

Creadores de Fraudes

## Creadores de phishing y pharming para dummy

**El crecimiento de malware o herramientas para realizar cualquier tipo de ataques-robos en la red están en crecimiento, este tipo de armas estaban solo disponible para individuos especializados, pero la comercialización y construcción de este tipo de herramientas ya están al alcance de cualquier persona, nos encontramos en la generación de creadores de fraudes para novatos.**

Se imagina encontrar publicidad en internet donde ponga; construya su propio phishing y gane dinero de forma rápida, ¿le parece irreal? Pues no lo es, existen este tipo de anuncios donde se pueden obtener por muy poco dinero o totalmente gratuito creadores para generar nuestro kit de fraude, en el siguiente estudio mostramos algunas herramientas que se utilizan para realizar este tipo de ataques fraudulentos en la red, el análisis de estos creadores de fraudes están enfocados en phishing y pharming, aunque muchos usuarios piensan que esta modalidad es anticuada y solo pican novatos la triste realidad demuestra lo contrario, el crecimiento de phishing y de estafadas es cada día mayor, pero no solo en esta modalidad, existen casos de personas que trabajan en el sector de seguridad informática donde sus ordenadores estaban infectados con malware que realizan ataques de denegación a web asiáticas, incluso personal de entidades bancarias que fueron víctimas de phishing, recuerden la ingeniería social hace que hasta el mas listo caiga en la trampa.

Una de las primeras web que encontramos nos ofrecen gratuitamente los kit montados para realizar nuestros ataques a distintas entidades financieras, donde solo debemos cambiar el correo electrónico donde van la claves de las víctimas, esta web esta operativa con otro nombre de dominio de la famosa **scam-2008.com**;

Lo único que tiene que hacer el delincuente es modificar los correos electrónicos del kit y subirlo al servidor trampa.

El siguiente servidor detectado nos ofrecen kit que afectan empresas españolas como **Paypal Spain, Ebankinter, ING Direct**, en el kit contiene el correo trampa que se envía a las víctimas y algunos pack de listas de correos electrónicos para realizar el ataque fraudulento, también herramientas para extraer cuentas mails de webs, resumiendo un tres por uno;

Ejemplo de listado de correos electrónicos incluidos en el kit:

La siguiente herramienta encontrada en esta investigación es un programa para generar nuestros phishing, existen dos versiones gratuitas, menos potentes y la de pago que te genera nuestra web trampa sin tener conocimientos en programación;

Durante la investigación nos encontramos una aplicación que es una joya por su facilidad y por el resultado final de las web fraudulentas generadas, basta decir que con solo dos clic de ratón podemos obtener una web fraudulenta para robar claves de mas de 20 sites web famosas, pero además se puede actualizar con plugins (plantillas) de nuevos sitios, tuvimos la fortuna de obtener la versión 3 de este producto:

Por ultimo analizamos una herramienta muy peligrosa, un generador de pharming, su función es generar un fichero que modifica los ficheros host de la victima para suplantar el sistema de resolución de nombres de dominio (DNS) y de esta manera conducir al usuario a una web fraudulenta, como anécdota de este tipo de ataques recuerdo durante una conferencia de Seguridad Informática en el 2006 en el parador de León, donde me negaron hablar de este tipo de fraudes (la inseguridad de la seguridad es no hablar de un hecho existente), cuando en realidad es uno de los mas peligrosos que puede ver junto a los nuevos troyanos bancarios, el generador o kit es básico pero a su vez letal, con solo teclear la dirección donde queremos que nuestra victima visite cuando teclee su entidad bancaria basta:

Durante la investigación se encontraron muchos mas herramientas y kit, pero en este articulo solo fueron analizadas las mas revelantes, la siguiente imagen muestra que existen muchas mas en el mercado del malware:

La conclusión de esta investigación; cualquier persona puede disponer de estas herramientas y realizar un fraude, el éxito del mismo será la ingeniería social usada, recuerden todos podemos ser víctimas, hasta los mas listos en seguridad.

### **Comisión de Seguridad en la Red.**

José María Luque Guerrero

<http://seguridad.internautas.org> - [www.seguridadenlared.org](http://www.seguridadenlared.org) - [www.seguridadpymes.es](http://www.seguridadpymes.es)

Asociación de Internautas. [www.internautas.org](http://www.internautas.org)

**Fecha artículo: 2008-04-13 11:59:41 - url artículo: <http://www.internautas.org/html/4348.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](mailto:asociacion@internautas.org)