SEGURIDAD A NIVEL USUARIO

Software malicioso

Con el nombre software malicioso agrupamos todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto. Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusivos. Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware.

A continuación detallamos, paso a paso, varias tareas habituales para la eliminación de un virus en el ordenador, como la edición del registro y la terminación de procesos.

1. Prueba a restaurar el sistema a un punto de restauración anterior a la aparición de los problemas, para ello sigue los pasos que se indican en el siguiente enlace: Restauración del Sistema.

2. Si de esta manera no has solucionado el problema, prueba a deshabilitar la opción de restauración del sistema, como se indica en el siguiente enlace: Deshabilitar la Opción de Restauración del Sistema.

3. Prueba a realizar un análisis en línea con alguna de las herramientas antivirus que se indican a continuación: Herramientas Antivirus.

4. También puedes realizar un análisis en línea con alguna de las herramientas anti espías que se indican en el siguiente enlace: Herramientas Anti espías

5. Si detectas algún archivo que el antivirus no puede eliminar, deberás hacerlo manualmente.
Para ello puedes seguir alguna de las opciones que se indican en el siguiente enlace: Eliminar librerías .DLL y .EXE.

6. Por último, realiza una limpieza del registro de Windows. Para ello sigue las instrucciones del siguiente enlace: Limpiar el Registro de Windows.

Antivirus

Los antivirus son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos. Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado.

Los virus, gusanos, spyware son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen la características de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información.

Una característica adicional es la capacidad que tienen de propagarse. Otras características son el robo de información, la pérdida de esta, la capacidad de suplantación, que hacen que reviertan en pérdidas económicas y de imagen.

Los daños que los virus dan a los sistemas informáticos son:

• Pérdida de información (evaluable según el caso)

• Horas de contención (Técnicos de SI, Horas de paradas productivas, tiempos de contención o reinstalación, cuantificables según el caso + horas de asesoría externa)

• Pérdida de imagen (Valor no cuantificable)

Hay que tener en cuenta que cada virus es una situación nueva, por lo que es difícil cuantificar a priori lo que puede costar una intervención. Tenemos que encontrar métodos de realizar planificación en caso de que se produzcan estas contingencias.

Software Espía

Los programas espías o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

Pueden tener acceso por ejemplo a: el correo electrónico y el password; dirección IP y DNS; teléfono, país; páginas que se visitan, qué tiempos se está en ellas y con qué frecuencia se regresa; qué software está instalado en el equipo y cuál se descarga; qué compras se hacen por internet; tarjeta de crédito y cuentas de banco.

Principales síntomas de infección son:

• Cambio de la página de inicio, la de error y búsqueda del navegador.
• Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto, la mayoría de temas pornográficos y comerciales (por ejemplo, la salida al mercado de un nuevo producto).
• Barras de búsquedas de sitios como la de Alexa, Hotbar, MyWebSearch, FunWeb, etc.. que no se pueden eliminar.
• Creación de carpetas tanto en el directorio raíz, como en "Archivos de programas", "Documents and Settings" y "WINDOWS".
• Modificación de valores de registro.
• La navegación por la red se hace cada día más lenta, y con más problemas.
• Es notable que tarda más en iniciar el computador debido a la carga de cantidad de software spyware que se inicia una vez alterado el registro a los fines de que el spyware se active al iniciarse la computadora.
• Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
• Aparición de un mensaje de infección no propio del sistema, así como un enlace web para descargar un supuesto antispyware.
• Al acceder a determinados sitios sobre el escritorio se oculta o bloquea tanto el panel de control como los iconos de programas.
• Denegación de servicios de correo y mensajería instantánea.

Phishing

Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Respuesta social

Una estrategia para combatir el phishing adoptada por algunas empresas es la de entrenar a los empleados de modo que puedan reconocer posibles ataques phishing. Una nueva táctica de phishing donde se envían correos electrónicos de tipo phishing a una compañía determinada, conocido como spear phishing, ha motivado al entrenamiento de usuarios en varias localidades, incluyendo la Academia Militar de West Point en los Estados Unidos. En un experimento realizado en junio del 2004 con spear phishing, el 80% de los 500 cadetes de West Point a los que se les envió un e-mail falso fueron engañados y procedieron a dar información personal.

Un usuario al que se le contacta mediante un mensaje electrónico y se le hace mención sobre la necesidad de "verificar" una cuenta electrónica puede o bien contactar con la compañía que supuestamente le envía el mensaje, o puede escribir la dirección web de un sitio web seguro en la barra de direcciones de su navegador para evitar usar el enlace que aparece en el mensaje sospechoso de phishing.

Respuestas técnicas

Hay varios softwares anti-phishing disponibles. La mayoría de estos programas trabajan identificando contenidos phishing en sitios web y correos electrónicos; algunos software antiphishing pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el phishing recibidos por el usuario.

El Anti-Phishing Working Group, industria y asociación que aplica la ley contra las prácticas de phishing, ha sugerido que las técnicas convencionales de phishing podrían ser obsoletas en un futuro a medida que la gente se oriente sobre los métodos de ingeniería social utilizadas por los phishers. Ellos suponen que en un futuro cercano, el pharming y otros usos de malware se van a convertir en herramientas más comunes para el robo de información.

Contraseñas Seguras

En el control del acceso para todo, se realiza una relación entre seguridad y conveniencia. Es decir, si algún recurso está protegido por una contraseña, entonces la seguridad se incrementa con la consecuente pérdida de conveniencia para los usuarios.

Algunos sistemas protegidos por contraseñas plantean pocos o ningún riesgo a los usuarios si éstos se revelan, por ejemplo, una contraseña que permita el acceso a la información de una Web site gratuita. Otros plantean un modesto riesgo económico o de privacidad, por ejemplo, un password utilizado para acceder al e-mail, o alguna contraseña para algún teléfono celular.

• Muchos de los usuarios no cambian la contraseña que viene predeterminada en muchos de los sistemas de seguridad. Listas de estas contraseñas están disponibles en el Internet.

• Una contraseña puede ser determinada si un usuario elige como contraseña una pieza de información personal que sea fácil de descubrir (por ejemplo: número de ID de estudiante, el nombre del novio/a, el día de cumpleaños, número telefónico, etc.)

•Una contraseña es vulnerable si puede ser encontrada en una lista. Los diccionarios (frecuentemente de forma electrónica) están disponibles en muchos lenguajes, y existen listas de contraseñas comunes.

• En pruebas sobre sistemas en vivo, los ataques de diccionarios son rutinariamente acertados, por lo que el software implementado en este tipo de ataques ya se encuentra disponible para muchos sistemas.