

II CAMPAÑA CONTRA EL FRAUDE ONLINE Y POR LA SEGURIDAD EN LA RED.

Como funciona un troyano bancario en el ordenador de una victima. (II Parte)

Hace unos días la Comisión de Seguridad de la Asociación de Internautas informó sobre el descubrimiento de un nuevo troyano bancario (el segundo detectado en menos de mes) y donde se realizó un primer análisis del mismo hasta llegar al descubrimiento de las entidades financieras afectas y donde van los datos robados. En este segundo artículo se describe como funciona un troyano bancario pero desde el ordenador de una victima, en el se analizan los dos troyanos bancarios detectados que afectan a entidades financieras españolas y brasileñas.

Antes de empezar el artículo queremos advertir que hay datos que se omiten por motivos de seguridad y también queremos recalcar que las entidades bancarias que mostramos en este artículo son unas de tantas que son afectadas por este tipo de malware, no se piense que por ser cliente de estas entidades bancarias serán víctimas de este robo de claves todo lo contrario, todas las entidades pueden ser víctimas, afortunadamente los clientes de estos dos bancos podrán comprobar, aprender y detectar su funcionamiento, por último también queremos avisar que este tipo de **troyano bancario son de nueva generación**, no son los clásicos troyanos que superponen imágenes encima de las reales y con mover cualquier tipo de ventana podemos ver que es falso, el troyano funciona con todos los navegadores.

Herramientas usadas en el laboratorio de pruebas malware:

- Maquina de análisis forense.
- Sniffer de tráfico en la red.
- Herramienta de procesos activos.
- Cortafuegos.

Pasos realizados en la dos demos:

- Ejecutamos el primer troyano downloader o el troyano principal.
- Capturamos los paquetes (información) que envía al exterior.
- Comprobamos los procesos activos que hay en nuestro sistema.
- Demostramos como cambia nuestro navegador.

Troyano bancario que afecta entidades bancarias españolas. Como funciona el troyano en el ordenador de una victima.



Ver video: [TROYANO BANCARIO ESPAÑOL.](#)

- 1.- Ejecutamos el troyano bancario.
- 2.- El cortafuego nos solicita permiso y comprobamos los nuevos procesos.
- 3.- Capturamos los primeros paquetes enviados por el troyano bancario, el troyano manda un correo electrónico alertando que hay una víctima que esta infectada, también detectamos la dirección del correo donde van los datos (dato muy importante).
- 4.- Vemos como actúa el troyano cuando queremos trabajar con una entidad bancaria, nos muestra el candado de seguridad conexión segura y el certificado de autenticidad, pero nos cambia las imágenes de nuestro navegador.
- 5.- El troyano nos solicita todas las claves, recuerde estas claves NO SE TIENE QUE TECLEAR SI NO REALIZA ALGUNA OPERACIÓN, tecleamos unas claves ficticias.
- 6.- Una vez tecleadas las claves, el troyano nos muestra un falso mensaje; no se puede conectar al servidor.
- 7.- El cortafuego nos solicita de nuevo permiso, el troyano quiere enviar de nuevo información, le damos permiso para que envíe los datos. Capturamos los paquetes enviados y vemos que envió TODAS LAS CLAVES TECLEADAS, en este paso también localizamos en que carpeta se queda alojado el troyano bancario.
- 8.- Matamos el proceso del troyano para ver que ocurre cuando no está activo.
- 9.- Operamos de nuevo con la web de la entidad bancaria.
- 10.- Comprobamos que ahora no solicita todas las claves.
- 11.- Activamos de nuevo el troyano para ver el efecto, cuando está activo el cortafuego nos solicita de nuevo permiso para enviar datos.
- 12.- Vemos claramente como nos cambia la web bancaria y como nos vuelve a solicitar todos las claves.

Por último para comprobar mejor el efecto trampa tecleamos en el navegador la web de seguridad de Asociación de Internautas <http://seguridad.internautas.org>, carga la web en el navegador PERO NO LA MUESTRA, matamos de nuevo el proceso del troyano bancario para comprobar como se quita de nuestro navegador el efecto trampa.

Final.

Nota este troyano analizado afecta a: **Banesto, Grupo Santander, Caixa de Catalunya, EPAGADO, Kutxa Caja Gipuzkoa San Sebastian, La Caixa.**

Más información sobre este troyano bancario:

Troyano bancario que afecta entidades bancarias brasileñas. Como funciona el troyano en el ordenador de una victima.

Ver video: [TROYANO BANCARIO BRASILEÑO.](#)

- 1.- Ejecutamos el troyano bancario que viene en una falsa tarjeta online.
 - 2.- El troyano quiere mostrarnos una web para hacer creer que es la postal online, a su vez descarga un segundo troyano mas potente y se ejecuta de forma silenciosa. Todo esto ocurre mientras la victima contempla la teórica tarjeta online
 - 3.- Comprobamos los procesos activos en nuestra maquina y vemos que el nuevo troyano ya esta ejecutado y trabajando.
 - 4.- Localizamos el nuevo troyano en la carpeta Windows/system32.
 - 5.- Vemos los pasos del troyano y sus conexiones gracias al trafico capturado.
 - 6.- Trabajos con una entidad afectada por este troyano bancario.
 - 7.- Podemos ver el candado de seguridad y su certificación valido.
 - 8.- Tecleamos claves ficticias y nos pide todas las claves de operaciones, recuerde estas claves nunca se solicitan al entrar a su entidad bancaria.
 - 9.- El cortafuegos nos alerta que el troyano quiere enviar conectarse al exterior.
 - 10.- Una vez tecleadas todas las claves en la web nos muestran un mensaje que lo intentemos mas tarde.
 - 11.- Comprobamos el trafico enviado desde nuestra maquina y el troyano envió por correo electrónico todas las claves tecleadas en la web, de paso acabamos de descubrir donde van estos datos robados.
 - 12.- Para ver el efecto que realiza el troyano, tecleamos en nuestro navegador la web de la Comisión de Seguridad de la Asociación de Internautas <http://seguridad.internautas.org>.
 - 13.-La web se carga y se claramente el efecto trampa.
 - 14.- Matamos el proceso para ver que ocurre.
 - 15.- Destapamos al troyano bancario.
- Final.

Mas información sobre este troyano bancario:

<http://seguridad.internautas.org/html/4185.html>

Nota: Estos troyanos fueron solicitados por algunas entidades bancarias a la Comisión de Seguridad de la Asociación de Internautas para un estudio mas profundo.

En este artículo se muestra de forma rápida como trabaja los troyanos bancarios de nueva generación.

Referencias:

[-Tarjeta online falsa que contiene un troyano bancario que afecta entidades financieras españolas.](#)

[-Detectado nuevo troyano bancario que afecta a varias entidades bancarias. \(Análisis del troyano 1ª parte\)](#)

Comisión de Seguridad en la Red.

José María Luque Guerrero

<http://seguridad.internautas.org> - www.seguridadenlared.org - www.seguridadpymes.es

Asociación de Internautas. www.internautas.org

Fecha artículo: 2007-04-29 23:40:15 - url artículo: <http://www.internautas.org/html/4189.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org