Delitos informáticos: Pharming

Osvaldo Callegari
Analista de Sistemas
ocalle@ar.inter.net

A partir de ahora los usuarios de Internet tendremos que tener más cuidado a la hora de navegar por la Red, principalmente cuando realicemos transacciones económicas o compras on-line, ya que ha nacido un nuevo fraude cibernético que va aún más lejos de los ya anticuados correos de comprobación de contraseñas -phishing-, dando un paso más adelante y convirtiendo las descargas, correos electrónicos y navegación en un nuevo peligro que puede dar lugar a la manipulación de la resolución de nombres.

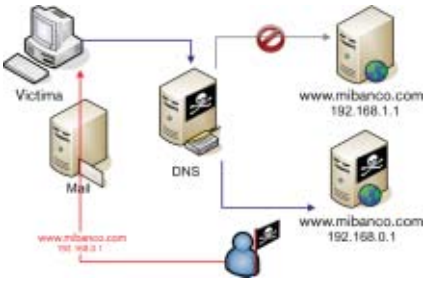
Introducción

Cuando parecía que cualquier usuario medio de Internet hacía caso omiso a los correos electrónicos provenientes de supuestas sucursales bancarias, en los que se solicitaba que el usuario incluyese sus contraseñas para intentar mejorar la seguridad del sistema, los delincuentes cibernéticos han encontrado otra forma para seguir haciendo crecer sus ingresos económicos y han originado, o pseudo-originado, un nuevo fraude informático: el *"Pharming"*, el cual resulta muy difícil de detectar y/o identificar, puesto que consiste en modificar el sistema de resolución de nombres de dominio, con lo que cada vez que introducimos una URL en nuestro ordenador para intentar acceder a una determinada página web -*tienda on-line o nuestro banco*- puede que estemos siendo víctimas del presente fraude sin ni siquiera darnos cuenta.

¿En qué consiste el pharming?

Se denomina *pharming* a la manipulación de la *"resolución de nombres en Internet"* producido por un código malicioso, normalmente en forma de troyano, que se ha introducido en el ordenador mientras realizámos una descarga, a través de correo electrónico (Spam), copia desde un CD-Rom, etc. Pero, *¿qué entendemos por resolución de nombres de Internet*? Se produce cuando introducimos la dirección de una página web, por ejemplo www.mibanco.com Esta dirección se traduce en un código numérico denominado dirección IP *(Internet Protocol)*, por ejemplo 192.168.1.1, denominándose a este proceso resolución de nombres, encargándose de esto las famosas DNS *(Domain Name Server)*.

Simplificando un poco el proceso antes comentado, el *pharming* consistiría en que, estando nuestro ordenador infectado por un troyano o programa que permita realizar los cambios en las DNS, nosotros intentaremos acceder a una página web introduciendo para ello la URL y, confiando en que esa es la web deseada, realizaríamos las compras o accesos a nuestras cuentas bancarias en una página falsa, con lo que finalmente los atacantes obtendrían nuestros códigos secretos y por ende la puerta abierta para cometer el fraude.



Diferencias entre phishing y pharming

Aunque aparentemente puedan parecer fraudes idénticos, el *pharming* va un paso más adelante, creando un grupo de usuarios vulnerables mucho mayor que en el *phishing*, ya que mientras en este último se necesita que se realice una acción aislada -que el usuario efectúe una operación bancaria accediendo a la página mediante un link que le proporcione el estafador-, en el *pharming*, sin embargo, el usuario intentará acceder directamente a la web de su banco o tienda on-line para evitar el ya conocido *phishing*, convirtiéndose en víctima del *pharming* aún adoptando todas las cautelas, ya que el estafador ha introducido un programa que modifica las DNS *(Domain Name Server)* y el acceso que se produce por el usuario es mediante un re-direccionamiento de la IP, diferente a la que en un principio deseábamos entrar.

Este tipo de estafa es mucho más peligrosa, porque la modificación de las DNS queda archivada en el ordenador, esperando el atacante a que el usuario acceda de nuevo, pudiendo atacar este fraude a un número mayor de usuarios.

Continúa en página 180

Anti-Pharming

Anti-Pharming es el término usado para referirse a las técnicas utilizadas para combatir el pharming.

Algunos de los métodos tradicionales para combatir el pharming son: Utilización de software especializado, protección DNS y addons para los exploradores web, como por ejemplo toolbars.

El Software especializado suele ser utilizado en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming y phishing, mientras que el uso de addons en los exploradores web permite a los usuarios domésticos protegerse de esta técnica.

La protección DNS permite evitar que los propios servidores DNS sean hackeados para realizar ataques pharming. Los filtros Anti-Spam normalmente no protegen a los usuarios contra esta técnica.

Métodos sencillos para evitar amenazas

Existen formas muy sencillas para eliminar los riesgos de ser víctima de estos fraudes, la mayoría de ellos tienen como principio el comportamiento del navegante cuando está en línea.

En primer lugar, nunca abra correos electrónicos no solicitados o aquellos que sean diferentes al comportamiento regular de alguien que usted conoce. Los códigos maliciosos que modifican la configuración del sistema para realizar ataques de pharming, usualmente llegan mediante otros códigos maliciosos por e-mail, gusanos o troyanos que al realizar su labor desaparecen dejando como huella un enorme agujero de seguridad en la dora conectada a Internet debe tener un mecanismo integral de protección y prevención de ataques maliciosos.

Esto es, una solución que ofrezca integralmente protección antivirus, un firewall que evite ataques de intrusos en línea, una herramienta contra el correo no deseado y contra el software espía o comercial, además de protección de redes inalámbricas, valoración de vulnerabilidades en el sistema y control del tipo de sitios Web que visitan los usuarios de cada máquina, entre otros.

No debemos permitir que los autores logren desestimular el uso de los instrumentos de la banca en línea o del comercio electrónico, que ha traído grandes beneficios a la economía mundial. Más bien, tomemos las medidas preventivas para no correr riesgo alguno en nuestra navegación cotidiana.

Software especializado

Aviso de Identidad de doble factor *Green Armor®* -*www.greenarmor.com*- es un sistema único de autenticación donde se verifica en profundidad si el usuario está interactuando con un sistema legal o es un sitio criminal clonado.

Este proceso no requiere registrarse, no tiene pasos previos durante el acceso a una página con login de usuario. Con ello se obtiene un nivel de seguridad mejorada.

Como funciona: Este producto se fusiona con el sitio web existente y se integra fácilmente, actúa por cierto detrás de la escena, donde verifica si la

procedencia de usuario es legítima además de legitimar el negocio.

El usuario ingresa su clave y nombre desde una máquina desconocida en ese período una contraseña es enviada por correo electrónico o SMS como un paquete de información "*Token*".

Se aplica por cierto una cierta criptografía en los envíos, con el doble control el usuario debe hacer click en un link provisto para validar su acceso, si el origen es dudoso no se produce la entrada al sistema.

Sólo sitios genuinos puede generar una marca, que con una serie de cálculos matemáticos aseguran la confiabilidad del la comunicación gemela.

Tampoco ofrece ayuda o preguntas para resolver la contraseña aumentando la seguridad.

Conclusiones

Parece ser que los "*laboratorios*" de virus son uno de los trabajos más estables que hay ahora, ya que es increíble la velocidad en la que están aumentando las técnicas "*escapistas*" de todo tipo de antivirus y las consecuentes creaciones "*nouvelle cousine*" de antivirus informáticos, pues la solución que hasta ahora existe para evitar ser estafados mediante pharming es la instalación en nuestros ordenadores de sistemas que detecten las acciones que se lleven a cabo en el ordenador y el bloqueo de las mismas. También conviene tener en cuenta que normalmente cuando se está produciendo una alteración de nuestros nombres -*pharming*-, en el momento que intentamos acceder a la Web deseada se produce una pequeña caída del sistema y posteriormente aparece la "*falsa*" página, en ese momento debemos sospechar de ser víctimas de un fraude y notificarlo a autoridades relacionadas con los fraudes informáticos de cada país.

La realidad es que necesitamos cada vez tener más aplicaciones para la defensa de nuestro computador, antes eran los virus y ahora anexamos el robo de nuestra información personal. Para ello es conveniente analizar diferentes empresas serias en este segmento de manera tal que tengamos una suite que nos cubra de los diferentes peligros sin olvidarnos de actualizar los productos a menudo con los parches que surgen del ensayo y error de los laboratorios. ☒

Las guías prácticas y parte de la documentación vertida es publicada con la debida autorización de Microsoft Corporation®. Las marcas y productos mencionados están debidamente registrados por sus respectivas empresas.