Pharming

¿Qué es el “Pharming"?

El pharming es una modalidad de ataque utilizada por los delicuentes, que consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducirle a una página Web falsa. El atacante logra hacer esto, al alterar el proceso de traducción entre la URL de una página y su dirección IP.

Comúnmente el atacante realiza el redireccionamiento a las páginas web falsas a través de código malicioso. De esta forma, cuando se introduce un determinado nombre de dominio que haya sido cambiado, por ejemplo http://www.cibanco.com, en tu explorador de Internet, accederá a la página Web que el atacante haya especificado para ese nombre de dominio.

Para llevar a cabo el redireccionamiento a las páginas Web falsas o maliciosas, se requiere que el atacante logre instalar en su sistema alguna aplicación o programa malicioso (por ejemplo: un archivo ejecutable .exe, .zip, .rar, .doc, etc.). La entrada del código malicioso en su sistema, puede producirse a través de un correo electrónico, descargas por Internet o removibles (USB).

¿Cómo funciona el “Pharming”?

A través del envío masivo de correos electrónicos. El correo electrónico puede provenir de distintas fuentes, las cuales resultan llamativas para el usuario; algunos de los principales temas que se utilizan son los siguientes:

- **Noticias falsas o amarillistas**. En este tipo de correos los intrusos crean una noticia llamativa y, en la mayoría de las ocasiones, utilizan un tema actual y de interés general para la sociedad.
- **Envío de tarjetas postales electrónicas**. En este caso, el intruso enviará un correo invitando al usuario a abrir una postal que supuestamente le ha enviado un amigo.
- **Supuesta obtención de algún premio**. El intruso le enviará una serie de correos electrónicos, informándole que ha sido ganador de uno o varios premios (Autos, Dinero, Viajes, etc.), y le podrá solicitar información personal, números de cuentas bancarias, depósitos, etc.