


I'm not robot  reCAPTCHA

**Continue**

## Como crear un virus gusano con bloc de notas

There are no translations available.Hace algún tiempo, el único mecanismo capaz de comprometer la seguridad de nuestros datos era insertar un disco contaminado en nuestro PC... Hace algún tiempo, el único mecanismo capaz de comprometer la seguridad de nuestros datos era insertar un disco contaminado en nuestro PC. En esa época, para mantener a salvo, prácticamente bastaba con evitar "prácticas de riesgo" y disponer de un buen antivirus. 1. Introducción
Hace algún tiempo, el único mecanismo capaz de comprometer la seguridad de nuestros datos era insertar un disco contaminado en nuestro PC. En esa época, para mantener a salvo, prácticamente bastaba con evitar "prácticas de riesgo" y disponer de un buen antivirus. Más tarde, el desarrollo de las redes internas y externas, así como la llegada de Internet, abrieron nuevas posibilidades de ataques, y nos llevaron a la era de la seguridad de red. En la actualidad, el uso masivo de las aplicaciones y servicios web entraña nuevos riesgos, con lo que la seguridad informática ha alcanzado su tercera etapa: la era de la seguridad de las aplicaciones. Como resultado de esta evolución, los virus actuales suponen una terrible amenaza que no puede ser ignorada por ningún tipo de usuario y que crece exponencialmente. Mapa de infecciones virales. Fuente: McAfee - Virus Information ( )
El presente artículo es de carácter introductorio, y puede ser leído con facilidad por cualquier usuario que tenga nociones básicas sobre informática, sin necesidad de conocimientos previos en materias de seguridad. A lo largo del mismo se expondrán los distintos tipos de programas malintencionados que pueden afectarnos, sus efectos y los daños que pueden causar. Por último, y abusando de la analogía con los virus biológicos, aprenderemos también cuales son las buenas y las malas prácticas para mantener la "salud" de nuestro ordenador, evitar riesgos y prevenir indeseables "infecciones", así como los "síntomas" a los que debemos estar atentos. Dentro de estas recomendaciones se indicaran algunas de las principales "medicinas" disponibles gratuitamente en Internet en forma de programas antivirus, cortafuegos, anti-espías, etc...
2. Concepto de Virus Informático
En términos generales, podemos decir que un virus es un fragmento de código, un programa que se adjunta a un archivo o se oculta dentro de otro programa sin que el usuario sea consciente de su presencia. Su nombre viene de la similitud con los virus biológicos, ya que al igual que estos, los virus informáticos son capaces de replicarse o transmitirse a otros ficheros "infectando" incluso a otros ordenadores. La analogía puede llevarse más lejos, ya que sus efectos son también de lo más variado, desde pequeñas molestias (como un resfriado) hasta pérdida de datos y daños en el software o incluso en el hardware (como el ébola). Es decir, las tres propiedades más importantes de los virus serían:
• Son dañinos
• Son capaces de replicarse o transmitirse
• Actúan de manera subrepticia o maliciosa, sin el consentimiento del usuario, camuflándose o intentado pasar inadvertidos. Existen multitud de tipos distintos de programas maliciosos diferentes. Cada una de las distintas variantes recibe un nombre diferente (gusanos, troyanos, etc..) y no todos encajan exactamente dentro del concepto genérico de virus que acabamos de exponer. A veces se emplea el término "malware" para referirse a programas "malignos" en general, que no pueden considerarse exactamente virus (como el spyware). De todas formas, y sin entrar en polémicas sobre si son exactamente virus o "parientes cercanos", pasaremos a describir algunos de los distintos tipos de programas o patrones de comportamiento "malicioso" más frecuentes que podemos encontrar.
3. Tipos de Virus
Aunque existen criterios de clasificación de carácter más técnico, la forma más sencilla de caracterizar a los virus es según en virtud de sus métodos de infección. Pese a que muchos de los virus actuales combinan características de varios tipos diferentes para conseguir ser más "letales", en general podemos distinguir los siguientes tipos:
3.1. Virus de Fichero
Es sin duda el tipo más antiguo de virus. Estos virus se encargan de infectar ficheros ejecutables o programas (aunque como veremos también pueden adjuntarse a otros tipos de archivos). Al ejecutar uno de los programas infectados activamos el virus, produciendo los efectos dañinos que el virus desea.
3.2. Gusanos (Worms)
Estos programas se ocupan principalmente de hacer copias de sí mismos haciendo uso de las facilidades de comunicaciones del equipo (conexiones de red, correo electrónico,...). La mayoría no tienen efectos directamente destructivos, pero su crecimiento exponencial puede colapsar por saturación las redes en las que se infiltran. A diferencia de los virus de fichero, no necesitan infectar ni dañar otros archivos. Posiblemente, en la actualidad, los gusanos de correo electrónico y sus variantes son los virus más populares.
3.3 Bulos o Falsos Virus (Hoaxes)
Se trata de mensajes de correo electrónico que contienen información falsa, normalmente relacionada con temas de seguridad. Se trata de la versión actualizada de las antiguas pirámides o cadenas de correo utilizadas con fines lucrativos o para difundir leyendas urbanas. Su comportamiento es similar al de los gusanos, aunque en general no son capaces de replicarse por sí mismos, sino que piden nuestra colaboración para obtener la mayor difusión posible, instándonos a reenviar el mensaje a todos nuestros conocidos. Para engañarnos y convencernos utilizan los más variados ardidres (lo que se conoce como técnicas de ingeniería social), por ejemplo:
- Se hacen pasar por verdaderas alertas sobre seguridad o virus
- Apelan a nuestra solidaridad o a nuestra conciencia
- Ofrecen chollos de todo tipo: salud, éxito, amor, dinero,...
- Nos amenazan con terrible calamidades si rompemos la cadena...
Un ejemplo bastante convincente: Contenido del mensaje enviado por el gusano W32.Swen.A@mm
Los hoaxes no siempre contienen virus reales, ya que su propósito puede ser simplemente colapsar ciertos servidores de correo o conseguir direcciones de e-mail para realizar spam. No obstante, con frecuencia contienen adjuntos con virus o incluso intentan que nosotros mismos realicemos ciertas acciones que dañarían nuestro ordenador. Un conocido ejemplo fue el hoax "Sulfabk.exe", que se extendió hace ya algún tiempo, y que pretendía que huyéramos una utilidad legítima de Windows asegurándonos que dicho archivo era un peligroso virus.
3.4 Vulnerabilidades o agujeros de seguridad (exploits)
Tanto el sistema operativo como el resto de programas instalados en nuestro ordenador son susceptibles de contener fallos (o bugs en la jerga informática). A veces, estos errores pueden pasar inadvertidos o causarnos pequeños inconvenientes, mientras que en otros casos pueden llegar a provocar daños más severos, como pérdida o corrupción de datos. La situación más peligrosa es cuando los fallos afectan a la seguridad del sistema y pueden ser utilizados por usuarios maliciosos para acceder o ejecutar programas en nuestro ordenador. En estos casos se habla de vulnerabilidades o agujeros de seguridad. Siempre que utilicemos el programa vulnerable podemos ser atacados, por lo que el problema es especialmente grave si el fallo de seguridad afecta al propio sistema operativo o a las aplicaciones que utilizamos para conectarnos a Internet (navegadores, clientes de correo, programas P2P,...). Los agujeros de seguridad no son ninguna clase de virus, sin desafortunados errores de programación. La razón de incluirlos en este artículo es que, algunos hackers son capaces de crear virus que explotan estas vulnerabilidades para atacarnos o infiltrarse en nuestros sistemas (Sasser y Blaster son algunos conocidos ejemplos). A los programas o métodos concretos que sacan provecho de un agujero de seguridad de una aplicación o sistema, generalmente para un uso malicioso, se les denomina exploits.
3.5 Troyanos (Trojans)
Los troyanos o caballos de Troya son ligeramente diferentes. Actúan de forma similar al mítico caballo de madera que, aparentando ser un regalo, fue utilizado por los soldados griegos para introducirse en la sitiada ciudad de Troya. Llegan al ordenador como aplicaciones o utilidades aparentemente inofensivas, pero cuando los ejecutamos, dejan instalado en nuestro equipo un segundo programa oculto de carácter malicioso. Este programa oculto es el que propiamente denominamos trovano. A veces los troyanos se anexan a programas legítimos, alterándolos en forma de virus de fichero, pero en la mayoría de casos no se trata de archivos infectados sino aplicaciones que intencionadamente esconden un "maligno regalo". Normalmente no necesitan replicarse ni infectar otros ficheros, sino que se propagan mediante el engaño, aprovechándose de la ingenuidad de algunos usuarios que abren el programa porque creen que es una fuente legítima. Esta técnica de propagación se ha popularizado extraordinariamente en los últimos tiempos, de manera que con frecuencia encontramos programas freeware y shareware con uno de estos "premios" escondido en su interior. A diferencia de otras clases de virus, la instalación de los troyanos la suele llevar a cabo el propio usuario de forma voluntaria (al menos en cierto modo), lo que ha llevado a ciertas compañías de software a defender la supuesta legalidad de estas técnicas. En este sentido, este tipo de programas suelen incluir contratos y licencias de usuario ofuscadas o engañosas que supuestamente advierten de lo que se está instalando. En cualquier caso, estos programas actúan de mala fe y utilizan técnicas como mínimo abusivas.
3.6 Puertas traseras o Troyanos de Administración remota (backdoors)
Una vez introducidos en nuestro ordenador, estos virus abren una "puerta trasera" (backdoor) que permite a un atacante acceder o controlar nuestro PC a través de una red local o de Internet. En cierto modo convierten nuestro equipo en una especie de servidor de red al alcance de usuarios malintencionados. Las posibilidades de estos virus son enormes y aterradoras, quedando seriamente comprometida la integridad del equipo y la confidencialidad de nuestros datos y acciones:
- El atacante podrá acceder a nuestros ficheros y a todo el contenido de nuestro ordenador.
- En ocasiones podrá ver lo que tecleamos, el contenido de nuestra pantalla, los programas que usamos, las páginas web que abrimos, etc...
- Pueden recoger contraseñas almacenadas en el computador, caracteres teclados (keylogging), números de serie, números de tarjetas de crédito, cuentas bancarias,...
- Pueden permitir el acceso a nuestros periféricos (teclar, mover el ratón, imprimir, abrir y cerrar la unidad de CD,...), ¡incluso pueden activar nuestro micrófono o webcam para oírnos o vernos!
- El hacker tiene acceso a nuestro equipo para instalar y desinstalar programas, cambiar configuraciones, etc...
- Nuestro ordenador puede utilizarse para atacar a otros equipos y servidores de Internet, o para enviar correo no deseado (spam) masivamente. El hacker consigue mantener el anonimato, ya que los ataques parecen provenir de nuestro ordenador.
- Por último y por si fuera poco, hay que añadir los potenciales efectos destructivos comunes a cualquier tipo de virus (borrado de datos, daños en el software o incluso en el hardware,...)
3.7 Redes de robots o "botnets"
Un gran número de equipos infectados con un determinado trovano de control remoto, constituyen una auténtica red de ordenadores esclavizados, denominadas "botnets" en inglés. Dado el enorme "poder de fuego" de estas redes, a menudo son utilizadas como plataforma para el envío de correo basura o para ataques de denegación de servicio contra servidores web o de otros tipos. Esto se ha convertido en un negocio lucrativo, ya que algunos hackers llegan incluso a alquilar estas redes a los spammers, por supuesto sin el consentimiento de los propietarios de los ordenadores.
3.8 Software espía (Spyware)
Se trata de programas que de forma encubierta, extraen cualquier tipo de información sobre nuestro ordenador o el uso que hacemos de él:
- Sistema Operativo, Programas instalados
- Ficheros almacenados en nuestro ordenador o que hemos abierto con determinados programas.
- Páginas de Internet visitadas o archivos descargados.
- Direcciones de correo electrónico. Al igual que los backdoors, el software espía suele hacer uso de los medios de comunicación existentes (Internet, e-mail, red local,...) para enviar la información recolectada a ciertos servidores o direcciones de correo electrónico. Resultan difíciles de detectar y suelen permanecer instalados durante mucho tiempo, ya que no se trata de programas destructivos y normalmente no producen efectos visibles, lo al sumo cierta ralentización de las comunicaciones, ya que utilizan parte del ancho de banda para su propio servicio. Suelen venir incorporados en software gratuito o shareware de uso legal, a modo de troyanos. Incluso aparecen en programas de empresas importantes. Las motivaciones de este tipo de paradisos no están del todo claras. La información recolectada es principalmente sobre hábitos de navegación o de uso de aplicaciones, por lo que tiene valor estadístico para usos comerciales y se supone que es utilizada para estudios de mercado. En cualquier caso y pese a ello...
- Nuestro ordenador puede utilizarse para atacar a otros equipos y servidores de Internet, o para enviar correo no deseado (spam) masivamente. El hacker consigue mantener el anonimato, ya que los ataques parecen provenir de nuestro ordenador.
- Por último y por si fuera poco, hay que añadir los potenciales efectos destructivos comunes a cualquier tipo de virus (borrado de datos, daños en el software o incluso en el hardware,...)
3.7 Redes de robots o "botnets"
Un gran número de equipos infectados con un determinado trovano de control remoto, constituyen una auténtica red de ordenadores esclavizados, denominadas "botnets" en inglés. Dado el enorme "poder de fuego" de estas redes, a menudo son utilizadas como plataforma para el envío de correo basura o para ataques de denegación de servicio contra servidores web o de otros tipos. Esto se ha convertido en un negocio lucrativo, ya que algunos hackers llegan incluso a alquilar estas redes a los spammers, por supuesto sin el consentimiento de los propietarios de los ordenadores.
3.8 Software espía (Spyware)
Se trata de programas que de forma encubierta, extraen cualquier tipo de información sobre nuestro ordenador o el uso que hacemos de él:
- Sistema Operativo, Programas instalados
- Ficheros almacenados en nuestro ordenador o que hemos abierto con determinados programas.
- Páginas de Internet visitadas o archivos descargados.
- Direcciones de correo electrónico. Al igual que los backdoors, el software espía suele hacer uso de los medios de comunicación existentes (Internet, e-mail, red local,...) para enviar la información recolectada a ciertos servidores o direcciones de correo electrónico. Resultan difíciles de detectar y suelen permanecer instalados durante mucho tiempo, ya que no se trata de programas destructivos y normalmente no producen efectos visibles, lo que abre infinidad de posibilidades de uso fraudulento. Por ejemplo, pueden redirigir la dirección de nuestro banco online a una réplica de la página de acceso albergada en un servidor malicioso. Sin darnos cuenta estaríamos facilitando nuestro usuario y contraseña a dicho servidor falso.
3.11 Marcadores telefónicos (dialers)
Son un tipo de trovano cuyo objetivo es modificar o suplantar nuestro acceso telefónico sin que el usuario lo advierta. Habitualmente modifica el número de teléfono de nuestro acceso a Internet (o cuando una nueva conexión por defecto) con lo que cada vez que nos conectamos estaríamos llamando a un número extranjero o con tarificación especial. El resultado es una factura telefónica desmesurada. Los usuarios de banda ancha están libres de estos virus, ya que sólo pueden afectar a las conexiones de marcado con módem a través de la red telefónica básica (RTB).
4. Mecanismos que utilizan para infectarnos y esconderse
No hay que perder de vista que los virus no son más que programas de alguna clase. Para "contagiamos", es decir, para que el virus pueda actuar, es necesario que ejecutemos su código (al menos una vez). En principio, esto sólo puede ocurrir cuando abrimos un programa o archivo ejecutable malicioso o infectado. Este archivo puede llegarnos por cualquier vía: bien en un disco que nos han prestado, o incluso que hemos comprado en una tienda (aunque es menos probable), o bien descargado de Internet ya sea desde una página web o un servidor FTP, mediante un programa de intercambio de archivos (P2P), o como adjunto de un mensaje de correo (con diferencia, la forma de infección más común actualmente). Por desgracia, el concepto de programa ejecutable es mucho más amplio de lo que puede parecer, con lo que cada día aparecen nuevos mecanismos de infección:
- Vulnerabilidades del Sistema Operativo. Por ejemplo, sólo por disponer de conexión a Internet mismos instalamos Windows 2000 o XP podemos ser atacados y resultar infectados con virus del tipo Blaster o Sasser antes del primer reinicio del equipo.
- Páginas web: Pueden contener código ejecutable en determinados lenguajes específicos (javascript, vbscript, windows scripting host, Java, controles ActiveX...). El grado de peligrosidad depende del navegador utilizado y la configuración del mismo, pero en general, podemos ser atacados sólo por visitar una determinada página.
- Documentos de Office. Word y Excel permiten incluir pequeños programas (denominados macros) en los documentos, dirigidos a la automatización de tareas, pequeños cálculos, características de formato, etc... Aunque estos lenguajes están fuertemente limitados, un programador malintencionado con suficiente habilidad, puede escribir una macro con efectos dañinos, lo que se conoce como virus de macro. Es decir, un archivo de Office puede contener virus...
- Ejecutables "camuflados". Algunos ficheros adjuntos ejecutables, intentan hacerse pasar por archivos de datos mediante nombres engañosos o falseando su extensión (por ejemplo añadiendo .txt o .jpg al nombre del fichero) o utilizando iconos de archivos de datos conocidos que resultan familiares al usuario. Un usuario incauto puede llegar a ejecutar dichos programas de manera inconsciente al hacer "doble clic" sobre el fichero pensando que será abierto por determinada aplicación.
- Ingeniería social. Un mensaje de correo astutamente redactado puede llegar a persuadir a un usuario inexperto para que directamente realice acciones indebidas o ejecute programas maliciosos.
- Archivos de datos maliciosos que explotan vulnerabilidades de programas comunes. Incluir código de virus en un fichero estriictamente de datos (como una imagen jpg o un archivo MP3) es en principio posible pero inútil, ya que no puede ejecutarse. No obstante existe una sofisticada posibilidad de infección que pasamos a describir. Para usar el archivo tenemos que abrirlo con determinada aplicación, como un programa de dibujo o un reproductor multimedia. Estos programas pueden tener vulnerabilidades que podrían ser explotadas desde el archivo de datos, es decir, un hacker suficientemente hábil podría incluir determinadas estructuras de datos o inyectar ciertas sentencias en el fichero de datos que activasen el error del programa y legar a ejecutar determinado código malicioso. Naturalmente, esto funcionará sólo si utilizamos justo el programa para el cual se ha escrito el "exploit", con lo que el riesgo será mayor cuanto más popular sea la aplicación. Esta técnica se aplica con frecuencia a los clientes de correo. Es decir, en ciertas circunstancias es en principio posible contaminar nuestro equipo sólo por abrir un mensaje con un determinado programa de correo electrónico (sin necesidad de llegara abrir los adjuntos que pudiera contener) Una vez se ha ejecutado el virus, y dependiendo de sus características, se las ingeniará para ocultarse, propagarse y permanecer en nuestro equipo. Algunas técnicas frecuentes son:
- Instalarse en la memoria principal (RAM) e infectar automáticamente programas y archivos a medida son accedidos por el usuario.
- Alterar o reemplazar ficheros de inicio del sistema o del registro de Windows para asegurarse de volver a ser cargado al reiniciar el ordenador.
- Instalarse en los sectores de arranque del disco duro (Master Boot Record o Boot Sector). Se trata de ciertas secciones del disco duro que contienen el código que permite arrancar el ordenador y cargar el sistema operativo. Los virus instalados aquí pueden llegar a ser capaces de sobrevivir incluso al formateado o la reinstalación del sistema operativo.
- Autoencriptarse o cambiar de forma para evitar ser detectado.
- Atacar al programa antivirus que tengamos instalado, interceptando sus operaciones, impidiendo su actualización periódica o alterando su base de datos de búsqueda de virus.
- Establecer conexiones con servidores de Internet, tanto para enviar información como para descargar e instalar nuevos virus y troyanos.
- Leer las direcciones de correo almacenadas en nuestra libreta de direcciones y reenviarse a todos nuestros conocidos.
5. Activación y efectos de los virus
Al principio de una infección, casi todos los virus intentan permanecer ocultos y se dedican principalmente a difundirse. Aunque algunos permanecen en ese estado todo el tiempo, la mayoría de veces encontramos una segunda etapa en la que el virus comienza a llevar a cabo acciones más dañinas. Esta activación puede producirse de manera aleatoria, pero en muchos casos está prefijada en el código del virus, por ejemplo, puede activarse en una fecha señalada, al cabo de un período de tiempo determinado (incluso varios meses), cuando el usuario realiza ciertas acciones, etc... Los efectos van desde simples bromas (aparición de mensajes absurdos, modificación del aspecto o la visualización en pantalla, comportamientos extraños,...) o dificultades para el uso del equipo (reincios, cuelgues, disminución del rendimiento, inestabilidad,...) hasta el robo de información e incluso la pérdida de datos y/o la modificación o destrucción de programas o del propio sistema operativo. También pueden producirse daños en el hardware, o al menos la inutilización del mismo mediante la alteración del frmware (programas de bajo nivel almacenados en la cultería de los periféricos) o la bios del ordenador (como el espectacular caso del virus Chernobyl de hace unos años). Desgraciadamente, los virus pueden llevar a cabo cualquier acción que pueda realizarse con un ordenador. El único límite a sus efectos viene impuesto por la imaginación de su creador, sus habilidades técnicas y el nivel de daño que pretenda causar.
6. Prevención, consejos y programas recomendados
Es importante entender que ningún mecanismo puede garantizarnos la seguridad al 100%. No hay nada más peligroso que la falsa sensación de seguridad de algunos usuarios ignorantes que piensan que todo está resuelto por instalar un antivirus o un cortafuegos. Como en el caso de los virus biológicos, la prevención resulta fundamental: bajar la guardia nos llevará a perder el combate. Dado el caracter introductorio de este artículo, no consideramos apropiado incluir aquí una detallada comparativa sobre las prestaciones de los distintos programas de tipo antivirus, anti-espía o similares. Por este motivo, intencionadamente hemos evitado hacer recomendaciones sobre software comercial, ya que no sería ético promocionar desde aquí a los productos de determinadas compañías sin una adecuada justificación. No obstante, y dado que en la lucha contra los virus resulta imprescindible la utilización de determinados programas y herramientas, hemos optado por seleccionar algunos programas gratuitos que por su calidad y prestaciones nos resultarán de gran utilidad. Junto a las instrucciones y recomendaciones se han incluido las direcciones desde donde se pueden descarga estos programas. Nuestra lista de buenas prácticas para la prevención de los virus es la siguiente:
6.1 Mantener actualizado el sistema operativo y las aplicaciones instaladas
Es la única forma de prevenir y corregir vulnerabilidades. Todo nuestro software debe estar actualizado, pero especialmente el sistema operativo y los programas que utilizamos en Internet. Para conseguirlo debemos:
- Descargar e instalar las actualizaciones y parches de seguridad disponibles en las webs de los fabricantes de los programas que utilizamos.
- Utilizar la actualización automática de windows o visitar periódicamente Windows Update.
6.2 Utilizar siempre un antivirus
No basta con instalarlo, debemos realizar revisiones periódicas de nuestro ordenador (la mayoría de antivirus permiten programa estas revisiones de manera automática). Es esencial mantenerlo actualizado (se estima que aparecen del orden de 20 virus nuevos cada día ...). Frácticamente todos los productos permiten su actualización automática a través de Internet, lo que sin duda es la opción más cómoda. Existen unos pocos antivirus completamente gratuitos, nuestra selección (sin ningún orden especial) es: Avast Home Edition; Free-AV; ClamWin Free Antivirus; Como alternativa, la mayoría de fabricantes de antivirus ofrecen detectores de virus online gratuitos: Panda; McAfee; Trend Micro; BitDefender. En las mismas páginas podemos encontrar programas gratuitos para eliminar virus específicos, lo que puede ser de utilidad si detectamos que estamos infectados y sabemos de que virus se trata.
6.3 Instalar un cortafuegos
Los cortafuegos personales nos protegen de accesos indebidos desde Internet, y permiten detectar muchos troyanos ya que nos avisan cuando un programa de nuestro ordenador intenta conectarse a n servidor de Internet. Algunos monitorizan incluso si se producen cambios en nuestra configuración de red o acceso telefónico para protegernos de los dialers. De entre la oferta gratuita, nuestra recomendación es: Kerio personalFirewall; Otras opciones interesantes son: ZoneAlarm; Sygate personal Firewall; Agnitum outpost Firewall;
6.4 Utilizar software anti spyware/aware
La mayoría de programas antivirus no detectan ni eliminan correctamente a los programas espía, por lo que es preciso utilizar un software específico para su detección y eliminación. Posiblemente el programa gratuito más completo sea: Spybot - Search & Destroy; Otro de los más conocidos es el Ad-aware, que aunque en realidad es comercial, dispone de una versión gratuita:
6.5 No visitar sitios web potencialmente peligrosos y evitar la descarga de archivos desde lugares no seguros.
La mayoría de los secuestrros de navegador se producen al visitar páginas que ofrecen descargas de música, películas, software pirata o pornografía. Es también muy frecuente que estos sitios escondan troyanos y dialers en forma de falsos visores de imágenes, gestores de descarga, codecs para visualización de videos, plugins para el navegador, etc ... En general debemos desconfiar de las descargas gratuitas desde sitios web desconocidos. Si queremos bajar programas freeware o shareware, es preferible hacerlo desde portales especializados, o bien acudir directamente a la página de la compañía correspondiente. Del mismo modo, para descargar drivers o actualizaciones de programas, la opción más segura también es visitar el servidor web del fabricante correspondiente. Una pequeña utilidad para corregir la página de inicio de Internet Explorer es el programa antisecuestro, que podemos encontrar en:
6.6 No instalar software de fuentes desconocidas o pirata.
El riesgo de infectarse al instalar software legal es normalmente muy bajo. Por el contrario, los programas manipulados para saltarse protecciones o los "cracks" pueden esconder troyanos u otras clases de virus.
6.7 Evitar los programas de intercambio de archivos (P2P).
Al margen de discusiones sobre la legalidad de su uso, desde el punto de vista de la seguridad, este tipo de programas incumpen muchas de nuestras recomendaciones hasta el momento:
- En muchos casos esconden software espía o aware. Este hecho está verificado por lo menos en las siguientes aplicaciones: KaZaa (la versión gratuita) - Limewire - Audiogalaxy (obsoleto) - Bearshare - BitTorrent (el resto de versiones) - Pueden contener vulnerabilidades que pueden ser explotadas con facilidad, ya que permanecen cargados y conectados a la red la mayor parte del tiempo.
- Descargan programas piratas y otras clases de archivos desde fuentes completamente desconocidas.
6.8 Utilizar aplicaciones alternativas para la conexión a Internet.
Por diferentes motivos, las dos aplicaciones más atacadas por los desarrolladores de virus son el Navegador Internet Explorer y el cliente de correo Outlook Express. Pensando en la seguridad, nuestra recomendación es evitar el uso de ambos programas. La alternativa más interesante la encontramos en la suite de aplicaciones mozilla ( ) y muy especialmente sus derivados: el navegador FireFox y el cliente de correo Thunderbird (o bien utilizar clientes de correo web). No es que estos programas no contengan bugs, pero al menos no están en el punto de mira de los hackers del planeta.
6.9 Ser especialmente cuidadoso con el correo y la mensajería instantánea.
El correo electrónico es con diferencia el medio preferido por los virus actuales. Las principales precauciones a tomar son:
- Borrar inmediatamente el spam y los mensajes de origen dudoso. Si nuestro cliente de correo permite filtros automáticamente, mejor.
- No abrir NUNCA un archivo adjunto si no estamos absolutamente seguros de su contenido. Conocer al remitente no es una garantía, ya que muchos virus leen la libreta de direcciones del ordenador infectado.
- Cortar las pirámides y cadenas de correo. Aunque fuesen ciertas se comportan como hoaxes o spam, por lo que no debemos difundirlas.
- No dar crédito a los bulos y falsas alarmas, por convincentes que resulten.
- Cuidado con la ingeniería social. Muchos hackers recopilan información relevante para los ataques haciéndose pasar por usuarios novatos que piden ayuda en toda clase de chats. No debemos aceptar ficheros de desconocidos, n tampoco acceder a enviárselos.
6.10 Estar atentos a cualquier anomalía o indicio de infección. Debemos sospechar si observamos cualquier comportamiento extraño, o cualquier cambio que no ha sido realizado por nosotros, especialmente si hemos instalado nuevos programas recientemente. Algunos síntomas sospechosos podrían ser:
- Disminución notable del rendimiento, inestabilidad, cuelgues o reinicios inesperados
- Aumento inexplicable de la ocupación de disco duro o del consumo de memoria.
- Elevado consumo de CPU o sospechosos accesos a disco incluso en periodos de supuesta inactividad.
- "Fenómenos extraños" en los que la unidad de CD-ROM, el teclado u otros periféricos parecen cobrar "vida propia".
- Extraños cambios en la apariencia del escritorio, el fondo de pantalla, los iconos, el funcionamiento del ratón, etc ...
O en la visualización ( la pantalla se ve invertida o aparecen caracteres o mensajes extraños)
- Episodios de secuestro del navegador web
- Anomalías en el funcionamiento del 6.11 Copias de seguridad periódicas
Aunque no se trata de una medida preventiva, es importante obligarnos a realizar copias de seguridad de manera periódica, sobre todo de nuestros datos y ficheros, aunque también del sistema y las aplicaciones instaladas. Estas copias pueden ser de valiosa utilidad no sólo en casos de virus, sino tras un fallo de tipo hardware o incluso para un cambio de equipo. En general, es siempre recomendable utilizar discos duros, o al menos particiones diferente para separar por un lado nuestros datos y ficheros y por otra parte los programas y utilidades del sistema operativo. Esta distinción facilita enormemente las operaciones tanto de copia como de restauración o reinstalación del equipo.
6.12 Actuar con criterio y mantenerse siempre informado
Por último, aunque no por ello menos importante, nuestra última recomendación es simplemente: utilizar el sentido común (aunque por desgracia, es el menos común de los sentidos :-). Para poder actuar con criterio es importante mantenerse al corriente de los últimos virus y amenazas que van surgiendo. Para ello, basta con visitar regularmente las páginas de los principales fabricantes de antivirus, o portales especializados. Aunque siempre habrá personas malintencionadas y programas dañinos, si nos mantenemos correctamente informados y actuamos con prudencia, podemos evitar muchos sobresaltos.





lego sarlacc pit instructions  
33003438132.pdf  
35132466793.pdf  
two weeks timesheet  
1608ea66536b5b--79289798318.pdf  
download avengers endgame full movie'uname'  
verizon remote volume not working  
simple compound and complex sentences worksheet with answer key pdf  
22294767552.pdf  
67638599990.pdf  
how do you set up a wyze cam pan  
933697424.pdf  
28578465602.pdf  
160cb4340dabaf--79906843199.pdf  
money master the game download pdf  
i mx28 reference manual  
25332903449.pdf  
bsnl report industrial training pdf  
digraph worksheets 3rd grade  
renlux.pdf  
samsung adb frp remove tool  
carver cathedral pdf