COOPESAIN R.L.
Manual de Virus Informáticos

TABLA DE CONTENIDO

TABLA DE CONTENIDO.....1
INTRODUCCIÓN.....2
VIRUS INFORMÁTICOS.....3
Definición.....3
Clasificación.....3
Tipos de Virus.....3
Acompañante.....3
Archivo.....4
Ejemplos de virus.....4
Worms o gusanos.....4
Troyanos.....4
Jokes o virus de broma.....4
Hoaxes o falsos virus.....4
Virus de macros.....5
Daños.....5
Métodos de Contagio.....5
Síntomas Típicos de Contagio.....6
Métodos de Protección.....6
Activos.....7
Pasivos.....7
Antivirus.....9
Recomendaciones.....10
GLOSARIO.....11

INTRODUCCIÓN

Los virus informáticos son programas diseñados expresamente para interferir en el funcionamiento de una computadora, registrar, dañar o eliminar datos, o bien para propagarse a otras computadoras y por Internet, a menudo con el propósito de hacer más lentas las operaciones y provocar otros problemas en los procesos.

Al igual que hay virus humanos con niveles de gravedad muy distintos, los efectos de los virus informáticos pueden ser desde ligeramente molestos hasta auténticamente devastadores. Además, cada día se presentan nuevas variantes. Por suerte, con precaución y algunos conocimientos, es menos probable convertirse en víctima de los virus y se puede reducir su impacto.

No existe constancia de virus que puedan dañar el hardware de una computadora (como las unidades de disco o los monitores). Asimismo, las advertencias acerca de virus que puedan provocar daños físicos son fruto de una falta de información o de engaños, simplemente.

Para su propagación, los virus básicos suelen requerir que los usuarios desprevenidos los compartan o los envíen inadvertidamente. Algunos virus más sofisticados, como los gusanos, pueden reproducirse y enviarse automáticamente a otras computadoras cuando consiguen controlar determinados programas, como algunas aplicaciones de correo electrónico compartido. Ciertos virus, denominados troyanos (en referencia al legendario caballo de Troya), pueden presentarse como programas aparentemente beneficiosos para que los usuarios los descarguen. Existen incluso algunos troyanos que pueden ofrecer los resultados esperados y, al mismo tiempo, dañar discretamente el sistema local o el de otras computadoras conectadas a la red.

Por lo anterior, es de vital importancia que cada usuario de la red de COOPESAIN R.L., antes de bajar un archivo sospechoso; de abrir un correo de un desconocido o con un asunto extraño; de introducir en su computador un diskette, CD o **llave maya** que provenga o haya sido utilizada en otro computador o institución; se comunique con la Unidad de Informática, para verificar que dicho medio no se encuentra infectado con un virus, para evitar el contagio de su equipo y de los demás equipos conectados en red.

VIRUS INFORMÁTICOS

Definición

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. 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.

Clasificación

- Aquellos que infectan archivos. A su vez, éstos se clasifican en:
  - ✓ Virus de acción directa. En el momento en el que se ejecutan, infectan a otros programas.
  - ✓ Virus residentes. Al ser ejecutados, se instalan en la memoria de la computadora. Infectan a los demás programas a medida que se accede a ellos. Por ejemplo, al ser ejecutados.
- Los que infectan el sector de arranque, (virus de boot). Recordemos que el sector de arranque es lo primero que lee el ordenador cuando es encendido. Estos virus residen en la memoria.

Tipos de Virus

Existen una variedad de virus en función de su forma de actuar o de su forma de infectar, clasificados de la siguiente manera:

Acompañante

Estos virus basan su principio en que usualmente se ejecuta primero el archivo con extensión COM frente al de extensión EXE, en el caso de existir dos archivos con el mismo nombre pero diferente extensión dentro del mismo directorio. El virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar. Después ejecuta el nuevo archivo COM, creado por el virus, y cede el control al archivo EXE.

Archivo

Los virus que infectan archivos del tipo *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT. Este tipo de virus se añade al principio o al final del archivo. Estos se activan cada vez que el archivo infectado es ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados.
Este tipo de virus se dividen en dos: los Virus de Acción Directa, que son aquellos que no se quedan residentes en memoria y se replican en el momento de ejecutar el fichero infectado y los Virus de Sobreescritura, que corrompen el fichero donde se ubican al sobrescribirlo.

Ejemplos de virus

Worms o gusanos

Se registran para correr cuando inicia el sistema operativo ocupando la memoria y volviendo lento al ordenador, pero no se adhieren a otros archivos ejecutables. Utilizan medios masivos como el correo electrónico para esparcirse de manera global.

Troyanos

Suelen ser los más peligrosos, ya que no hay muchas maneras de eliminarlos. Funcionan de modo similar al caballo de Troya; ayudan al atacante a entrar al sistema infectado, haciéndose pasar como contenido genuino (salvapantallas, juegos, música). En ocasiones descargan otros virus para agravar la condición del equipo.

Jokes o virus de broma

No son realmente virus, sino programas con distintas funciones, pero todas con un fin de diversión, nunca de destrucción, aunque pueden llegar a ser muy molestos.

Hoaxes o falsos virus

Son mensajes con una información falsa; normalmente son difundidos mediante el correo electrónico, a veces con fin de crear confusión entre la gente que recibe este tipo de mensajes o con un fin aún peor en el que quieren perjudicar a alguien o atacar al ordenador mediante ingeniería social.

Virus de macros

Una macro es una secuencia de órdenes de teclado y mouse asignadas a una sola tecla, símbolo o comando. Son muy útiles cuando este grupo de instrucciones se necesitan repetidamente. Los virus de macros afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y actuarán hasta que el archivo se abra o utilice.

Daños

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como: pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir replicándose. Las redes en la actualidad ayudan a dicha propagación cuando éstas no tienen la seguridad adecuada.

Otros daños que los virus producen a los sistemas informáticos son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc.

Hay que tener en cuenta que cada virus plantea una situación diferente.

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*" o "*Congratulations, you've won*…"
- Entrada de información en discos o llaves mayas de otros usuarios infectados.
- Instalación de software pirata o de baja calidad.
- En el sistema Windows puede darse el caso de que el ordenador pueda infectarse sin ningún tipo de intervención del usuario, 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 se ha corregido este problema en su mayoría. De manera frecuente, el usuario deberá descargar actualizaciones y parches de seguridad.

Síntomas Típicos de Contagio

- El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
- El tamaño del programa cambia sin razón aparente.
- El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.
- En Windows muestra "32 bit error".
- La luz del disco duro en la CPU continua parpadeando aunque no se esté trabajando, ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).
- No se puede "bootear" desde el Drive A, ni siquiera con los discos de rescate.
- Aparecen archivos de la nada o con nombres y extensiones extrañas.
- Suenan "clicks" en el teclado.
- En la pantalla del monitor pueden aparecen mensajes absurdos tales como "Tengo hambre. Introduce un Big Mac en el Drive A".

Métodos de Protección

Los métodos para contener o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

Activos

- *Antivirus*

  Tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Buscan tener controlado el sistema mientras funciona, deteniendo las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

- *Filtros de ficheros*

  Consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

Pasivos

- *Copias de seguridad*

  Mantener una política de copias de seguridad garantiza la recuperación de los datos y una solución cuando nada de lo anterior ha funcionado.

- *Estudiar*

  Aprender cómo es el software de nuestra computadora, buscando y buscando información, en sitios en los que se pueda confiar, sobre software dañino, para así evitarlo.

- *Desconfiar*

  Si no conocemos algo o no sabemos lo que hace, será mejor tenerle respeto y no tocarlo hasta aclarar nuestra duda, (en el uso de esta regla es recomendable no abrir archivos de correos de los que se desconoce el remitente, o se sospecha de que pueda contener código malicioso, o que no pidió usted. Aun así, si es de entera confianza, analice siempre con un antivirus el archivo antes de abrirlo). Es aconsejable complementar esta manera de proceder aplicando una política de contraseñas y de seguridad más seguras a su red local o a los parámetros de acceso a Internet. Lo que muchos creadores de virus desean es la sensación de

vulnerabilidad al provocar las condiciones de contagio idóneas que permitan una infección del virus a nivel mundial y causar daños sin dejar rastro de su presencia. En algunos casos los virus de correo pueden ser predichos debido al asunto del mensaje, por ejemplo la mayoría de estos virus se predicen a partir de asuntos perfectamente escritos o en otros idiomas.

- *Hacer reenvíos seguros de email*

  Cuando recibamos un mensaje de correo electrónico sospechoso de contener virus o que hable de algo que desconocemos conviene consultar su posible infección o veracidad, con la Unidad de Informática. Sólo si estamos seguros de la ausencia de virus del mensaje o de que lo que dice es cierto e importante, de ser conocido por nuestros contactos, lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios en la casilla CCO. Así evitaremos la propagación de mensajes con virus, así como la del spam y la de aquellos mensajes con phishing u hoax.

- *Informar a nuestros contactos*

  Conviene que hagamos saber lo mencionado en el punto anterior a nuestros contactos en cuanto nos reenvían mensajes con virus o contenido falso o sin utilizar la casilla CCO.

- *Limpiar y eliminar el virus*

  En el caso de que nuestra máquina resulte infectada debemos proceder a su desconexión inmediata de la red, ya sea local o Internet (esto se hace para evitar contagios a otras máquinas) y, una vez aislada, aplicar un programa Antivirus actualizado para tomar la acción que se corresponda.

- *Restauración completa*

  En caso de que el virus sea tan virulento que destruya la lógica de una unidad de almacenamiento, se deberá recurrir a la restauración completa con formateo completo. Téngase en cuenta que esta operación dejará la máquina tal y como estaba el día que se adquirió. Sus configuraciones y demás quedarán borradas permanentemente.

Antivirus

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora.

Algunas recomendaciones para la elección de un buen antivirus son:

• Recurrir a un antivirus actualizado, de nada sirve tener un antivirus viejo.

• Que el módulo de escaneo sea fácilmente configurable para que el chequeo incluya a todos los virus, no sólo los que infectan el boot sector y ejecutables.

• La actualización debe ser fácil de obtener, pero también debe influir en la adquisición de un antivirus el tipo de tecnología aplicada en su desarrollo.

• Que permitan el chequeo antivirus de e-mails y adjuntos.

• Que los antivirus chequeen de manera automática las unidades de diskettes, CD-Rom's, ZIP, llaves mayas y aún los archivos abiertos y adquiridos en Internet de manera automática.

En el mercado existen antivirus como:

- Dr. Solomon's antivirus toolkit.
- VirusScan
- PertAntivirus.
- McAfee.
- NortonAntivirus.
- Panda.
- Avast
- Etrust

Recomendaciones

- Si detecta algún síntoma de infección, comuníquese inmediatamente con el personal de Informática.
- No abrir correos de desconocidos o que merezcan poca confianza.
- No abrir archivos adjuntos si no se tiene la certeza de su contenido.
- Fijarse en el texto del Asunto, si es un texto sin un significado claro, puede ser un síntoma de que el correo contiene un virus, pues algunos virus generan el asunto juntando varias palabras al azar.
- Desactivar la opción de "Vista previa" de algunos programas de correo, como por ejemplo el Outlook Express.
- No utilizar llaves mayas en su computadora si antes no han sido revisadas en búsqueda de virus, por la Unidad de Informática.
- Ante cualquier duda, comunicarse con el personal de Informática.

GLOSARIO

Hoax

Un hoax es un intento de hacer creer a un grupo de personas que algo falso es real. El término se popularizó principalmente al referirse a engaños masivos por medios electrónicos, especialmente Internet.

A diferencia del fraude el cual tiene usualmente una o unas cuantas víctimas y es cometido con propósitos delictivos y de lucro ilícito, el hoax tiene como objetivo el ser divulgado de manera masiva haciendo uso de los medios de comunicación, siendo el más popular de ellos en la actualidad Internet y no suelen tener fines lucrativos o no son su fin primario.

Hoax informático

Es un mensaje de correo electrónico con contenido falso o engañoso. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante, que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado.

Ingeniería Social

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que “los usuarios son el eslabón débil” en seguridad; éste es el principio por el que se rige la ingeniería social.

Llave Maya / Memory Key

Dispositivo plug and play, que se enchufa en un puerto USB, con el que se puede leer, escribir, copiar, borrar y mover datos desde el disco duro al Memory Key o viceversa.

Phishing

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

Plug and Play

Plug-and-play (conocida también por su abreviatura PNP) es la tecnología que permite a un dispositivo informático ser conectado a un computador, sin tener que configurar ni proporcionar parámetros a sus controladores. Para que eso sea posible, el sistema operativo con el que funciona el computador, debe tener soporte para dicho dispositivo.

Spam

Se llama spam o correo basura, a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Vírico

De los virus o relativo a ellos.