Consejos contra el malware

ESET Latinoamérica
http://www.eset-la.com

Consejos contra el malware (I)

Esta serie de artículos tendrán como objetivo informar sobre las amenazas actuales y brindar una serie de consejos simples y buenas prácticas para prevenir las mismas. En el presente comenzaremos con las formas más comunes de infección de virus y su prevención.

Los virus actuales usan el correo el electrónico, las redes P2P, los programas de mensajería instantánea y la web como principales medios de propagación.

Es por ello que debemos proteger estos medios de comunicación de la mejor forma posible para ello:

1. No descargar archivos de sitios de dudosa reputación.

2. Descargar actualizaciones de programas sólo de sitios de confianza. En el caso de las actualizaciones de productos de Microsoft, por ejemplo, las mismas son informadas sólo el segundo martes de cada mes (con muy raras excepciones en caso de urgencia). Esto último facilita las actualizaciones que debemos realizar. Cuando se pueda es recomendable dejar actuar a las actualizaciones automáticas de cada producto.

3. No confiar en correos con programas adjuntos y mucho menos si la misma dice ser una actualización de un producto determinado. Las empresas nunca envían adjuntos con actualizaciones, sólo informan de la misma.

4. Evitar los programas ilegales (como los warez) ya que los mismos suelen contener troyanos, keyloggers, etc. Si desea utilizar programas libres o gratuitos puede recurrir a las soluciones OpenSource.

5. Ya no es suficiente eliminar correos de personas desconocidas o que no hayamos solicitado, ya que esta forma de prevención es fácilmente burlada por cualquier virus actual. Así que debemos recurrir a estar protegidos con un Antivirus con capacidades proactivas que nos permita detectar un programa dañino si el mismo es descargado desde un correo electrónico. Esto también aplica para cualquier otro tipo de descarga.

6. Cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos. Si algún archivo posee doble extensión es recomendable eliminarlo directamente, ya que existe una alta probabilidad de que el mismo sea un archivo dañino.

7. En caso de recibir archivos o enlaces para descarga (que no esperábamos) por los programas de mensajería, es una buena práctica preguntar a nuestra contra parte si él ha enviado ese enlace, ya que es común que sistemas infectados ofrezcan estos enlaces para auto-descargarse y continuar su propagación.

8. En caso de descargar archivos de redes P2P es indispensable hacerlo con un Antivirus actualizado ya que nada asegura que lo que estamos descargando sea lo que dice ser. A esto debemos sumarle que si acostumbramos a descargar archivos con frecuencia sería conveniente hacerlo en una computadora que sólo destinemos a este fin y que nuestros datos sensibles no sean almacenados en la misma.

9. Utilizar el sistema operativo con un usuario con sólo los privilegios necesarios para la ejecución de los programas utilizados. Es común utilizar "Administrador" para realizar cualquier tarea. Esto no es necesario en la mayoría de los casos y sólo incrementa el nivel de daños en caso de infección.

10. Debe prestarse atención cuando se navega para evitar ingresar a sitios peligrosos y evitar ejecutar programas que "auto-ofrecen" descargarse, ya que es común ver programas dañinos que simulan ser soluciones de seguridad o Antivirus.

Estos recomendaciones, en su mayoría fácil de seguir, nos evitarán muchos dolores de cabeza y nos permitirán hacer un uso más seguro de nuestros sistemas.

Consejos contra el malware (SPAM)

En esta entrega continuamos con la serie de artículos iniciado en el boletín anterior entregando consejos para prevenir el malware. Les hablaremos de la **prevención del SPAM** debido a que gran porcentaje del correo recibido actualmente se encuadra en este tipo de mensajes.

Se define SPAM a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico pero puede presentarse por programas de mensajería instantánea o por teléfono celular.

Actualmente hay empresas que facturan millones de dólares al año recolectando direcciones de correo electrónico, vendiéndolas y enviándolas mensajes de promociones, ofertas, y publicidad no solicitada.

Las recomendaciones para evitar el SPAM son las siguientes:

1. No enviar mensajes en cadena ya que los mismos generalmente son algún tipo de engaño (hoax).

2. Si aún así se deseara enviar mensajes a muchos destinatarios hacerlo siempre Con Copia Oculta (CCC), ya que esto evita que un destinatario vea (robe) el mail de los demás destinatarios.

3. No publicar una dirección privada en sitios webs, foros, conversaciones online, etc. ya que sólo facilita la obtención de las mismas a los spammers (personas que envían spam).

4. Si se desea navegar o registrarse en sitios de baja confianza hágalo con cuentas de mails destinada para ese fin. Algunos servicios de webmail disponen de esta funcionalidad: protegemos nuestra dirección de mail mientras podemos publicar otra cuenta y administrar ambas desde el mismo lugar.

5. Para el mismo fin también es recomendable utilizar cuentas de correos temporales y descartables como las mencionadas al pie del presente.

6. Nunca responder este tipo de mensajes ya que con esto sólo estamos confirmando nuestra dirección de mail y sólo lograremos recibir más correo basura.

7. Es bueno tener más de una cuenta de correo (al menos 2 o 3): una cuenta laboral que sólo sea utilizada para este fin, una personal y la otra para contacto público o de distribución masiva.

Algunos filtros de correo funcionan efectivamente previniendo gran cantidad de SPAM, pero ninguno funciona lo suficientemente bien como para olvidarnos de estos simples consejos que, utilizados correctamente, nos ayudará a recibir menos correo no deseado. Otra característica negativa de los filtros es que algunos funcionan tan sensiblemente que terminan filtrando correo normal.

Más información

Prevención efectiva contra el SPAM

http://www.segu-info.com.ar/articulos/articulo33.htm

Correos temporales:

http://www.tempinbox.com/spanish/

http://trashmail.net/

http://www.spambob.com/

http://www.spamday.com/

Consejos contra el malware (Phishing)

En esta entrega continuamos con la serie de artículos iniciado en los boletines anteriores dando consejos para prevenir el malware. Hoy les hablaremos de la **prevención del phishing** debido a que es una amenaza en alta.

Se define phishing como la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. Normalmente, se utiliza con fines delictivos enviando SPAM e invitando acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios.

Las recomendaciones para evitar este tipo de estafa son las siguientes:

1. Evite el spam ya que es el principal medio de distribución de cualquier mensaje que intente engañarlo. Para ello puede recurrir a nuestro boletín anterior.

2. Tome por regla general rechazar adjuntos y analizarlos aún cuando se esté esperando recibirlos.

3. Nunca hacer clic en un enlace incluido en un mensaje de correo. Siempre intente ingresar manualmente a cualquier sitio web. Esto se debe tener muy en cuenta cuando es el caso de entidades financieras, o en donde se nos pide información confidencial (como usuario, contraseña, tarjeta, PIN, etc.).

4. Sepa que su entidad, empresa, organización, etc., sea cual sea, nunca le solicitará datos confidenciales por ningún medio, ni telefónicamente, ni por fax, ni por correo electrónico, ni a través de ningún otro medio existente. Es muy importante remarcar este punto y en caso de recibir un correo de este tipo, ignórelo y/o elimínelo.

5. Otra forma de saber si realmente se está ingresando al sitio original, es que la dirección web de la página deberá comenzar con https y no http, como es la costumbre. La S final, nos da un alto nivel de confianza que estamos navegando por una página web segura.

6. Es una buena costumbre verificar el certificado digital al que se accede haciendo doble clic sobre el candado de la barra de estado en parte inferior de su explorador (actualmente algunos navegadores también pueden mostrarlo en la barra de navegación superior).

7. No responder solicitudes de información que lleguen por e-mail. Cuando las empresas reales necesitan contactarnos tienen otras formas de hacerlo, de las cuales jamás será parte el correo electrónico debido a sus problemas inherentes de seguridad.

8. Si tiene dudas sobre la legitimidad de un correo, llame por teléfono a la compañía a un número que conozca de antemano... nunca llame a los números que vienen en los mensajes recibidos.

9. El correo electrónico es muy fácil de interceptar y de que caiga en manos equivocadas, por lo que jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través de este medio.

10. Resulta recomendable hacerse el hábito de examinar los cargos que se hacen a sus cuentas o tarjetas de crédito para detectar cualquier actividad inusual.

11. Use antivirus y firewall. Estas aplicaciones no se hacen cargo directamente del problema pero pueden detectar correos con troyanos o conexiones entrantes/salientes no autorizadas o sospechosas.

12. También es importante, que si usted conoce algún tipo de amenaza como las citadas, las denuncie a la unidad de delitos informáticos de su país.

Consejos contra el malware (Adware-Spyware)

En esta entrega continuamos con la serie de artículos iniciada en los boletines anteriores dando consejos para prevenir el malware**: el adware y el spyware**. Se define como adware al software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario.

Generalmente, estas aplicaciones agregan iconos gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo. Estas barras de tareas personalizadas tienen palabras claves predefinidas para que el usuario llegue a sitios con publicidad, sea lo que sea que el mismo esté buscando.

Se define como spyware o software espía a las aplicaciones que recopilan información sobre una persona u organización sin su conocimiento, ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas.

Normalmente, estas amenazas envían información a sus servidores en función de los hábitos de navegación del usuario. También recogen datos acerca de las webs que se visitan y la información que se solicita en esos sitios, así como direcciones IP y URLs que se navegan.

Esta información es explotada para propósitos de mercadotecnia y muchas veces es el origen de otra plaga como el SPAM, ya que pueden encarar publicidad personalizada hacia el usuario afectado. Con estos datos, además, es posible crear perfiles estadísticos de los hábitos de los internautas.

Las recomendaciones para evitar la instalación de este tipo de software son las siguientes:

1. Verificar cuidadosamente los sitios por los que navega, ya que es muy común que estas aplicaciones auto-ofrezcan su instalación o que la misma sea ofrecida por empresas de dudosa reputación.

2. Si es posible, lea atentamente las políticas de privacidad de estas aplicaciones. Generalmente incluyen puntos como "recolectamos la siguiente información del usuario" o "los daños que causa la aplicación no es nuestra responsabilidad" o "al instalar esta aplicación Ud. autoriza que entreguemos sus datos a...".

3. Estas aplicaciones normalmente prometen ser barras con funcionalidades extras que se instalan sobre el explorador.

4. Actualmente, se nota una importante aparición de aplicaciones que simulan ser software anti-spyware que en realidad contiene spyware. Una lista de los mismos puede ser encontrada en la dirección que se detalla al pie del presente.

5. Cuando una aplicación intente instalarse sin que Ud. lo haya solicitado, desconfíe y verifique la lista anterior.

6. Es común que los sitios dedicados al underground o pornográficos, contengan un alto contenido de programas dañinos que explotando diversas vulnerabilidades del sistema operativo o del explorador, le permiten instalarse.

7. Verificar los privilegios de usuarios. Es común que todos los usuarios que hacen uso de la computadora lo hagan con permisos administrativos. Esto no necesariamente debe ser así, es recomendable que cada usuario tenga su propio perfil, sólo con los permisos necesarios para realizar sus tareas. Ya que esto disminuye el campo de acción de un posible intruso (virus, backdoor, usuario no autorizado, etc.).

8. Estas aplicaciones evolucionan continuamente por lo que contar con un antivirus actualizado y con capacidades proactivas es fundamental para detectar estas aplicaciones y evitar su instalación.

Antispyware sospechosos:

http://www.spywarewarrior.com/rogue_anti-spyware.htm

Este sitio ofrece una lista de software sospechoso. La lista es mantenida por Eric L. Howes profesor en la GSLIS (Graduate School of Library and Information Science) de la Universidad de Illinois, EE.UU.