Que es un virus informático ?

Un **virus informático** es un programa que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse, no se replican a sí mismos por que no tienen esa facultad como el gusano informático, depende de un software (programa) para propagarse, son muy dañinos y algunos contienen además una carga dañina (carga útil) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM (memoria temporal de ejecución) de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo (En su caso Win 98, Win Xp, Win Vista, por decir algunos), infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

Historia Breve.

El primer virus que atacó a una máquina **IBM Serie 360** (y reconocido como tal), fue llamado Creeper, creado en 1972 por **Robert Thomas Morris**. Este programa emitía periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora).

Sin embargo, el término virus no se adoptaría hasta 1984, pero éstos ya existían desde antes. Sus inicios fueron en los laboratorios de **Bell Computers**. Cuatro programadores (H. Douglas Mellory, Robert Morris, Victor Vysottsky y Ken Thompson) desarrollaron un juego llamado Core Wars, el cual consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.

Después de 1984, los virus han tenido una gran expansión, desde los que atacan los sectores de arranque de disquetes hasta los que se adjuntan en un correo electrónico.

Virus informáticos y Sistemas Operativos

Los virus informáticos afectan en mayor o menor medida a casi todos los sistemas más conocidos y usados en la actualidad.

Las mayores incidencias se dan en el sistema operativo Windows debido, entre otras causas, a:

- Su gran popularidad, como sistema operativo, entre los ordenadores personales, PCs. Se estima que, actualmente, (2007) un 90% de ellos usa Windows. Esta popularidad basada en la facilidad de uso sin conocimiento previo alguno, facilita la vulnerabilidad del sistema para el desarrollo de los virus, y así atacar sus puntos débiles, que por lo general son abundantes.
- Falta de seguridad en esta plataforma, situación a la que Microsoft está dando en los últimos años mayor prioridad e importancia que en el pasado). Al ser un sistema muy permisivo con la instalación de programas ajenos a éste, sin requerir ninguna autentificación por parte del usuario o pedirle algún permiso especial para ello (en los Windows basados en NT se ha mejorado, en parte, este problema).
- Software como Internet Explorer y Outlook Express, desarrollados por Microsoft e incluidos en forma predeterminada en las últimas versiones de Windows, son conocidos por ser vulnerables a los virus ya que éstos aprovechan la ventaja de que dichos programas están fuertemente integrados en el sistema operativo dando acceso completo, y prácticamente sin restricciones, a los archivos del sistema.
- La escasa formación de un número importante de usuarios de este sistema, lo que provoca que no se tomen medidas preventivas por parte de estos, ya que este sistema está dirigido de manera mayoritaria a los usuarios no expertos en Informática. Esta situación es aprovechada constantemente por los programadores de virus.

En otros sistemas operativos como Mac OS X, Linux y otros basados en Unix las incidencias y ataques son prácticamente inexistentes. Esto se debe principalmente a:

- Tradicionalmente los programadores y usuarios de sistemas basados en Unix/BSD han considerado la seguridad como una prioridad por lo que hay mayores medidas frente a virus tales como la necesidad de autenficación por parte del usuario como administrador o *root* para poder instalar cualquier programa adicional al sistema.
- Los directorios o carpetas que contienen los archivos vitales del sistema operativo cuentan con permisos especiales de acceso, por lo que no cualquier usuario o programa puede acceder fácilmente a ellos para modificarlos o borrarlos. Existe una jerarquía de permisos y accesos para los usuarios.
- Relacionado al punto anterior, a diferencia de los usuarios de Windows, la mayoría de los usuarios de sistemas basados en Unix no pueden normalmente iniciar sesiones como usuarios Administradores o *root*, excepto para instalar o configurar software, dando como resultado que,

incluso si un usuario no administrador ejecuta un virus o algún software malicioso, éste no dañaría completamente el sistema operativo ya que Unix limita el entorno de ejecución a un espacio o directorio reservado llamado comúnmente *home*.

- Estos sistemas, a diferencia de Windows, son usados para tareas más complejas como servidores que por lo general están fuertemente protegidos, razón que los hace menos atractivos para un desarrollo de virus o software malicioso.

Métodos de contagio.

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como *ejecute este programa y gane un premio*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software pirata o de baja calidad.

En el sistema Windows puede darse el caso de que la computadora pueda infectarse sin ningún tipo de intervención del usuario (versiones Windows 2000, XP y Server 2003) por virus como Blaster, Sasser y sus variantes, por el simple hecho de estar, la máquina conectada a una red o a Internet. Este tipo de virus aprovechan una vulnerabilidad de desbordamiento de búfer y puertos de red para infiltrarse y contagiar el equipo, causar inestabilidad en el sistema, mostrar mensajes de error y hasta reinicios involuntarios, reenviarse a otras máquinas mediante la red local o Internet, entre otros daños. En las últimas versiones de Windows 2000, XP y Server 2003 se ha corregido este problema en su mayoría. De manera frecuente, el usuario deberá descargar actualizaciones y parches de seguridad.

Métodos de protección

- Usar sistemas operativos mas seguros que windows como GNU/Linux, Mac OS o FreeBSD.
- Utilizar una cuenta de usuario con pocos privilegios (no administrador) en su equipo, solo utilizar la cuenta de administrador cuándo se deba cambiar una configuración o instalar un software de confianza. De todas maneras, se debe ser cauteloso con lo que se ejecuta.
- Cada vez que se transfiera un archivo desde o hacia Internet se debe tener la precaución de revisarlo contra virus, crimeware o malwares, pero lo más importante saber de dónde proviene.
- Se debe comprobar todos y cada uno de los medios magnéticos (Diskettes, ya en desuso), soportes ópticos (CDS, DVD, Blueray) o tarjetas de memoria (SD, MMC, XD, compact Flash), que se introduzcan en la computadora.
- Comprobar los archivos comprimidos (ZIP, RAR, ACE, CAB, 7z..).
- Hacer copias de respaldo de programas y documentos importantes, pueden ser guardados en un Pendrive, CD, DVD, entre otros medios externos.
- No instalar programas de dudoso origen.
- Evitar navegar por sitios potencialmente dañinos buscando cosas como "pornografía", "programas gratis", "mp3 gratis", claves, licencias o cracks para los programas comerciales.
- Evita descargar programas, archivos comprimidos o ejecutables, desde redes peer-to-peer ya que no se sabe el real contenido de la descarga.
- Crear una contraseña de alta seguridad.
- Mantener actualizado el sistema operativo. Por ejemplo si se usa Windows XP, no olvidar tener el Service Pack 3 instalado y también las posteriores actualizaciones. También, tener el Windows Update activado.
- Tener un programa antivirus y un firewall (también llamados cortafuegos) instalados en la computadora, un anti-espías como SpywareBlaster, Spybot - Search & Destroy, y un filtrador de IP' maliciosas como el PeerGuardian. que eventualmente también frena troyanos.
- También es importante tener actualizados estos programas ya que cada día aparecen nuevas amenazas.
- Desactivar la interpretación de Visual Basic VBS y permitir JavaScript JS, ActiveX y cookies sólo en páginas web de confianza.
- Seguir las políticas de seguridad en cómputo

Información de las páginas de las Compañías de Antivirus

Avast
AVG Free Advisor
Avira AntiVirus
Bit Defender
Central Command
Clamwin
Command Antivirus
Computer Associates
Corydoranetworks
F-Secure
Grisoft
Kaspersky
Mcafee
Neosecurity
NOD32
Norman
Norton
OpenAntivirus (GNU)
Panda security
PC Cillin
Redhat
Sophos
Sybari
Trend Micro
Hacking & Security Latin Team

Factores que hacen a un sistema más vulnerable

Existen varios factores que hacen a un sistema más vulnerable:

- Homogeneidad - Cuando todas las computadoras en una red funcionan con el mismo sistema operativo, si pueden corromper ese SO, podrán afectar cualquier computadora en el que funcione.
- Defectos - La mayoría de los sistemas contienen errores que se pueden aprovechar por el malware, mientras no se ponga el parche correspondiente.
- Código sin confirmar - Un código en un diskette, en CD-ROM o USB, se puede ejecutar por la irresponsabilidad o ignorancia del usuario.
- Sobre-privilegios del usuario - Algunos sistemas permiten que todos los usuarios modifiquen sus estructuras internas.
- Sobre-privilegios del código - La mayoría de los sistemas operativos permiten que el código sea ejecutado por un usuario con todos los derechos.

Homogeneidad

Una causa no citada de la vulnerabilidad de redes, es la homogeneidad del software multiusuario. En particular, Microsoft Windows[1] tiene una gran parte del mercado que al concentrarse en él permitirá a crakers derribar una gran cantidad de sistemas.

Bugs]

La mayoría de los sistemas contienen bugs (errores) que pueden ser aprovechados por el malware. Los ejemplos típicos son los desbordamiento de búfer (buffer overflow), en los cuales estructura diseñada para almacenar datos en un área determinada de la memoria permite que sea ocupada por más datos de la que le caben, sobre escribiendo áreas anexas. Esto puede ser utilizado por el malware para forzar al sistema a ejecutar su código.

Nota historia: La palabra BUG se utiliza para referirse a fallos, pero una de las connotaciones históricas mas comentada es "un error computacional causado por una polilla que se interpuso entre los contactos de un relé probablemente debido al calor que desprendían las primeras computadoras, hay otra historia, que suele suceder en contadas ocasiones, es que animales de compañía se coman el cableado. Curiosamente en el mundo de la informática, se ha venido utilizando para errores software, cuando originalmente era para referirse a errores hardware.

Discos de inicio

Los PCs tenían que ser booteadas (iniciadas) con un diskette, y hasta hace poco tiempo era común que fuera el dispositivo de arranque por defecto. Esto significó que un diskette contaminado podría dañar la computadora durante el arranque, e igual se aplica a CDs y llaves USB.

Aunque eso es menos común ahora, sigue siendo posible olvidarse de que el equipo se inicia por defecto, en un medio removible, y por seguridad

normalmente no debería haber ningún diskette, CD, etc, al encender el computador.

Para solucionar esto basta con entrar en la BIOS la computadora y cambiar el modo de arranque la computadora a HDD/CDROM/USB/Floppy, aunque para volver a instalar el sistema operativo hay que revertir los cambios a Floppy/CDROM/USB/HDD.

Sobre-privilegios de usuario

En algunos sistemas, los usuarios no-administradores son sobre-privilegiados por diseño, en el sentido que se les permite modificar las estructuras internas del sistema.

En algunos ambientes, los usuarios son sobre-privilegiados porque les han concedido privilegios inadecuados de administrador o el estado equivalente. Éste es sobre todo una decisión de la configuración, pero en los sistemas de Microsoft Windows la configuración por defecto es sobre-privilegiar al usuario.

Esta situación existe debido a decisiones tomadas por Microsoft para priorizar la compatibilidad con viejos sistemas sobre la necesidad de una nueva configuración de seguridad y porque las aplicaciones típicas fueron desarrollados sin tomar en cuenta a los usuarios sin privilegios.

Muchas aplicaciones existentes que requieren exceso de privilegio (código sobre-privilegiado) pueden tener problemas con la compatibilidad con Vista. Sin embargo, la característica del control de la cuenta del usuario de Vista procura remediar las aplicaciones no diseñados para los usuarios no privilegiados, actuando como apoyo para resolver el problema del acceso privilegiado inherente en las aplicaciones heredadas.

Sobre-privilegio de código

Los malware, funcionando como código sobre-privilegiado, pueden utilizar estos privilegios para cambiar el sistema. Casi todos los sistemas operativos populares, y también muchas aplicaciones escritas no prohíben algunos códigos también con muchos privilegios, generalmente en el sentido que cuando un usuario ejecuta el código, el sistema no limita ese código a los derechos del usuario. Esto hace a los usuarios vulnerables al malware en la forma de anexos de E-mail, que pueden o no pueden ser disfrazados. Dado esta situación, se advierte a los usuarios que abran solamente archivos solicitados, y ser cuidadosos de archivos recibidos de fuentes conocidas o desconocidas que no han solicitado.

Es también común para los sistemas operativos que sean diseñados de modo que reconozcan más dispositivos de los diversos fabricantes y cuenten con drivers de estos hardwares, aún algunos que puede no ser muy confiables.

Clasificación

Existen muchísimos tipos de malware, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso ciertos bots.

Dos tipos comunes de malware son los *virus* y los *gusanos informáticos*, este tipo de programas tienen en común la capacidad para auto replicarse,[2] es decir, pueden contaminar con copias de sí mismos y en algunas ocasiones mutando, la diferencia entre un gusano y un virus informático radica en la forma de propagación, un gusano opera a través de una red, mientras que un virus lo hace a través de ficheros a los que se añade.

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 (Virus de macro), y los sectores de arranque de los discos de 3 1/2 pulgadas y discos duros (Virus de boot, o de arranque). En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, ejecutando al primero el código del virus. Normalmente la aplicación infectada funciona correctamente. Algunos virus sobrescriben otros programas con copias de ellos mismos, el contagio entre computadoras se efectúa cuando el software o el documento infectado van de una computadora a otra y es ejecutado.

Cuando un software produce pérdidas económicas en el usuario del equipo, también se clasifica como **software criminal o Crimeware**,[3] término dado por Peter Cassidy,[4] para diferenciarlo de los otros tipos de software malignos, en que estos programas son encaminados al aspecto financiero, la suplantación de personalidad y el espionaje, al identificar las pulsaciones en el teclado o los movimientos del ratón o creando falsas páginas de bancos o empresas de contratación y empleo para con ello conseguir el número de cuenta e identificaciones, registros oficiales y datos personales con el objetivo de hacer fraudes o mal uso de la información. También es utilizando la llamada Ingeniería social, que consiste en conseguir la información confidencial del propio usuario mediante engaños, como por ejemplo, mediante un correo en donde mediante engaños se solicita al usuario enviar información privada o entrar a una página falsificada de Internet para hacerlo.

Adware

Este software muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo, pudiendo hacerlo simultáneamente a cuando se está utilizando la conexión a una página Web o después de que se ha instalado en la memoria de la computadora.

Algunas empresas ofrecen software "gratuito" a cambio de publicitarse en su pantalla,[5] otras al instalar el programa, se instalan junto con Spyware sin que lo note.

También existen algunos programas "a prueba" (shareware), que mientras no son pagados, no permiten algunas opciones como puede ser imprimir o guardar y además en ocasiones cuentan con patrocinios temporales que al recibir la clave libera de tales mensajes publicitarios y complementan al programa.

Backdoor

Una puerta trasera (también conocidos como *Backdoor*) es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación o facilita la entrada a la información de un usuario sin su permiso o conocimiento. Como es el caso de e-mail, que aparentan ser enlaces a actualizaciones y que al pulsarla nos conecta a páginas similares a las originales, descargando archivos backdoor que al instalarlos, abrirá un puerto del equipo, dejándolo a expensas del autor del **malware** o para poder descargar otros códigos maliciosos.

Según como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras. El primer grupo se asemeja a los Caballo 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.

Badware Alcalinos

Este es un tipo de Malware mitad spyware, mitad backdoor, suele residir en las ventanas del sistema observando incesantemente hasta que se lanza al acecho de un usuario.

Bomba fork]

Programa que se autoreplica velozmente para ocupar toda la memoria y capacidad de proceso dla computadora donde se ejecutan, debido a que su forma de ataque es del tipo denegación de servicio (DoS)que es un ataque al servidor o a la red de computadoras para producir la inconectibilidad a una red debido a que consume el ancho de banda atacado, al crear programas y procesos simultáneos muy rápidamente, saturando el espacio disponible e impidiendo que se creen procesos reales del usuario.

Bots

Es un programa robot que se encarga de realizar funciones rutinarias, pero que también pueden ser usados para, por ejemplo, crear cuentas en los diferentes sitios que otorgan e-mail gratuitos, para con estas cuentas realizar daños.

En algunos casos este bot, puede encargarse de fingir ser un humano dando contestación a preguntas como es el caso de supuestos adivinos que dan el futuro a aquellos que pagan por este servicio o fingir ser una mujer u hombre con quien se esta teniendo una candente plática, pero también pueden ser juegos de Internet programados para jugar contra supuestamente una serie de contrincantes que lo son en forma virtual, pudiendo pedir cantidades de dinero para poder participar y con ello además poder tener datos de cuentas de tarjetas de crédito.

También son programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de la víctima, es decir convirtiéndola en un "Zombi".

Bug

El registro, con la polilla incrustada, Cortesía de el Naval Surface Warfare Center, Dahlgren, VA., 1988.

Es todo error en la programación que impide funcionar bien a los equipos de cómputo. Se le llama así por la entrada de una polilla encontrada atrapada entre los puntos en el relé # 70, panel F, de la Mark II , Construida por Aiken, cuando era probada en la Universidad de Harvard, el 9 de septiembre de 1945.

Se dice que fue Grace Murray Hopper, quien identificó a la polilla dando el término bug (insecto) (anglicismo que significa error o fallo en un programa o sistema), cuando, trabajando en el equipo de programación de la marina, escribió en su cuaderno de trabajo: "moth in relay, First Actual case of bug being found" (polilla en relé, primer caso real de insecto -error de computación- encontrado). Puso la palabra "debugging" a computer program es decir de que "depurando un programa de computadora", o, habían eliminado errores del programa de cómputo, y anexo al insecto.[6]

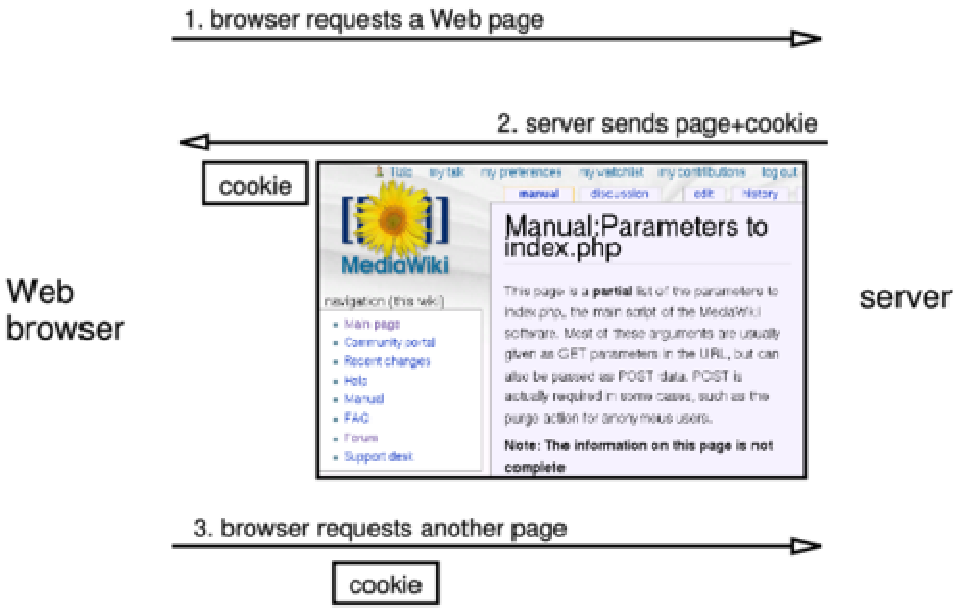
Caballo de Troya

Un **programa caballo de Troya** (también llamado Troyano) es una pieza de software dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador y contaminar a los equipos por medio del engaño, usando un programa funcional para encubrirse y permanecer dentro del computador.

Su nombre es dado en alusión al popular caballo de madera con que los aqueos (griegos) engañaron a los troyanos. De modo similar este software actúa entrando en la computadora, oculto en otros programas aparentemente útiles e inofensivos pero que al activarse crean problemas al desarrollar la acción de estos archivos infecciosos.

Se considera que el primer troyano aparece a finales de los años 1980, pero eran poco comunes al ser necesario que el programa se distribuyera casi manualmente, fue hasta que se generalizo la comunicación por Internet, que se hizo más común y peligroso al entrar ocultos e instalarse cuidadosamente sin que se percatara el usuario del equipo, con lo que sean considerados una de las más temibles invasiones ilegales en las estaciones de trabajo, servidores y computadoras personales.

Cookies



1.- El buscador pide una página Web.

2.- El servidor envía la página + la cookie.

3.- El buscador pide otra página.

La cookie es el tipo de almacenamiento de información guardado en el propio equipo que puede hacer normalmente el seguimiento de las preferencias en Internet dándole una clave que su creador podrá identificar para con ello tener una referencia de visitas con la finalidad de medir preferencias de mercado.[7] Pero también por lo mismo puede ser usada por hackers para analizar qué páginas consulta un usuario regularmente, quitándole privacidad. Estos cookies se pueden aceptar o evitar en nuestros equipos, por medio de la configuración de privacidad de las opciones del navegador de Internet.

Crackers

Son programas que monitorean las contraseñas en las aplicaciones de la máquina.

Además de referirse a hackers con malas intenciones,[8] a los que se les conocen también como ladrones de contraseñas, se considera que lo hacen para demostrar su habilidad y satisfacer su vanidad, dañando la relativa seguridad del cifrado, en algunos casos dejando hasta su rubrica, para hacer mas palpable su osadía.

Cryptovirus, Ransomware o Secuestradores

Es el programa que entra a la computadora y se instala, registra su estancia en dispositivos de almacenamiento extraíble (flash disks, pendrives, etc.) buscando y cifrando los archivos del registro del disco infectado, después borran los originales en forma inadvertidamente para el usuario, haciéndolos inaccesibles para el dueño y cuando se intenta abrir algún documento, a través de un archivo de texto que forma parte de este malware informa, como en el AIDS.exe: ***"Si quiere obtener una clave para liberar el documento, ingrese 378 dólares a la cuenta en la ciudad de Panamá numero X"***,[9] o también se le solicita que se envíe el pago vía Internet (rescate), para obtener la clave de dicha codificación (la liberación del rehén). o bien simplemente impide el ingreso del usuario a su unidad de almacenamiento extraíble ocasionando el bloqueo temporal del sistema hasta la desconexión del dispositivo de la PC. Como en el "Cn911.exe" (aplicación encubierta como ejecutable que se instala en el registro de usuario y lo modifica.) La codificación es de claves simétricas simples, es decir son aquellas que utilizan la misma clave para cifrar y descifrar un documento lo que ocasiona la reducción de la capacidad de almacenamiento del disco extraíble, sin embargo algunos usuarios con conocimientos informáticos avanzados, descifran, cuales son dichas claves y pueden llegar a recuperar la capacidad real del dispositivo, trucada por el malware.

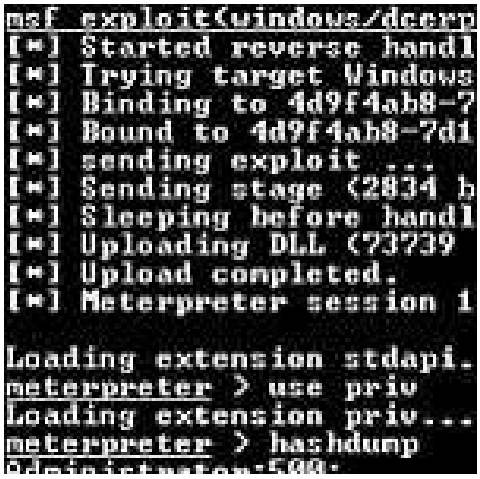
Dialers

Los dialers son programas que llaman a un número telefónico de larga distancia, o de tarifas especiales, para, a través del módem, entrar de forma automática y oculta para el usuario y sin su consentimiento, principalmente a páginas de juegos, adivinación o pornográficas, que van a redituar en beneficio económico a los creadores del malware, pero que además al usuario le crean la obligación de pagar grandes tarifas por el servicio telefónico.

Existen en Internet páginas preparadas para descargar, instalar y ejecutar dialers de conexión y virus informáticos capaces de llevar a cabo todo lo anterior, con la desventaja de su rápida propagación.

Actualmente las conexiones por medio de banda ancha, han evitado estos problemas.

Exploit



Exploit que evade a la mayoría de antivirus

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.

Hijacker

Programa que realiza cambios en la configuración de la página de inicio del navegador, que lo redirige a otras páginas de características indeseables como son las pornográficas y más peligrosamente a copias casi fieles de las bancarias.

Hoaxes, Jokes o Bulos

Son bromas que semejan ser virus, pero que, ciertamente no los son. Normalmente una persona conocida nuestra recibe una "alarma" de un supuesto virus y nos "hace el favor" de notificarnos para que tomemos precauciones en nuestro equipo.

El objetivo de la persona que inició el rumor o hoax se ha cumplido, al preocupar al usuario con la broma y que, en muchos casos, puede hacer al usuario auto eliminar algún supuesto archivo contaminado, lo cual podría afectar realmente al funcionamiento del sistema, llegando incluso a tener que reinstalarlo.

Keystroke o keyloggers

Son programas espías, que toman el control de los equipos, para espiar y robar información, monitorea el sistema, registrando las pulsaciones del teclado, para robar las claves, tanto de páginas financieras y correos electrónicos como cualquier información introducida por teclado, en el equipo utilizado para saber lo que la víctima ha realizado como conversaciones que la misma tuvo, saber donde ha entrado, qué ha ejecutado, qué ha movido, etc.

Pueden ser también aparatos o dispositivos electrónicos colocados intencionalmente en equipos, que se intercalan entre el dispositivo y el computador.

Ladilla virtual

Conocido como (virtual crab). Este tipo de programa maligno que, como analogía al parásito de transmisión sexual, entra en una computadora a través del sexo virtual, sitios pornográficos o cualquier aplicación relacionada. Los sitios web pornográficos suelen ser un gran caldo de cultivo para estos Malware virtuales.

Leapfrog

Las ranas como también se conocen en español son programas que entran a los equipos para conocer las claves de acceso y las cuentas de correo almacenadas en la libreta de direcciones para ser utilizadas en la replicación de estos, a través de enviar copias del gusano.

Parásito Informático

Este tipo de malware es el que se adhieren a archivos (especialmente ejecutables), como lo haría un parásito. Ese archivo ejecutable es denominado portador (o Host) y el parásito lo utiliza para propagarse. Si el programa es ejecutado, lo primero que se ejecuta es el parásito informático, y luego, para no levantar sospechas, se ejecuta el programa original. Muchas veces es aquí donde los parásitos fallan, porque hay programas que detectan estas

modificaciones y lanzan errores (incluso errores de advertencias de presencia de malware).

Pharming

Es el software maligno que suplanta el DNS, en el archivo host local, para conducirnos a una página Web falsa, con lo cual, al intentar entrar a un determinado nombre de dominio en nuestro navegador nos redirecciona al que el cracker, ha cambiado.

Por ejemplo la página de un banco pudiera ser www.bankito.com (xxx.156.24.196),[10] nos lo cambia por www.ban**quita**.com (YYY.132.30.60),[11] con lo que al parecerse, no nos percatamos normalmente que nos esta enviando a otra página controlada por el bandido cibernético.

Para poder instalarnos la página que realizara el direccionamiento, se instalará en nuestro sistema algunos programas malware ejecutables, que recibimos a través de un correo electrónico, descargas por Internet, programas P2P, etc.

Siendo en este momento el más común el envió de una supuesta tarjeta de Gusanito.com, que al entrar en el vinculo contenido en el correo electrónico, no solo nos da la sorpresa de la tarjeta, sino que ha realizado la descarga correspondiente que se encargará de auto ejecutarse creando el host que redirecciona nuestro navegador a las IP de las páginas falsas administradas por el hacker.

Phishings

Del inglés "fishing" (pescando), se utiliza para identificar la acción fraudulenta de conseguir información confidencial, vía correo electrónico o página web, con el propósito de que los usuarios de cuentas bancarias lo contesten, o entren a

páginas aparentemente iguales a la del banco o de los portales con ingreso por contraseña.

El phishing se basa en el envío por parte de un estafador de un mensaje electrónico o enlace de una empresa supuestamente respetable. Éstas a menudo conducen a una página Web falsificada que han creado, y engañan al usuario para que introduzca su contraseña y su información personal. Así lo convierten en un blanco fácil del robo de información personal o financiera de manera electrónica utilizando el nombre de un tercero (banco) y últimamente las páginas del acceso a e-mails de compañías como Yahoo!.

Nunca debe darse información de cuentas bancarias por otros medios que no sea en las sucursales correspondientes al banco, ya que por medio de correos electrónicos con enlaces falsos, supuestamente del banco, pueden solicitar los números de cuentas y contraseña privados, con lo que se les está dando todo para que puedan cometer el fraude.

En falsas cartas bancarias:

- Se presiona al cliente con supuestas fallas en su información o en los servidores que es urgente atender.
- El documento puede contar con faltas de acentos ortográficos en palabras como línea, dirección, activación, cámbiela, etc.
- Para dar confianza al usuario se colocan botones e imágenes que le son conocidos por la página real y las advertencias usuales de la página de acceso normal.
- Para completar el engaño, advierte del envío de e-mails falsos, siendo en sí mismo uno de ellos.
- El medio para entrar a la página web suplantada puede ser "http://" (en lugar del real "https://")+ nombre de la página web (siendo este la dirección real a la que entramos normalmente) + "@" + dirección del sitio al que nos redirige.

Generador de claves dinámicas

El método de entrar a las páginas Web de los diferentes Bancos de algunos países, es usando el generador de claves dinámicas de las compañías Secure Computing[12] y el RSA SecurID,[13] con lo que se espera terminar con los Phishing.

Por lo tanto ahora el ataque de los pescadores de datos (fishing), es pidiéndole que sincronice su generador de claves, con lo que inmediatamente entran a la cuenta del usuario sacando lo que puedan y cambiando hasta las claves de acceso.

También Yahoo da protección por medio de la creación del llamado sello de acceso personalizado,[14] que consiste en colocar una imagen o texto, el cual debe aparecer cada vez que se inicie sesión en Yahoo, en la computadora en que se ha colocado, púes se vincula a ella y no al usuario del correo. Si el sello de acceso **NO** está, es probable que sea una página falsificada creada por un estafador para robar los datos personales.

Pornware

Describe programas que usan el Módem de la computadora para conectarse a servicios de pago por evento pornográfico o para bajar contenidos pornográficos de la Web. Es un caso particular de Dialers.

Es un auténtico fraude mediante información engañosa, manifiestan que es completamente gratuito, el sitio a visitar es en efecto sin costo, pero solo se tiene acceso por vía telefónica (MODEM), que resulta con una alta tarifa por minuto que se refleja en el recibo telefónico (por lo regular utilizan una clave de larga distancia internacional (900) con un cargo aproximado de $20.00 USD por minuto). Esta técnica fraudulenta se utiliza también usando como señuelo videojuegos, salva pantallas, programas o cualquier otra falacia que requiera acceso mediante un MODEM telefónico.

Primero se descarga desde algún sitio que ofrece todo absolutamente gratis un pequeño programa ejecutable, que coloca en el escritorio de la PC un llamativo ícono para que cualquier incauto con un simple click haga el enlace mencionado, aparecen insistentes mensajes sugiriendo de que todo es completamente gratis y sin límite de tiempo.

Sin embargo, se están extinguiendo por dejarse de lado los Módems convencionales de 56Kbps, y usarse Tarifas Planas en Red Ethernet de Banda ancha o ADSL.

Rabbit o conejos

Reciben este nombre algunos gusanos informáticos, cuyos códigos malignos llenan el disco duro con sus reproducciones en muy poco tiempo y que también pueden saturar el ancho de banda de una red rápidamente además de poder mandar un numero infinito de impresiones del mismo archivo, colapsando la memoria de la impresora al saturarla.

Riskware

Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas.

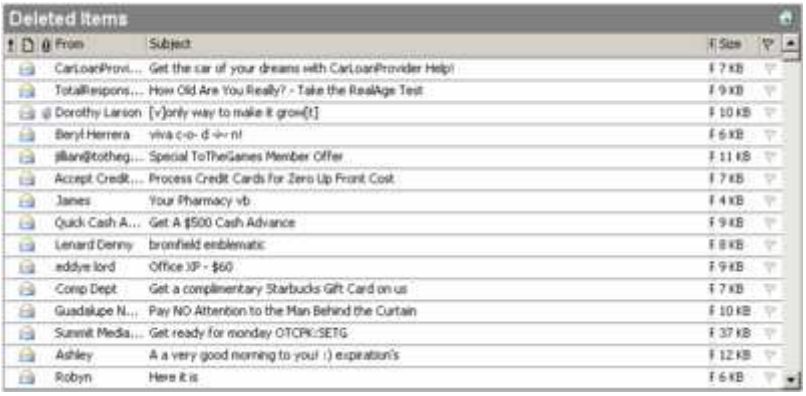
Rootkit

Los rootkits 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 y evitan ser desinstalados o eliminados a toda costa, pues cuenta con protección para no permitirlo, con lo cual se convierte en un programa indeseable y molesto. Los rootkit se volvieron famosos a partir de uno que estaba incluido en un mecanismo anticopia en algunos CD de música de la empresa Sony.[15]

Scumware o escoria

Scumware o escoria es cualquier software que hace cambios significativos en la apariencia y funciones de las páginas Web sin permiso del Administrador (Webmaster) o propietarios. Por ejemplo, un número de productos sobreponen la publicidad de los banners con otros anuncios, a veces para los productos de la competencia. El Scumware puede agregar hyperlinks desautorizados a la sección opinión de una página Web - a veces usar de un usuario acoplamientos a los sitios posiblemente desagradables. Tales programas pueden interferir con hipervínculos (hyperlinks) existentes agregando otros destinos a los previstos. A veces, el Scumware es conocido como thiefware.

Spam



Lista de correos spam

Se le llama spam a los e-mailes basura, que son enviados a direcciones electrónicas compradas por empresas con la finalidad de vender sus productos.[16]

Últimamente han surgido páginas con mensajes que aparecen en un corto instante de tiempo (efecto *flash*) tratando de producir en el inconsciente de la mente la necesidad de comprar el producto anunciado como si de un mensaje subliminal se tratara.[17] [18]

Actualmente existen filtros que bloquean los spam en la mayoría de los servidores de correo, además de existir ya legislación contra los spam,[19] México cuenta desde el 2000,con una ley en donde se prohíben las prácticas comerciales no solicitas por correo electrónico, además de artículos en la Ley Federal de Protección al Consumidor, que regulan el comercio electrónico,[20] aunque los spam son enviados desde otros países para evadir estas y otras restricciones mundiales.[21]

Se calcula que alrededor del 75% del correo electrónico que circula en la red son spam,[22] pero podemos observar que tiene variaciones mensualmente.[23] Sophos, en su lista “Dirty dozen spam relaying countries”, incluye una categoría de generación de spam por país con estos porcentajes: United States 23.2%, China (inc. Hong Kong) 20.0%, Corea 7.5%, Francia 5.2%, España 4.8%, Polonia 3.6% , Brasil 3.1%, Italia 3.0%, Alemania 2.5%, Inglaterra 1.8%, Taiwán 1.7%, Japón 1.6%, Otros 22.0%.[24]

Spyware

Los Spywares o Programa espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar programas de terceros, por lo que rara vez el usuario es consciente de ello.[26] Normalmente trabajan y contaminan sistemas como lo hacen los Caballos de Troya.

Ventanas emergentes/POP-UPS

Son, generalmente, ventanas muy molestas que aparecen al navegar y muestran publicidad o información que es difícil de eliminar y que aparece constantemente.

Son una forma en línea de publicidad en el World Wide Web, que aumentan el tráfico de la red o que son también usadas para capturar direcciones de e-mail. Trabaja cuando ciertos sitios abren una ventana del buscador para exhibir los anuncios.

La ventana pop-up que contiene un anuncio es generada normalmente por JavaScript, pero se puede generar por otros medios también.

Una variante en las ventanas pop-up es hacer aparecer el anuncio debajo de la ventana activa o en direcciones fuera del área visual, normalmente en la parte inferior derecha, y suelen aparecer como intentos de abrir una página nueva durante unos milisegundos, hasta cargarse y cumplir su cometido, cerrándose inmediatamente, con lo cual el usuario no se percata cuando surge, sino hasta

que cierra su navegación, con lo que difícilmente puede identificar junto a que página surgió, sobre todo en aquellas sesiones en que se tienen varios documentos abiertos.

Worms o gusanos

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.

El caso más conocido es el del gusano Blaster que se distribuyo por internet rápidamente gracias a una vulnerabilidad de Windows, que reinicia la computadora al cabo de 1 minuto, e intenta infectar a un numero de 256 computadores cercanos a la maquina (en redes locales) y lejanos (en internet) de forma aleatoria