Malware

La palabra malware proviene de una agrupación de las palabras malicious software. Este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.

Dos tipos comunes de malware son los virus y los gusanos informáticos, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismo que en algunas ocasiones ya han mutado, la diferencia entre un gusano y un virus informático radica en que el gusano opera de forma más o menos independiente a otros archivos, mientras que el virus depende de un portador para poderse replicar.

Los virus informáticos utilizan una variedad de portadores. Los blancos comunes son los archivos ejecutables que son parte de las aplicaciones, los documentos que contienen macros, y los sectores de arranque de los discos de 3,1/2 pulgadas. En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, ejecutando al mismo tiempo el código del virus. Normalmente la aplicación infectada funciona normalmente. Algunos virus sobrescriben otros programas con copias de ellos mismos, el contagio entre computadoras se efectúa cuando el software o el documento infectado va de una computadora a otra y es ejecutado.

Los gusanos informáticos son similares a los virus, pero los gusanos no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades del objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios y poderse ejecutar.

Un programa **caballo de troya** es una pieza de software dañino disfrazado de software legítimo. Los caballos de troya no son capaces de replicarse por si mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño. Una puerta trasera es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación. De acuerdo en como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras. El primer grupo se asemeja a los caballos de troya, es decir, son manualmente insertados dentro de algún otro software, ejecutados por el software contaminado e infecta al sistema para poder ser instalado permanentemente. El segundo grupo funciona de manera parecida a un gusano informático, el cuál es ejecutado como un procedimiento de inicialización del sistema y normalmente infecta por medio de gusanos que lo llevan como carga.

Un exploit es aquel software que ataca una vulnerabilidad particular de un sistema operativo. Los exploits no son necesariamente maliciosos –son generalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas maliciosos como los gusanos informáticos.

Los rootkit, son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante. Los rootkit pueden incluir puertas traseras, permitiendo al atacante obtener de nuevo acceso al sistema o también pueden incluir exploits para atacar otros sistemas.

El spyware es todo aquel software que recolecta y envía información de los usuarios. Normalmente trabajan y contaminan sistemas como lo hacen los caballos de troya.
Los programas espía 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.
Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, como el programa Magic Lantern desarrollado por el FBI, o bien puede estar oculto en la instalación de un programa aparentemente inocuo.
Los programas de recolección de datos instalados con el conocimiento del usuario no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen.
Los cookies son un conocido mecanismo que almacena información sobre un usuario de Internet en su propio ordenador, y se suelen emplear para asignar a los visitantes de un sitio de Internet un número de identificación individual para su reconocimiento subsiguiente. Sin embargo, la existencia de los cookies y su uso generalmente no están ocultos al usuario, quien puede desactivar el acceso a la información de los cookies. Sin embargo, dado que un sitio Web puede emplear un identificador cookie para

construir un perfil del usuario y éste no conoce la información que se añade a este perfil, se puede considerar a los cookies una forma de spyware. Por ejemplo, una página con motor de búsqueda puede asignar un número de identificación individual al usuario la primera vez que visita la página, y puede almacenar todos sus términos de búsqueda en una base de datos con su número de identificación como clave en todas sus visitas subsiguientes (hasta que el cookie expira o se borra). Estos datos pueden ser empleados para seleccionar los anuncios publicitarios que se mostrarán al usuario, o pueden ser transmitidos (legal o ilegalmente) a otros sitios u organizaciones.

Ejemplos de spywares:
Claria Corporation
Claria es un spyware que se instala en el ordenador, solo con la navegación por sitios que lo publican como propaganda. El claria es bloqueado por el anti-spyware spybot y es detectado como "Avenue Inc", si se logra instalar en el ordenador ocasiona problemas de conexión a redes, o que programas de mensajería instantánea no logren conectarse, en algunos casos altera el protocolo TCP/IP y no se logra ninguna conexión a red, hay que re-instalar el protocolo.

Bonzi Buddy es un programa espía (spyware en inglés).
Se trata de un simio de color violeta que aparece en un pop-up y dice en inglés : "Estoy solo. ¿No querés ser mi amigo?". Al aceptar la instalación se instala un software gratuito en la computadora que hará que el gorila cante, baile, ayude en las descargas y de paso registre el comportamiento en Internet de aquel que aceptó ser amigo de BonziBuddy. También cambia la página de inicio del navegador a la de Bonzi. Los niños suelen descargar este programa por su interfaz divertido, sin percatarse de su naturaleza publicitaria.

Magic Lantern
Según una fuente mencionada por el servicio de noticias MSNBC, el FBI estaría desarrollando su propio caballo de Troya, para combatir al terrorismo.
La idea del programa, es robar las contraseñas de todo aquel (en principio sospechoso), que use correo electrónico encriptado para sus comunicaciones.
Este troyano, conocido como Magic Lantern (Linterna Mágica), podría enviarse a cualquier sospechoso, como un adjunto a un mensaje aparentemente inocente.
Aprovechándose de algunas vulnerabilidades, podría incluso instalarse sin el conocimiento del destinatario, y a partir de allí capturaría las contraseñas usadas por el supuesto terrorista, enviándolas a las oficinas del FBI.
Linterna Mágica sería parte de un programa más complejo de vigilancia, llamado Cyber Knight (Caballero cibernético), el cuál incluiría una base de datos que permitiría al FBI cruzar información proveniente de e-mails, salas de chat, mensajeros instantáneos tipo ICQ y llamadas telefónicas por Internet.
Algunas fuentes consultadas del FBI, ni negaron ni admitieron la noticia, pero declararon que no es nada nuevo que la organización ha estado trabajando con especialistas de la industria de la seguridad, para crear una herramienta que fuera eficaz en combatir tanto al terrorismo, como a otros actos delictivos. Y aunque no debería ser una sorpresa, tampoco es apropiado que se revelen las tecnologías que específicamente se usarán, explicó un vocero.
Por otro lado, está el gran tema que involucra a nuestras libertades individuales. Organizaciones norteamericanas que defienden los derechos civiles de los ciudadanos, ya han reaccionado ante lo que consideran un claro abuso a estos principios.
Mientras algunos discuten si el uso de este software por parte del FBI debería limitarse a casos especiales, otros están seguros que este tipo de tecnología no va a impedir los actos criminales serios, aunque si va a comprometer la privacidad de usuarios inocentes en todo el mundo.

Obtenido de http://es.wikipedia.org/wiki/Malware

Pedido de auxilio de un usuario

Tengo Un Problema Con Mi Pc, Esta Infectada Con Spyware Mi Pantalla Tiene Como Fondo Un Recuadro Que Dice: Danger: Spyware Y Me Manda Supuestamente A Una Pagina De Smart Security, Aparte De Eso En El Escritorio El Boton Secundario Del Mouse No Funciona Y Cuando Creo Un Acceso Directo Me Manda Dos Iconos, Tambien Me Abre Una Pagina Cuando Entro A Internet La Pagina Es Daosearch.com, Y Cuando Estoy Navengando Me Subraya Las Palbaras Claves Y Me La Busca Mandandome A La Pagina De Daosearch. Tengo El Adware 6.0, El Spybot 1.3, El Antispyware Beta De Microsoft, Y He Descargado El Hiackthis.

Como Soluciono Mi Problema.

Programas que ayudan a detectar y remover (con suerte) a los Spyware y Hijack:

Ad-Aware, Spybot, CWSHredder, Hijack This.

LISTADO DE PALABRAS RELACIONADAS CON EL TEMA DE VIRUS (Recopilado de Internet)

A:

ActiveX: Es un sistema de tecnologías de Microsoft que permite el contenido interactivo para el Web mundial. Desafortunadamente, los ajustes flojos de la seguridad de ActiveX del defecto en Internet Explorer pueden permitir que cualquier página web instale secretamente los controles de activeX automáticamente. Puesto que estos controles de activeX pueden hacer casi cualquier cosa (instalación incluyendo de software, tal como spyware), muchos los consideran una amenaza significativa de la seguridad.

Adware: Normalmente se confunde este término con el de Spyware; la diferencia es que el Adware no recolecta información del equipo donde está instalado, sino que se limita a mostrar publicidad mientras que el usuario está utilizando una aplicación.

B:

Browser Hijackers: (Secuestradores del Navegador) Son los programas que procuran cambiar la pagina de inicio y búsqueda y/o otros ajustes del navegador. Estos pueden ser instalados en el sistema sin nuestro consentimiento al visitar ciertos sitos web mediante controles ActiveX o bien ser incluidos por un troyano.

C:

Cookies: Son pequeños archivos que generan sitios de Internet para facilitarnos la utilización de algunas paginas. Algunas empresas utilizan a las inofensivas cookies para monitorear la actividad online de los usuarios, incurriendo en una clara invasión a la privacidad, aunque no siempre se utilizan para esto.

Cuarentena: Consiste en proteger nuestro equipo dejando aislado a uno o varios archivos infectados con el propósito de poder desinfectarlos en próximas actualizaciones de nuestro producto antivirus si fuese posible

G:

Gusanos: Los gusanos tienen ciertas similitudes con los virus informáticos, pero también diferencias fundamentales. Un gusano se parece a un virus en que su principal función es reproducirse, pero por el contrario de cómo lo hacen los virus, en lugar de copiarse dentro de otros archivos, un gusano crea nuevas copias de si mismo para replicarse.

Gusano de Internet: Tienen las mismas funciones de los gusanos comunes pero además aprovechan los medios que provee la red de redes para reproducirse a través de ella.

H:

Heurística: Método de revisión de archivos y/o memoria basado en la búsqueda de patrones de actividad que puedan considerarse como un virus. Normalmente utilizados para la detección de nuevas versiones de virus ya conocidos o familias de virus.

Hijacker: Comúnmente llamado "Secuestrador de Navegador" al poder apoderarse de la pagina de inicio, de búsqueda, de error, etc.. de navegadores como Internet Explorer.

Hoaxes: La palabra hoax viene del inglés y tiene dos interpretaciones. Por un lado, puede ser utilizado como un verbo que significa embaucar; en cambio, si se utiliza como sustantivo, se traduce como engaño, bulo o broma de mal gusto.

J:

Jokes: Los Jokes, o programas de broma, son aplicaciones inofensivas que simulan ser virus informáticos.

K:

Keylogger: (Capturadotes de Teclado) Aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado. Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.

M:

Malware: Es la abreviatura de Malicious software, término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Trojan

(Caballo de Troya), Gusano (Worm), Parásito, Spyware, Adware, Hijackers, Keyloggers, etc….

P:

Parches: También conocidos como actualizaciones (en inglés patches o updates), son soluciones a problemas o agujeros de seguridad en aplicaciones o sistemas operativos.

Phishing: Se utiliza el término "phishing" para referirse a todo tipo de prácticas utilizadas para obtener información confidencial (como números de cuentas, de tarjetas de crédito, contraseñas, etc.).

S:

Spam: Es llamado Spam al correo basura (e-mail), el cual llega a nuestras casillas de correo sin que nosotros lo hayamos solicitado.

Spyware: Son pequeños programas que se instalan en nuestro sistema con la finalidad de robar nuestros datos y espiar nuestros movimientos por la red. Luego envían esa información a empresas de publicidad de internet para comercializar con nuestros datos. Trabajan en modo 'background' (segundo plano) para que no nos percatemos de que están hasta que empiecen a aparecer los primeros síntomas.

T:

ToolBar: (Barra de herramientas) Son pequeños programas que se adjuntan a nuestro navegador y nos proveen de funciones extras. Hay muchas barras de herramientas conocidas como la de Google, Yahoo, MSN pero al igual hay muchas que realizan funciones de espía como Alexa, Hotbar, WebSearch, Lop, etc..

Troyanos: (Caballos de Troya) Programas que, enmascarados de alguna forma como un juego o similar, buscan hacer creer al usuario que son inofensivos, para realizar acciones maliciosas en su equipo. A diferencia de los virus y gusanos los troyanos no se pueden reproducir por si mismos.

V:

Virus: Son sencillamente programas creados para infectar sistemas y otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente.

FIREWALL: Pared de Fuego, cortafuegos. Mecanísmo (de hardware o software) utilizado para proteger una red o computadora conectada a Internet de accesos no autorizados. Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.
Un firewal es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewal examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.
De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.
Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con softwares específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

Ejemplo de software Firewall:

Outpost Firewall, Zone Alarm, Keiro, Sygate, etc. Ver http://www.infospyware.com/Firewall/