

Troyano bancario.

Falsa actualización de Java que contiene troyano bancario.

Una vez mas tenemos que hablar de un malware que afecta entidades financieras. En este reiterado intento de fraude en linea, simulan una actualización de Java, en el siguiente análisis se muestra las entidades afectadas y donde van los datos obtenidos.

El servidor analizado hospeda distintos troyanos, destacamos uno que afecta teléfonos móviles.

Advertimos que algunos de los malware no son detectados por los antivirus y donde los ciber-delincuentes intentaron ponerlo mas difícil para obtener un análisis y funcionamiento.

En el siguiente análisis se omiten varios datos por motivos de seguridad.

La forma de llegar este nuevo troyano es por medio del **clásico correo electrónico** (método que muchos expertos en seguridad informática comentaban que estaba anticuado y en desuso, menos mal..., lo que esta claro que aun funciona) que simula ser una actualización de Java.

Si una victima del engaño ejecuta la falsa actualización empieza en su maquina el mecanismo de nueva descarga de un nuevo troyano.

El primer troyano tiene el siguiente nombre:
install_javav6up2.exe de 188 KB. (comprimido)

De la familia downloader, esto quiero decir que realiza una nueva descarga de un servidor que contiene el malware principal.

Realiza la nueva descarga y ejecución del nuevo troyano bancario que se llama:
source.exe de 961 KB. (comprimido)

Lo primero que realiza el troyano bancario es añadir una línea en el registro para que se ejecute cada vez que se encienda la maquina afectada, de esta forma el troyano se ejecuta siempre,:

Registro de Windows:\\HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\

El segundo paso es enviar un correo electrónico para avisar al delincuente que hay una nueva victima del troyano bancario, el correo es enviado a:

overalltheam@gmail.com>

220 mx.google.com ESMTP 7si903033wrh
EHLO MAQUINA AFECTADA
250-mx.google.com at your service, [IP]
250-SIZE 28311552
250-8BITMIME
250 ENHANCEDSTATUSCODES
RSET
250 2.1.0 Flushed 7si903033wrh
MAIL FROM:
250 2.1.0 OK
RCPT TO:**overalltheam@gmail.com>**
250 2.1.5 OK
DATA
354 Go ahead
From: "overall~"
Subject: De: MAQUINA AFECTADA
To: overalltheam@gmail.com
Date:
X-Priority: 3
X-Library: Indy 9.00.10

Thundercats again!

.
250 2.0.0 OK 1180814264 7si903033wrh
QUIT
221 2.0.0 mx.google.com closing connection 7si903033wrh

El troyano ya esta preparado para modificar nuestro navegador cada vez que visitemos las web de entidades bancarias afectadas por este troyano, advertimos que este troyano puede afectar a todas las entidades, solo depende del delincuente como lo programe.

Continuamos con el análisis del malware y vemos algunas de las entidades afectadas;

www.unibanco.com.br
www.nossacaixa.com.br
www.santanderbanespa.com.br
www.bradesco.com.br

Las siguientes imágenes son extraídas del troyano bancario, esta suplantan en nuestro navegador la imagen real de la entidad bancaria, el grave problema de estos troyanos es que la falsificación es conseguida al 100% ;

Una victima al visitar o trabajar con las entidades afectadas, al teclear sus datos y claves serán enviados de forma transparente para la victima al siguiente correo electrónico:

overalltheam@gmail.com

Consejos y advertencias:

Si usted recibe un correo de un extraño, un correo no deseado, incluso este tipo de tarjetas les recomendamos la máxima prudencia y si es posible no haga caso de este tipo de correos electrónico y NUNCA pulsar sobre los enlaces que contiene.

La mayoría de los antivirus no detecta este tipo de ficheros malware.

Mas datos sobre troyanos bancarios;

Como funciona un troyano bancario en el ordenador de una victima:

<http://seguridad.internautas.org/html/4189.html>

Análisis del troyano: <http://seguridad.internautas.org/html/4185.html>

Como funciona un troyano bancario en el ordenador de una victima, Internautas Televisión:

<http://www.internautas.tv/?tv=100>

Agradecemos a todos los intenautas que nos alertaron de este nuevo malware y en especial a Lostmon que realizo una análisis previo.

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: 2007-06-03 13:04:04 - url artículo: <http://www.internautas.org/html/4238.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