellos se quedan con un porcentaje de ese dinero, normalmente en torno al 3-5% y después de sus cuentas se transfieren a través de un sistema de pago o de envío de dinero anónimo, para pasar a manos de los ciberdelincuentes. Utilizan un sistema de pago/de envío de dinero anónimo para que no puedan ser localizados.

En caso de que las víctimas del robo denuncien los hechos a la policía y se inicie la investigación, en principio los únicos que han dejado un rastro son los muleros.

De esta manera todos salen ganando excepto los propios usuarios afectados y los muleros, ya que en caso de que la policía investigue, serán los que figuren como los ladrones.

7.- Los ejemplares más destacados

En esta sección, vamos a incluir los ejemplares de malware bancario más destacados bien por sus características o por los mensajes de correo electrónico en los que han sido distribuidos.

BANCOKILL.A

BancoKill.A, detectado en agosto de 2007, fue distribuido en un mensaje de correo electrónico en el que se informaba de una supuesta colaboración entre Panda Software y cierto banco mexicano para proteger a sus clientes frente a posibles amenazas.

El mensaje no puede ser más engañoso, puesto que se ofrece a los usuarios una herramienta para protegerles de las amenazas y diseñada especialmente para cierta entidad bancaria. Sin embargo, todos los usuarios que intenten descargarse dicha herramienta de protección estarán introduciendo precisamente un troyano diseñado para robar los datos bancarios de la entidad bancaria colaboradora.

El mensaje en el que se distribuía era el siguiente:

Fig.4 Mensaje en el que se distribuía BancoKill.A

A pesar de que Panda Security (antes Panda Software) mantiene colaboraciones con las entidades bancarias para proteger a sus usuarios de estas amenazas, en este caso, se trata de una técnica de ingeniería social utilizada por los ciberdelincuentes para engañar a los usuarios.

BANBRA.FTI

Banbra.FTI, detectado en mayo de 2008, se trata de un troyano que llega al ordenador haciéndose pasar por una imagen que muestra un recibo bancario. Cuando el archivo es ejecutado, a pesar de que muestra la imagen del recibo bancario, en un segundo plano se estará ejecutando el archivo malicioso en el ordenador del usuario.

Mediante esta técnica, se consigue desviar la atención del usuario hacia la imagen y que no sospeche que además se ha ejecutado un troyano.

Para conseguir información bancaria del usuario, este troyano habilita la opción de guardar las contraseñas introducidas en el navegador de Internet Explorer. Una vez habilitada, accede al directorio en el que se almacenan las contraseñas y roba aquellas relacionadas con entidades bancarias. Después, envía estos datos a su creador a través de correo electrónico.

BANKER.LAX

Uno de los elementos de seguridad que las entidades bancarias han facilitado a los usuarios de banca electrónica para dificultar el robo de información bancaria por parte de los ciberdelincuentes son las tarjetas de coordenadas. Se trata de tarjetas que contienen un conjunto de claves, unas sesenta aproximadamente.

Gracias a estar tarjetas, aunque un ciberdelincuente obtenga la clave de acceso de un usuario no podrá realizar ningún movimiento en sus cuentas, ya que además se solicita una segunda clave seleccionada aleatoriamente de la tarjeta de coordenadas.

El problema comienza cuando un ciberdelincuente diseña un troyano que solicita al usuario todas las claves de su tarjeta de coordenadas, tal es el caso del Banker.LAX.

Este troyano cuenta con un listado de direcciones web de entidades bancarias a monitorizar. Cuando el usuario accede a la página web que coincide con las de su lista, es redirigido a una página que imita a la original.

En la página maliciosa se solicitan las contraseñas de inicio de sesión del usuario. Una vez introducidas, se abre una página en la que se solicitan las claves de la tarjeta de coordenadas del usuario:

Fig.5 Tarjeta de coordenadas mostrada por el troyano

Si el usuario introduce todas las claves de su tarjeta de coordenadas, estas pasarían a manos del ciberdelincuente, permitiéndole acceder libremente a las cuentas del usuario.

Y es que a un usuario de banca electrónica solo le solicitarán una combinación aleatoria de la tarjeta de coordenadas para autenticarse, nunca todas las claves, porque la eficacia de esta tarjeta reside precisamente en que las posibles combinaciones de claves son muy elevadas.

BANBRA.FUD

Banbra.FUD, detectado en junio de 2008, llega al ordenador simulando ser un acceso a una página web de Internet Explorer. Sin embargo, si es ejecutado, se instalará un troyano en el ordenador afectado.

Este troyano está diseñado no solo para robar información bancaria sino también información del ordenador, como nombre del equipo, dirección IP o versión del sistema operativo.

Para obtener los datos, monitoriza la navegación del usuario y cuando se registra en la página web de ciertas entidades bancarias brasileñas, muestra un mensaje de error y abre una página web falsa que imita a la original.

En esta falsa página web se vuelven a solicitar los datos de acceso del usuario, así como una serie de datos de la tarjeta de coordenadas. Toda la información que el usuario introduzca será registrada y enviada a su creador.

Los ciberdelincuentes suelen recurrir a la técnica de crear páginas web que imitan a las páginas web legítimas de los bancos para conseguir que los usuarios no sospechen. Sin embargo, normalmente estas páginas falsificadas se diferencian en algunos aspectos de la original, ya que suelen solicitar más información de lo habitual. Este detalle es importante a la hora de desconfiar de estas páginas web.

BANBRA.FXT

Banbra.FXT, detectado en julio de 2008, es un troyano diseñado para afectar a usuarios brasileños ya que se distribuye en un mensaje que se hace pasar por una notificación del Ministerio Público Federal de Brasil. En dicha notificación se solicita la comparecencia del usuario por un tema que se detalla en un documento adjunto.

La curiosidad o incertidumbre de un usuario al que le llegue este mensaje puede llevarle a ejecutar el archivo adjunto y a introducir un troyano en su ordenador.

Una vez instalado, este troyano monitoriza la navegación del usuario y cuando accede a las páginas web correspondientes a ciertas entidades bancarias brasileñas, registra la información que el usuario introduzca en ella, obteniendo sus claves bancarias.

BANKER.LGC

Banker.LGC, detectado en julio de 2008, tiene como objetivo los usuarios de cierta entidad bancaria española. Utiliza una noticia impactante y morbosa para engañar a los usuarios: un supuesto accidente de tráfico del piloto de Fórmula 1 Fernando Alonso. El mensaje contiene una breve noticia y un vídeo en el que se ve una imagen de dos coches en llamas, imagen que supuestamente se corresponde con el accidente.

Se trata de una noticia que despierta gran expectación en los usuarios que no dudarán en ver el video. Además, el mensaje parece enviado por El País por lo que el usuario en principio no sospecharía de que se trata de una noticia falsa.

La noticia es la siguiente:

Fig.6 Noticia sobre el supuesto accidente de Fernando Alonso

Si el usuario pulsa sobre el video para verlo, no visualizará el vídeo sino que se descargará una copia del troyano en el ordenador.

Este tipo de noticias tan impactantes o morbosas buscan despertar una enorme curiosidad en los usuarios para que se sientan tentados en ver la noticia y no se fijen en otros detalles que podrían alertarles sobre la dudosa veracidad de la noticia.

SINOWAL.VTJ

Algunas variantes de troyanos bancarios se distribuyen en correos electrónicos que pretenden amedrentar a los usuarios con amenazas falsas para conseguir que ejecuten un archivo o pulsen algún enlace.

En el mensaje en el que se distribuye Sinowal.VTJ, detectado en septiembre de 2008, una persona anónima recrimina al usuario diciendo que ha recibido mensajes con virus enviados desde su dirección de correo y amenaza con avisar a la policía si no deja de recibir estos mensajes.

Además, engaña al usuario diciendo que tiene una prueba que demuestra el envío de dichos mensajes y le solicita que imprima el documento que se adjunta en el mensaje y se lo envíe a su ISP (Internet Service Provider) para que solucione el problema.

El mensaje tiene un archivo adjunto que supuestamente contiene las pruebas. En realidad, lo que contiene es una copia del troyano.

BANBRA.GBQ

Otra de las artimañas que utilizan estos ejemplares consiste en hacerse pasar por un documento aparentemente inofensivo, como puede ser un Word, un Excel o un pdf. El problema es que en realidad se trata de archivos exe camuflados, ya que aunque tienen doble extensión (doc y exe), normalmente los troyanos se encargan de ocultar la extensión para que el usuario confíe en los archivos.

Tal es el caso de Banbra.GBQ, detectado en octubre de 2008, que llega al ordenador con un icono de un documento Word. Cuando el usuario lo ejecuta, se abre el siguiente documento, que parece una notificación enviada por un organismo oficial:

TRIBUNAL REGIONA ELEITORAL

São Paulo 01/10/2008

Caro senhor Geraldo Matias dos Santos,
Vimos por meio dessa, intima-lo a comparecer ao Tribunal Regional Eleitoral mais próximo de sua cidade para esclarecer o porque de não ter respondido a convocação para trabalhar de mesário nas eleições para prefeito de sua cidade no ano de 2008.
Lembrando que a participação nas eleições além de ser um ato de cidadania, é também obrigatório por lei, sendo que a pena pelo não comparecimento é de multa de 150 ufirs.

Aguardamos justificativa pelo fato ocorrido.

Sem mais para o momento

Fig.7 Notificación enviada por un supuesto organismo oficial

Mientras el usuario está leyendo la notificación, el troyano se instalará en el ordenador, sin que el usuario sospeche nada.

BANKER.LLN

Este troyano bancario se detectó poco después de que Barack Obama fuera elegido presidente de los Estados Unidos. En concreto Banker.LLN está diseñado para robar las claves de acceso de los usuarios de cierta entidad bancaria peruana. Para ello, previamente modifica el archivo HOSTS, de tal manera que si el usuario accede a la página web de dicha entidad bancaria peruana, es redirigido a otra que imita a la original.

Si el usuario introduce sus datos bancarios, estos serán capturados por el troyano y enviados a su creador.

Llega al ordenador en un archivo con el nombre BARACKOBAMA.EXE y el icono de la bandera de Estados Unidos:

Fig.8 Icono y nombre del archivo

BANBRA.GDB

Una de las limitaciones de los troyanos bancarios es que no tienen la funcionalidad de propagarse por sí mismos. Normalmente suelen ser distribuidos en mensajes de spam, pero para ello es necesaria la intervención de un ciberdelincuente.

Sin embargo, se han detectado algunas variantes de familias de malware bancario que tienen la funcionalidad principal de los gusanos, que es la de propagarse. Tal es el caso del W32/Banbra.GDB.worm. Este gusano se distribuye en dos tipos de mensajes con una temática diferente.

Uno de ellos parece provenir del departamento de investigación de delitos informáticos:

Fig.9 Uno de los mensajes en los que se distribuye Banbra.GDB

También se distribuye en un mensaje que utiliza como remitente el propio usuario infectado y que trata sobre la amistad y el amor.

Ambos mensajes contienen un enlace que si se pulsa lleva a una página web en la que se descarga una copia del malware.

BANKERFOX.A

El navegador más aprovechado para realizar este tipo de delitos informáticos es Internet Explorer. Esto de sebe principalmente a su uso tan extendido. Sin embargo, otros navegadores poco a poco están ganando terreno y cada vez más usuarios los utilizan, tal es el caso de Firefox.

Conscientes de ello, los ciberdelincuentes ya han diseñado un troyano para este navegador, se trata de BankerFox.A, detectado en diciembre de 2008.

Aunque el modus operandi de este troyano no es muy diferente al habitual, sorprende el número de países y entidades bancarias afectadas. Algunos de los países afectados son España, Italia, Reino Unido, Francia, Estados Unidos y Australia.

En cuanto a su funcionamiento, el troyano cuenta con un listado de páginas web correspondientes a entidades bancarias de diferentes países. Monitoriza la navegación del usuario con el navegador Firefox y cuando el usuario visita alguna de las páginas web afectadas, el troyano se activa y registra la información introducida en ella.

SINOWAL.VXR

Sinowal.VXR, detectado en diciembre de 2008, está diseñado para robar información confidencial relacionada con ciertas entidades bancarias británicas. Se activa cuando el usuario accede a la página web de alguna de las entidades bancarias afectadas.

Cuando el usuario va a registrarse, muestra una página web falsa que contiene un formulario en el que además del nombre de usuario y contraseña de acceso, requiere que responda a una serie de preguntas personales bajo el pretexto de que se trata de una medida de seguridad. Preguntas como cuál es su comida o restaurante favorito, el nombre de un lugar memorable o su película favorita.

Tantas preguntas personales deberían hacer sospechar a los usuarios y hacerles desconfiar de esta página web.

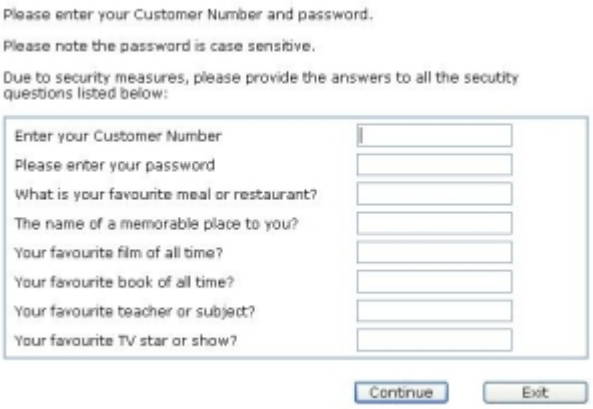

Fig.10 Información solicitada para autenticarse

8.- Recomendaciones

Los mensajes de spam continúan siendo una asignatura pendiente para los usuarios a la hora de evitar la instalación de malware en sus ordenadores. En ocasiones, el contenido de ciertos mensajes que por ejemplo utilizan logotipos conocidos puede llevar a los usuarios a confiar equivocadamente de los mismos.

Sin embargo, muchos otros mensajes presentan una serie de características como faltas de ortografía o información incoherente, que debería frenar la tentación de los usuarios de ejecutar archivos o hacer clic en enlaces.

En el caso de los mensajes que contienen archivos adjuntos es importante que antes de ejecutarlos, el usuario lo analice con una solución antivirus para comprobar si contiene malware.

Si se trata de enlaces a páginas web, antes de pulsar el enlace, es recomendable situar el cursor sobre el enlace para comprobar si el enlace que se indica a través del cursor es el mismo que el proporcionado en el mensaje. Y es que en muchas ocasiones, los enlaces que se incluyen en los mensajes están camuflados y en realidad apuntan a una dirección maliciosa desde la que se descargaría el malware.

Por otra parte, los ciberdelincuentes utilizan la infección de páginas web legales para introducir troyanos bancarios en los sistemas de los usuarios. Para ello, es importante tener los sistemas correctamente actualizados y parcheados para evitar que se pueda explotar alguna vulnerabilidad en sus ordenadores.

09.- Anexo

En la introducción y en el apartado Crimen organizado mencionamos que es relativamente sencillo crear troyanos bancarios gracias a los denominados kits bancarios.

Un ejemplo de estos kits es el Zeus.

ZEUS CRIMEWARE KIT

Se trata de un kit bancario que permite crear troyanos pertenecientes a la familia Sinowal.

Cualquiera en la comunidad criminal puede comprar este kit bancario al que suelen referirse con el nombre de Zeus por unos 700 dólares.

El kit consta de tres partes:

- Bot (troyano).
- Panel de control web.
- Generador de troyanos.

El troyano es el programa que se ejecutara en el ordenador del usuario afectado y puede realizar las siguientes acciones:

- Servidor de sockets y Proxy.
- Auto-actualizarse.
- Usar un encriptador polimórfico, lo que le permite generar diferentes copias de sí mismo.
- Capturar certificados.
- Cambiar las DNS locales.
- Borrar cookies para forzar al usuario a introducir de nuevo las contraseñas.
- Realizar capturas de pantalla de las máquinas infectadas.
- Recibir órdenes de control remoto.
- Añadir campos adicionales a un sitio web y monitorizar los datos que envía.
- Robar contraseñas almacenadas de diversos programas, como datos de Protected Storage y contraseñas pop3 y ftp independientemente del puerto.

Envía la siguiente información de los ordenadores infectados:

- Versión del sistema operativo.
- Service Pack.
- Idioma.

El troyano introduce hooks en ciertas funciones de la API de Windows con el fin de interceptarlas. Estos hooks permiten conocer las páginas solicitadas por cualquier navegador que haga uso de la API de Windows. Dichas peticiones son comparadas con una lista de entidades a monitorizar que el troyano descarga del servidor.

En el momento en que se detecta una coincidencia total o parcial entre las peticiones del navegador y las cadenas de monitorización se activa el mecanismo de robo de las credenciales.
Los hooks introducidos en las funciones de la API también permiten interceptar tráfico de red, redirigir tráfico, capturar datos introducidos en formularios y registrar las teclas pulsadas una vez se detecta la visita de una entidad monitorizada.

El panel de control web permite controlar y gestionar toda la botnet. A través del panel de control puede realizar las siguientes acciones, entre otras:

- Consultar estadísticas de infección.
- Consultar los archivos subidos.
- Buscar los registros de información almacenados.

El generador de troyanos permite configurar y crear los ejemplares de malware. Cuenta con diferentes opciones de configuración:

StaticConfig
botnet – Nombre de la botnet. Por defecto suele ser "btn1"

timer_config - define el intervalo de tiempo para obtener la configuración.

timer_logs - define el intervalo de tiempo que transcurre para enviar los logs al servidor.

timer_stats - define cada cuánto tiempo se envían las estadísticas al servidor.

url_config - URL en la que se encuentra el archivo de configuración principal en el servidor.

url_compip - determina el sitio donde se puede comprobar la dirección IP del ordenador.

blacklist_languages - determina la lista de códigos de lenguaje de Windows, por ejemplo, RU - 1049, EN - 1033.

DynamicConfig,

url_loader – determina la URL, de la que se puede descargar la actualización del bot.
url_server - determina la URL a la que se enviarán las estadísticas, archivos, logs, etc de los ordenadores infectados.

file_webinjects – especifica el nombre del archivo que contiene el listado de las URLs en las que se inyectarán campos adicionales.

AdvancedConfigs – enumera una lista de URLs de las que se puede descargar un backup de la configuración del archivo.

WebFilters – URLs de sitios web a monitorizar.

WebFakes – enumera una lista de direcciones que redireccionan a sitios web falsos. Hay que especificar primero la dirección del banco original y después dónde se encuentra la página falsa que sustituirá a la del banco.

TanGrabber - URLs de bancos a monitorizar.

DnsMap - Lista de urls e IP asociada a añadir en el archivo: %SystemRoot%\Drivers\etc\hosts.

10.- Referencias

Blog Panda Research

http://research.pandasecurity.com/archive/Banking-Trojans-I.aspx

http://research.pandasecurity.com/archive/Banking-Trojans-II.aspx

http://research.pandasecurity.com/archive/Banking-Trojans-III.aspx

Enciclopedia de malware

http://www.pandasecurity.com/spain/homeusers/security-info/

Pharming

http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

Notas de prensa

http://www.pandasecurity.com/spain/homeusers/media/press-releases/viewnews?noticia=9289

Ataques iframe

http://www.pandasecurity.com/img/enc/Boletines%20PandaLabs_1_Pag_Web_legales_jaque.pdf