

Pharming bancario, un caso real y activo.

Uno de los peligros más importantes para los usuarios de Internet es el pharming y consiste en la manipulación de las direcciones DNS en la maquina de un usuario, una simple modificación en nuestro fichero host puede engañarnos y conseguir que ciertas web que visitemos no sean realmente las originales.

Ejemplo de falsificación;

```
209.85.171.83 hotmail.com >> %windir%\system32\drivers\etc\hosts
```

Si tecleamos en nuestro navegador la url Hotmail nos enviara a la web de Google.

Después de ver el ejemplo podemos ser conscientes del alcance de peligrosidad de esta modalidad, por ello la Comisión de Seguridad de la Asociación de Internautas prefiere alerta y informar a todos aquellos usuarios que aun desconocen este tipo de peligros reales en al red y no entrar en la clásica dinámica del ocultismo para dar una sensación de seguridad , uno de los grandes pecados de la seguridad informática en estos tiempos, la falsa seguridad se convierte en inseguridad.

La Comisión de Seguridad Informática de la Asociación de Internautas en colaboración de miles de usuarios que colaboran diariamente en la lucha contra el fraude, detecto hace semanas un caso de Pharming bancario, como era normal se esperaba que el cierre de este caso fuera inmediato o pocas horas, desgraciadamente esto no ocurre, por mucho que algunos galácticos representantes de seguridad de información de ciertos estamentos públicos repiten y repiten que cuando ocurre este tipo de casos o similares los perjudicados conocen el problema, cosa que no parece muy cierta, algunos pequeños ejemplos:

[Phishing al DNI Electrónico.](#)

[Agencia Tributaria se olvidó borrar los servidores de prueba.](#)

La mayoría de las entidades bancarias españolas pueden confirmarlo diariamente, donde agradecen la información reportada.

Dejando a un lado el pequeño tiron de orejas sobre la sensación de seguridad produciéndose una gran inseguridad, el estudio y análisis diario de servidores fraudulentos dio fruto del descubrimiento de esta modalidad de pharming ya que la mayoría de los casos conocidos se producen por infección de troyanos o malware.

El caso detectado simula la recepción de una tarjeta de felicitación o la dirección web para que veamos la tarjeta, al pulsar sobre los enlace nos conduce a un servidor trampa, las siguientes imágenes son de un ejemplo real y activo;

Durante la visualización del mensaje se produce la descarga del fichero malicioso encargado de modificar el fichero HOST de la victima:

Este fichero nos modifica el fichero HOST de nuestra maquina, el fichero HOST se puede localizar en;

Windows NT/2000: C:\WINNT\System32\drivers\etc\hosts

Windows XP: C:\WINDOWS\system32\drivers\etc\hosts

Windows 2003: C:\WINDOWS\system32\drivers\etc\hosts

Windows Vista: C:\WINDOWS\system32\drivers\etc\hosts

Unix (en general): /etc/hosts

Linux (en general): /etc/hosts

MacOS (en general): /etc/hosts

Puede variar si la configuración de la maquina fue realizada de forma personalizada.

Tras la modificación de nuestro fichero HOST producida por el malware, cada vez que tecleemos en nuestro navegador la url banamex.com.mx o las mostrada en la imagen anterior nos enviara a un servidor que suplanta la imagen de la entidad afectada;

Aunque el ejemplo sea de una entidad financiera de Méjico recordamos que existen mensualmente varios cosas de pharming de entidades españolas.

Estructura del servidor trampa;

Como siempre la Asociación de Internautas recomienda que no se pulse sobre enlaces de correos de desconocidos o enlaces enviados por mensajería instantánea y nunca faciliten sus datos a terceros.

Dirección electrónica si quiere denunciar web trampa o sospechosas de malware, robo de identidad, etc; phishing@internautas.org

Pregunta en el aire; ¿Quiénes son los responsables de informar a la comunidad internauta sobre estos peligros y denunciar ante la justicia este tipo de sitios web para su cierre inmediato?

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: 2008-07-09 10:25:36 - url artículo: <http://www.internautas.org/html/4391.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