

Los peligros que acechan en Internet

¿Qué es lo que puede infectar a un ordenador? (II)

✔ Le será de suma utilidad la revisión de la [primera parte](#) de este informe antes de comenzar la lectura de este documento.

En la primera parte de este artículo, discutimos sobre las amenazas impuestas por los programas maliciosos y los ataques externos que sufren los ordenadores conectados a Internet.

En el presente trabajo, trataremos las dos amenazas que quedaron pendientes, las cuales también deben conocerse.

Amenaza Nº 3: *Spam, Phishing y Spoofing* en los sitios Web

Se denomina *Spam* al envío masivo y sin ser solicitado de mensajes de correo electrónico, que promocionan algún tipo de producto, servicio o sitio Web. Para la mayoría de los usuarios de Internet, es un problema importante, y muchos han tenido que cambiar sus cuentas de correo debido a la cantidad de Spam que reciben, sobrepasando ampliamente a los mensajes legítimos.

Un *Spam* proviene generalmente de ordenadores secuestrados y posee direcciones de remitente falsas. Por eso la única forma efectiva de quejarse es por medio del análisis de los encabezados de los correos (que normalmente se encuentran ocultos y será necesario ver las instrucciones del programa de correo para poder obtener esa información) para de ese modo, encontrar la fuente verdadera y buscar los detalles de los sitios Web mencionados. Sin embargo *SpamCop* (www.spamcop.net) puede hacer esto automáticamente: sólo será necesario copiar los detalles completos (inclusive los encabezados) de los correos que se reciben. Aparte de esto, los filtros de Spam (los cuales ahora vienen incluidos en varios clientes de correo) son la mejor opción, aunque se corre el riesgo que confundan correo legítimo por *Spam*.

Mejor prevenir que curar cuando se trata de *Spam*:

- El usuario debe asegurarse que su dirección de correo no sea publicada en algún sitio Web, ya que la mayoría de los piratas los rastrean con un programa especial para extraer las direcciones de correo.
- Si resulta necesario publicar la dirección de correo, se deben tomar ciertas medidas para ocultar la dirección de dichos programas invasivos.
Mayor información:

- www.spam.abuse.net/userhelp/#hide
- www.u.arizona.edu/~trw/spam

- Finalmente, se debe considerar el uso de un servicio de redireccionado de correo como:

- *SpamGourmet*
www.spamgourmet.com
- *SpamMotel*
www.spammotel.com
- *SneakEmail*
www.sneakemail.com

Estos servicios le permitirán al usuario crear direcciones “alias” y así podrá darle una dirección diferente a cada persona o sitio Web.

Si una de las direcciones empieza a recibir Spam, esto no sólo le permitirá saber cuál es la fuente más probable sino que también podrá cerrar ese alias sin afectar a los otros.

Los ataques denominados **Phishing** se ejecutan a través de mensajes de correo electrónico diseñados para parecer correos oficiales de una institución financiera (bancos, sitios de comercio en línea como Paypal u otros) que invitan al usuario a visitar sus sitios Web, generalmente con la excusa de alguna verificación para su seguridad. Sin embargo el vínculo no se dirige al sitio verdadero sino a uno creado por impostores (el cual esta diseñado para parecerse lo más posible al original). Al ingresar el nombre de usuario y la contraseña en este sitio, estas les serán reveladas al impostor quien después podrá utilizarlas (o venderlas a otros). Puede encontrar más detalles sobre este tema en www.antiphishing.org y en el primer artículo de nuestra serie de divulgación, de [mayo de 2005](#).

Los ataques denominados **Spoofing** de sitios Web (también conocidos como ataques **Pharming**, de fraude en línea) son una variante de la técnica antes mencionada: al introducir la dirección del sitio Web, el usuario es redirigido hacia una falsa.

Esto se logra porque que los secuestradores de navegadores o programas espía, cambian las configuraciones del sistema o les proporcionan a los servidores proveedores del servicio de Internet (ISP) información falsa (técnica conocida como **DNS spoofing**) lo que origina que todos los clientes sean redirigidos hacia un sitio Web falso.

Para hacerle frente a los *correos masivos* (*Spamming*, *Phishing* y *Pharming*) el usuario debe:

- Asegurarse que su dirección de correo no sea publicada.
- Utilizar un filtro de *Spam* (correo masivo) o informar sobre ellos a SpamCop y aunque esto no afectará a los generadores de *Spam* pornográfico, sí a varios de *Spam* "semi-legítimos".
- Instalar un programa anti-spam que permita el filtrado del correo entrante.
- Instalar una aplicación contra los ataques *Phishing* y *Spoofing* como:
 - *Earthlink Toolbar* www.earthlink.net/software/free/toolbar
 - *Fraud Eliminator* www.fraudeliminator.com/download.php
 - *Online Armor*
www.tallemu.com

Amenaza Nº4: Rastreo y Búsqueda de perfiles

A menudo, ciertas páginas Web tienen un legítimo interés en sus visitantes: saber qué explorador están utilizando, de qué países provienen o qué sistemas operativos están utilizando en sus ordenadores (Windows, Linux, OSX). En algunos casos, esto puede beneficiar a que ciertos sitios mejoren sus diseños para una mejor adaptación con ciertos grupos, como por ejemplo, la gran cantidad de usuarios de Firefox.

Sin embargo los intereses de los comerciantes y anunciantes van mucho más allá ya que desean recolectar otro tipo de información, como edades, intereses, riquezas y direcciones.

Mientras que un navegador no revelará dicha información, es posible que los piratas la consigan recolectando detalles en los sitios Web visitados y en la compras hechas.

Para juntar toda la información, se utilizan dos características del explorador de Internet:

- *Cookies*
- *Referrers*.

Cuando un usuario visita un sitio Web pulsando en algún vínculo, el navegador le informará a ese sitio Web cuál es su posición.

Esto es útil para los administradores de sitios ya que les informa de dónde viene el tráfico (por ejemplo, una mención en otro sitio o de una lista mejorada en algún motor de búsqueda).

De forma similar, la mayoría de los sitios Web colocan una etiqueta (llamada *Cookie*) en el sistema del usuario para poder identificarlo cuando vuelva a visitar ese sitio.

Ambas características (*Referrers* y *Cookies*) tienen uso legítimo y las *Cookies* pueden ser genuinamente útiles en algunos casos (por ejemplo: almacena el contenido del carrito de compras en un sitio Web o mantiene al usuario registrado en un foro de discusión, entre otras posibilidades).

Pero existe un lugar donde se puede abusar fuertemente de estas dos facilidades: la publicidad.

Muchos anuncios se mantienen en dominios separados (por ejemplo, doubleclick.net, mediaplex.com) entonces, cuando un navegador visita estos sitios para descargar publicidad, pueden establecer (y después leer) una *Cookie* como también identificar de cuál sitio proviene el usuario.

Con el tiempo, pueden construir un perfil basándose en la imagen (parcial) de los sitios que el usuario visita y combinan esto con otro tipo de información personal (como el historial de los créditos).

Un pequeño truco técnico denominado Web bug, consistente en pequeñas imágenes de 1 pixel de tamaño, pueden permitirle a los comerciantes obtener información similar sin tener ningún aviso visible en el sitio. Más información al respecto: www.eff.org/Privacy/Marketing/web_bug.html .

Aunque esto es un asunto de privacidad más que de seguridad, es necesario que la mayoría de los usuarios le presten atención.

Para evitar que descubran su perfil, es necesario:

- Evitar que ciertos sitios utilicen la información de *Cookies* y *Referrers*, excepto aquellos sitios Web confiables. El filtro de contenido activo de Outpost puede bloquearlos, así como también los filtros Web como Web Washer o Proxomitron. Algunos navegadores (por ejemplo, *Opera*) le permiten al usuario evitar que sitios pertenecientes a terceros le inserten *Cookies*.
- Limpiar periódicamente todas las *Cookies* del navegador aunque esto requerirá que el usuario se registre otra vez en ciertos sitios, por eso es recomendable no hacerlo muy seguido.
- Utilizar un filtro de publicidad (como el complemento de específico de Outpost) para quitar todas las imágenes publicitarias de las páginas Web visitadas.

Para obtener más información, visite la lista de la Fundación Electrónica, "Frontier's Privacy Top 12" en www.eff.org/Privacy/eff_privacy_top_12.php

Conclusión

Los peligros más grandes provienen de lugares muy lejanos de Internet:

- Páginas con **programas piratas** ("warez")
- Redes para compartir archivos
- Canales subterráneos de mensajería (*Chat*).

Sin embargo, estos sitios están a sólo un vínculo de distancia y aún un sitio legítimo puede ser alterado para incluir un vínculo con el fin de secuestrar ordenadores desprotegidos.

Por eso es necesario una precaución eterna para estar a salvo.

Por suerte, con la seguridad se incluye un mejor control, y si un usuario sigue las recomendaciones dadas anteriormente, podrá obtener una mejor experiencia en línea junto con un sistema más seguro.