Cómo protegernos del Pharming y el Spim

Internet ha traído gran cantidad de beneficios a los usuarios pero también ha propiciado la aparición de ciertas amenazas que ponen en peligro la integridad de nuestros datos. Estamos acostumbrados a escuchar hablar sobre virus, phishing o spam, pero hoy os hablaremos de otras dos modalidades menos conocidas pero que a buen seguro os habrán aparecido: Pharming y Spim.

Pharming

Hay muchas personas que opinan que el pharming se trata de una variante más del phishing, y aunque así se puede considera, cabe decir que se trata de una amenaza mucho más peligrosa que esta última.

Básicamente, el pharming tiene la finalidad de llevar al usuario a una página falsa desde donde robarle sus credenciales y datos personales, pero a diferencia del phishing, para lograr este objetivo se utilizan técnicas mucho más complejas, ya que no sólo se intenta engañar al usuario, sino que se intenta modificar el comportamiento de los equipos informáticos para que resuelva las direcciones URL correctas y bien formadas hacia números IP diferentes de los originales y consecuentemente lleve al usuario a destinos no deseados.

Un ejemplo de este tipo de ataque podría ser el siguiente. En la primera imagen de arriba vemos la página de acceso a la red social de Facebook, mientras que la segunda es una página creada por un atacante. ¿Cómo diferenciarlas? Primero debemos fijar en la url de ambos sitios, y en este caso aparece en las dos el nombre 'es-es.facebook.com', pero la primera hace uso del protocolo de seguridad SSL, como vemos indicado con el protocolo 'https' y el candado (https://).

Esta amenaza tiene a su vez tres variantes posibles:

a) **Pharming Local**
En este caso el atacante es capaz de introducir un troyano o virus en el equipo de la víctima, el cual se encarga de alterar los registros de nombres que se encuentran en el archivo 'hosts' del sistema operativo. De esta forma, cuando el usuario escribe una url, el navegador lo llevará hacia la dirección IP el atacante haya escrito en ese archivo 'hosts'.

b) **Drive-By Pharming**
En esta variante, el ataque se realiza sobre los firewalls o routers, cambiando la dirección del servidor DNS a la de un servidor DNS que controla el atacante, que hará que muestre la página web falsa con la que poder engañar a los usuarios.

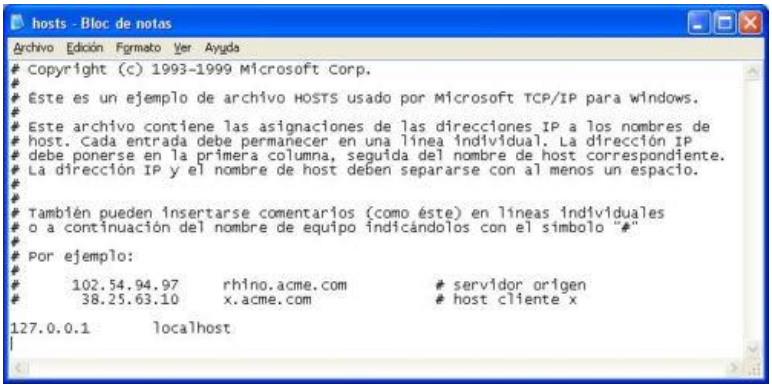
c) **Envenenamiento de DNS**
Esta última variante es muy difícil de llevar a cabo, ya que hacen uso de las vulnerabilidades de los servidores de DNS en lo que respecta al control de su caché de direcciones. Hoy en día es complicado que se dé un caso de este tipo debido a que los servicios de DNS de gran escala están en manos de proveedores de Internet como acens que han corregido este tipo de fallos.

¿Cómo puedo detectar si he sido víctima de un ataque Pharming?

Si creemos que hemos sufrido un ataque pharming, lo podemos verificar consultando el contenido del archivo 'hosts' de nuestro sistema operativo. Dependiendo de éste, su ubicación será diferente:

- **Sistemas Windows**: C:\WINNT\System32\drivers\etc\hosts
- **Linux**: /etc/hosts
- **iOS**: /private/etc/hosts
- **Android**: /system/etc/hosts

Este tipo de archivo, por defecto, tiene una apariencia similar a la que podéis ver en la siguiente imagen.



Si al abrirlo vemos otras entradas que no hemos añadido nosotros, podemos asegurar que hemos sido víctimas de uno de estos ataques.

Para solucionar el problema, lo que debemos hacer es editar ese archivo y eliminar todas las entradas distintas a 127.0.0.1 localhost.

Consejos para protegernos del Pharming

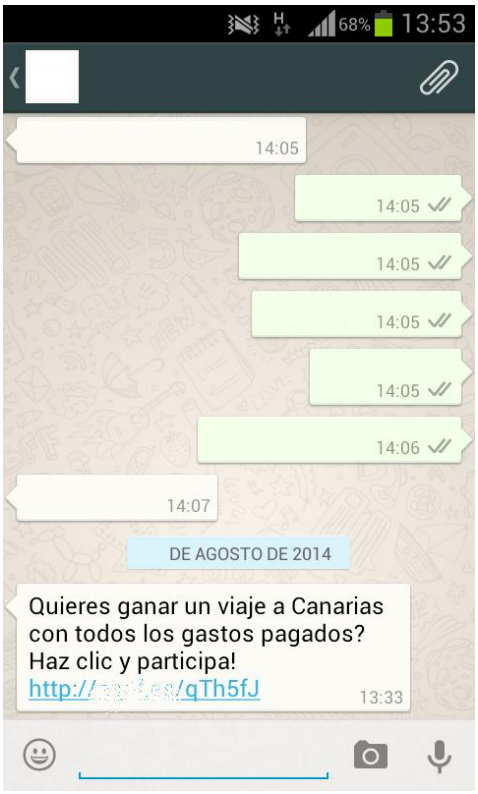
- Utilizar un antivirus actualizado que nos ayudará a protegernos si el atacante utiliza un archivo adjunto infectado como método para acceder a nuestro equipo.
- Desconfiar de la página si al acceder a ella ésta tiene un aspecto diferente al que estamos acostumbrados.
- Siempre que tengamos que introducir un usuario y una contraseña en un portal que contenga datos de gran importancia, hay que **asegurarse que utilice el protocolo HTTPS**.
- Si la página de nuestro banco ha cambiado de aspecto y parece sospechosa, contactar con el servicio de atención al cliente para verificar si es correcta o no.

SPIM

Hablar del problema del SPIM es hacer referencia al conocido spam, pero con la diferencia de que éste llega al usuario por medio de alguno de los **programas de mensajería instantánea como WhatsApp** que tan de moda está en los últimos años, lo que ha favorecido en aumentar su presencia.

Como ocurre con los correos basura, el SPIM se apoya en programas robot para propagarse por la red. Estas aplicaciones obtienen direcciones de contacto de nuestras aplicaciones de mensajería instantánea. Estos mensajes fraudulentos aparecen en formato de ventanas emergentes o enlaces en las conversaciones dependiendo de la aplicación que estemos utilizando.

Un ejemplo de este problema podía ser el siguiente:



Al igual que ocurre con el SPAM, el objetivo no es otro que hacer que el usuario acceda a una url desde donde se descargará algún archivo infectado que permitirá al atacante conseguir información relevante del usuario. El problema del SPIM es que es muy fácil caer en el engaño ya que en este tipo de programas solemos hacer caso de toda la información que nos envían nuestros contactos, por lo que si la información viene de alguien conocido, lo más fácil es que pulsemos sobre él y seamos infectados.

Al igual que ocurre con otros tipos de ataques, la mejor forma de evitar caer en sus garras es tirar de intuición y no hacer casos de aquellos mensajes que nos puedan parecer raros. De todas formas podemos tener en cuenta algunos consejos para esquivarlos:

- Si recibimos algún mensaje de algún remitente que no conocemos o con faltas de ortografía, mejor no hacer caso de él e ignorar cualquier cosa que nos envíe.
- Si en medio de una conversación recibimos un enlace que no tiene nada que ver con el tema que estamos tratando, desconfiar de él o preguntar a la otra persona si lo ha enviado él.
- Configurar las condiciones de privacidad de toda aplicación de mensajería instantánea que utilicemos.
- Por último y no menos importante, mantener siempre actualizadas las aplicaciones que utilicemos para contactar con nuestros amigos, familiares...

A lo largo de este White Paper hemos visto dos amenazas que pueden ser poco conocidas por los usuarios, pero que son iguales o más peligrosas que otras más conocidas.