VIRUS Y ANTIVIRUS

Un virus informático es un programa que puede infectar a otros programas, modificándolos de tal manera que causen daño en el acto (borrar o dañar archivos) o afectar su rendimiento o seguridad. Este software constituye una amenaza muy seria; se propaga más rápido de lo que se tarda en solucionarlo. Por lo tanto es necesario que los usuarios se mantengan informados acerca de los virus, huyendo de la ignorancia que les han permitido crecer hasta llegar a ser un grave problema.

Un caballo de Troya es un programa que hace algo oculto y que el usuario no ha aprobado, como abrir una conexión para que alguien externo tenga acceso a nuestra información. Finalmente, mucha gente usa el término "Troyano" para referirse solamente a un programa malicioso que no se copia a si mismo, a diferencia de los llamados "gusanos" que estos si se copian y propagan rápidamente.

La primera clase incluye los que **infectan archivos adjuntos** a programas ordinarios, aunque algunos pueden infectar cualquier archivo. Un virus de acción directa selecciona uno o varios programas para infectar cada vez que el programa es ejecutado. Uno **residente** se esconde en alguna parte de la memoria la primera vez que un programa infectado se ejecuta, y después infecta a otros programas cuando son ejecutados.

La segunda categoría es la de los que infectan **archivos de sistema** o sector de arranque. Estos virus, infectan el área de sistema en un disco. Hay algunos que se ejecutan al **iniciarse Windows**, y virus que infectan directamente al **sector de arranque** de discos duros, pudiendo incluso dañarlos permanentemente. Hay otros virus que **modifican las entradas** a la tabla de archivos para que el virus se ejecute. Hay que tener en cuenta que estos pueden causar perdida de información (archivos).

La forma más común en que se transmiten los virus es por transferencia de archivos, descarga o ejecución de archivos adjuntos a correos. También puede encontrarse con un virus simplemente visitando ciertos tipos de páginas web que utilizan un componente llamado ActiveX o Java Applet. Además, puede ser infectado por un virus simplemente leyendo un e-mail dentro de ciertos tipos de programas de e-mail como Outlook o Outlook Express.

Cuando un virus lleva a cabo la acción para la que había sido creado, se dice que se ejecuta la carga, pueden intentar producir un daño irreparable al ordenador personal destrozando archivos, desplazando/sobrescribiendo el sector de arranque principal, borrando los contenidos del disco duro o incluso escribiendo sobre la BIOS, dejando inutilizable el equipo. La mayoría de los virus no borran todos los archivos del disco duro. La razón de esto es que una vez que el disco duro se borra, se eliminará el virus, terminando así el problema.

Algunos virus se crean por el desafío que implica crear una amenaza que sea única, no detectable, para su víctima. El creador espera que el virus se propague de tal manera que le haga famoso. La notoriedad aumenta cuando el virus es considerado tal amenaza que los fabricantes de antivirus tienen que diseñar una solución.

Muchos virus se anuncian ellos mismos produciendo un sonido o mostrando un mensaje, pero también es común que un virus no muestre señales de su presencia en absoluto. Un antivirus actualizado es el único que puede indicarnos si tenemos una infección.

La mejor herramienta para combatir virus es saber como actúan, infectan y se propagan. Se recomienda lo siguiente:

El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización. Cualquier correo recibido puede contener virus aunque no le acompañe el símbolo de datos adjuntos (el habitual "clip"). Además, no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado. Un indicativo de posible virus es la existencia en el asunto del mensaje de palabras en un idioma diferente (generalmente inglés).

Muchas páginas de Internet permiten la descarga de programas y archivos a los ordenadores de los usuarios. Cabe la posibilidad de que estos archivos estén infectados con virus.

Como no existen indicadores claros que garanticen su fiabilidad, debemos evitar la descarga de programas

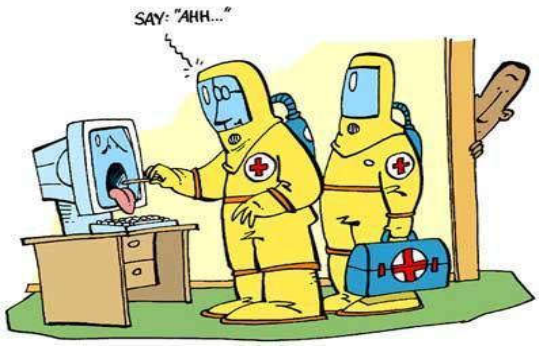
gratis. Por lo general, son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen; también los avalados por organizaciones tales como editoriales, organismos oficiales, etc.

Un amplio número de virus utiliza los chats para propagarse. Lo hacen enviando ficheros adjuntos (generalmente con nombres muy sugerentes). En general, si desconocemos el usuario que nos envía el archivo, debemos de rechazarlo.

Una muy buena forma de minimizar el impacto de un nivel corporativo como particular, es realizar copias periódicas y frecuentes de nuestra información. De esta manera, una pérdida de datos, causada por ejemplo por un virus, puede ser superada mediante la restauración de la última copia.

Un bulo es una noticia o una información falsa. Normalmente llega por correo electrónico y tiene un mensaje con contenido falso: por ejemplo que debemos borrar tal o cual fichero de nuestro sistema porque se trata de un virus. Los bulos se sirven de la propia mentira para propagarse a sí mismos: recomiendan que ese mensaje sea enviado a tantas personas como sea posible. Solo el administrador de sistema puede borrar archivos de Windows o del sistema.

La clave de los antivirus reside en unos ficheros de configuración donde se almacenan una serie de patrones que sirven para identificar los virus. El antivirus analiza cada uno de los correos entrantes en el sistema, ficheros, disquetes, etc. y busca dentro ellos esos patrones. Si el fichero o correo bajo análisis tiene alguno de los patrones, entonces se ha detectado el virus. Dependiendo de la configuración del antivirus, éste informará al usuario o simplemente lo borrará. Por esta razón es muy importante que los ficheros de datos del antivirus estén permanentemente actualizados. En general, los antivirus modernos se actualizan automáticamente (conectándose al proveedor) cada vez que se inicia una conexión con Internet.



Tomado: http://www.desarrolloweb.com

ACTIVIDAD:

Lee el siguiente artículo y responde las siguientes preguntas en tu cuaderno.

1. ¿Qué son los virus informáticos?
2. ¿Cuál es la diferencia entre un caballo de Troya y un gusano?
3. ¿Cuáles son los principales tipos de virus para PC?
4. ¿Qué hacen los virus?
5. ¿Cómo se transmiten los virus?
6. ¿Por qué la gente crea virus?
7. ¿Cómo sé si mi PC tiene un virus?
8. ¿Cómo puedo evitar que mi PC se infecte?
9. ¿Qué hacer si mi PC ha sido infectado?
10. ¿Qué es un bulo?
11. ¿Cómo funciona un antivirus?
12. Encuentra en la sopa de letras palabras sobre el tema

Q	L	Q	X	O	S	O	F	T	W	A	R	E	T	S	T
R	H	I	O	T	Z	P	C	X	S	K	O	E	H	K	I
Z	Y	P	A	D	I	P	K	F	G	V	G	D	U	Ñ	O
E	B	N	M	M	M	R	X	A	N	A	L	I	Z	A	R
Z	K	A	D	D	E	H	M	W	A	U	C	H	A	T	V
Z	S	A	M	E	T	S	I	S	D	Ñ	X	G	E	O	V
C	T	Ñ	R	A	Z	A	N	E	M	A	Y	K	P	L	R
A	H	Q	A	R	I	U	R	T	S	E	D	O	I	U	Z
Y	H	I	B	C	P	S	J	L	N	J	U	A	A	B	U
Z	I	V	S	U	R	I	V	S	O	V	I	H	C	R	A
H	U	A	P	R	O	G	R	A	M	A	Ñ	S	U	U	K
C	R	O	B	A	N	T	I	V	I	R	U	S	N	V	C

AMENAZAR-ANALIZAR-ANTIVIRUS-ARCHIVOS-BULO-CHAT
DESTRUIR-EMAIL-PROGRAMA-SISTEMA-SOFTWARE-VIRUS.