Virus Informático

Un virus informático es un malware 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 un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.
El por qué se les llama virus, se debe a que se comportan de igual manera que sus pares biológicos. Se auto-reproducen una vez infectado el cuerpo, son muy pequeños, y terminan perjudicando gravemente a la entidad que los recibe. De hecho, muchas computadoras, pierden toda su información, al ser atacadas por un virus. Muchas veces se debe reformatear la computadora, para limpiarla completamente, lo cual conlleva a instalar todas las aplicaciones nuevamente; esto a su vez ocasiona nuevos problemas, ya que muchas veces no se encuentran los discos originales de instalación. Por estos motivos, los técnicos en computación, recomiendan que de tiempo en tiempo, los dueños de computadoras, vayan respaldando todo aquello que se considere de importancia.
Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos por que no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Características Generales de los virus informáticos

El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo.
Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo", menos comunes son los no-residentes que no permanecen en la memoria después que el programa-huésped es cerrado.
Los virus se transportan a través de programas tomados de BBS (Bulletin Boards) o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga "ejecutables" o "macros" puede ser portador de un virus: downloads de programas de lugares inseguros; e-mail con "attachments", archivos de MS-Word y MS-Excel con macros. Inclusive ya existen virus que se distribuyen con MS-Power Point. Los archivos de datos, texto o Html **NO PUEDEN** contener virus, aunque pueden ser dañados por estos.
Los virus de sectores de "booteo" se instalan en esos sectores y desde allí van saltando a los sectores equivalentes de cada uno de los drivers de la PC. Pueden dañar el sector o sobrescribirlo. Lamentablemente obligan al formateo del disco del drive infectado.

Incluyendo discos de 3.5" y todos los tipos de Zip de Iomega, Sony y 3M. (No crean vamos a caer en el chiste fácil de decir que el más extendido de los virus de este tipo se llama MS

Clases de Virus

Existen diversos tipos de virus, varían según su función o la manera en que éste se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

Troyano: que consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.

Gusano: tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Bombas Lógicas o de Tiempo: son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.

Hoax: Los hoax no son virus ni tienen capacidad de reproducirse por si solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo") y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los ínter nautas novatos.

Como detectar infecciones virales

- Cambio de longitud en archivos.
- Modificación de la fecha original de los archivos.
- Aparición de archivos o directorios extraños.
- Dificultad para arrancar el PC o no conseguir inicializarlo.
- El PC se "re-bootea" frecuentemente
- Bloqueo del teclado.
- El PC no reconoce el disco duro.
- Ralentización en la velocidad de ejecución de los programas.
- Archivos que se ejecutan mal.
- El PC no reconoce las disqueteras.
- Se borran archivos inexplicablemente.
- Aparecen nuevas macros en documentos de Word.
- La opción "ver macros" se desactiva.
- Pide passwords no configurados por el usuario.

Técnicas de prevención

Copias de seguridad

- Realice copias de seguridad de sus datos. Éstas pueden realizarlas en el soporte que desee, disquetes, unidades de cinta, etc. Mantenga esas copias en un lugar diferente del ordenador y protegido de campos magnéticos, calor, polvo y personas no autorizadas.

Copias de programas originales

- No instale los programas desde los disquetes originales. Haga copia de los discos y utilícelos para realizar las instalaciones.
- No acepte copias de origen dudoso
- Evite utilizar copias de origen dudoso, la mayoría de las infecciones provocadas por virus se deben a discos de origen desconocido.
- Utilice contraseñas
- Ponga una clave de acceso a su computadora para que sólo usted pueda acceder a ella.

Cómo protegerse de los virus informáticos

Los Virus informáticos se han convertido en una continua pesadilla, especialmente, para los usuarios del correo electrónico. Para su información, seguidamente listamos una serie de normas básicas que le ayudarán a protegerse de los virus informáticos:

- Instale en su computador un software Antivirus confiable (ver lista de opciones en la siguiente sección).
- Para su información, seguidamente listamos una serie de normas básicas que le ayudarán a protegerse de los virus informáticos:
- Instale en su computador un software Antivirus confiable (ver lista de opciones en la siguiente sección).
- Actualice con frecuencia su software Antivirus (mínimo dos veces al mes).
- Analice con un software Antivirus actualizado, cualquier correo electrónico antes de abrirlo, así conozca usted al remitente.
- Analice siempre con un software Antivirus los archivos en disquete o Cd-Rom antes de abrirlos o copiarlos a su computador.
- No descargue, ni mucho menos ejecute, archivos adjuntos (attachement) a un mensaje de correo electrónico sin antes verificar con la persona que supuestamente envió el mensaje, si efectivamente lo hizo.
- Tenga cuidado con los mensajes alusivos a situaciones eróticas (versión erótica del cuento de Blancanieves y los Siete Enanitos, fotos de mujeres desnudas, fotos de artistas o deportistas famosos, etc.).
- Nunca abra archivos adjuntos a un mensaje de correo electrónico cuya extensión [6] sea ".exe", ".vbs", ".pif", ".bat" o ".bak".
- Cerciórese que el archivo adjunto no tenga doble extensión. Por ejemplo: "NombreArchivo.php.exe".
- Evite el intercambio por correo electrónico de archivos con chistes, imágenes o fotografías.

Antivirus

Los **antivirus** nacieron como una herramienta simple cuyo objetivo fuera detectar y eliminar virus informáticos.
Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar un Virus informáticos, sino bloquearlo, desinfectar y prevenir una infección de los mismos, así como actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.
Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el ordenador, con técnicas como Heurística, HIPS, etc.
Usualmente, un antivirus tiene un (o varios) componente residente en memoria que se encarga de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso.
Asimismo, cuentan con un componente de análisis bajo demando (los conocidos scanners, exploradores, etc), y módulos de protección de correo electrónico, Internet, etc.

Antivirus populares

- Kaspersky Anti-virus.
- Panda Security.
- Norton antivirus.
- McAfee.
- avast! y avast! Home
- AVG Anti-Virus y AVG Anti-Virus Free.
- BitDefender.
- F-Prot.
- F-Secure.
- NOD32.
- PC-cillin.
- ZoneAlarm AntiVirus.

Tipos de antivirus
Cortafuegos (Firewall)

Programa que funciona como muro de defensa, bloqueando el acceso a un sistema en particular. Se utilizan principalmente en computadoras con conexión a una red, fundamentalmente Internet. El programa controla todo el tráfico de entrada y salida, bloqueando cualquier actividad sospechosa e informando adecuadamente de cada suceso.

Antiespías (Antispyware)

Aplicación que busca, detecta y elimina programas espías (spyware) que se instalan ocultamente en el ordenador.

Los antiespías pueden instalarse de manera separada o integrado con paquete de seguridad (que incluye antivirus, cortafuegos, etc).

Antipop-ups

Utilidad que se encarga de detectar y evitar que se ejecuten las ventanas pop-ups cuando navegas por la web. Muchas veces los pop-ups apuntan a contenidos pornográficos o páginas infectadas.

Algunos navegadores web como Mozilla Firefox o Internet Explorer 7 cuentan con un sistema antipop-up integrado.

Antispam

Aplicación o herramienta que detecta y elimina el spam y los correos no deseados que circulan vía email.

Funcionan mediante filtros de correo que permiten detectar los emails no deseados. Estos filtros son totalmente personalizables.

Además utilizan listas de correos amigos y enemigos, para bloquear de forma definitiva alguna casilla en particular.

Algunos sistemas de correo electrónico como Gmail, Hotmail y Yahoo implementan sistemas antispam en sus versiones web, brindando una gran herramienta en la lucha contra el correo basura.