¿Qué es un virus computacional y qué hacer en caso de virus?

¿Qué es un virus computacional? Como hay de varios tipos, la definición de virus computacional dependerá de lo que haga, ya que han ido surgiendo nuevos tipos a lo largo del tiempo.

Los virus típicos

- Son los que se esconden y replican en la PC.
- Para arrancar una infección, el virus se liga a un archivo ejecutado por el sistema operativo de la PC.
- Depende de la intervención humana para activarse. Intentan infectar otros equipos.
- Se activan cuando se cumple una fecha o cuando se teclea una combinación de teclas específica.

Los gusanos

- Estos son virus que se alojan en el cerebro o memoria real de la PC y poco a poco van consumiendo los recursos de ésta.
- Se propaga por si mismo a lo largo de la red, utilizando las "facilidades" del correo electrónico, enviando el virus a las direcciones encontradas en el directorio del email (adress book).
- Se ejecuta en una PC sin la intervención humana.
- Entra a un equipo aprovechando las vulnerabilidades.
- Permanecen en memoria.

Los caballos de Troya

- Estos no necesariamente se multiplican por si solos, sin embargo, tal y como lo dice su nombre, al inocularse en una PC, abren una puerta trasera para que alguien en forma remota pueda acceder a la computadora, sin que el usuario se de cuenta.
- Uno de los virus de este tipo fue el *Back Orifice*, que se activó en la fecha de la final del mundial de football de Francia. Una versión corregida y aumentada del anterior es el *SubSeven,* afortunadamente ambos ya son detectados por los antivirus.

Timos (Hoax)

De vez en cuando llegan a nuestro buzón de entrada mensajes notificando la existencia de un peligroso virus, que ejerce su maligna acción a través del correo electrónico. En estos mensajes siempre se informa de peligrosos virus que al abrirlos ejercen su destructiva acción, entre las que generalmente se incluye el borrado del disco duro. Son totalmente falsos, son lo que se consideran «Hoax» o timo.

Pero toda la mitología acerca de este tipo de virus puede acabar por ser cierta, todo ello propiciado por los nuevos lectores de correo capaces de soportar todo tipo de controles Java y ActiveX.

En las páginas de los fabricantes de antivirus siempre hay una sección donde tienen identificados los “Hoax”, por ello recomendamos referir a esta sección para validar si un aviso de virus es cierto o falso.

Vacunas

Las vacunas, son el software antivirus fabricado por diferentes casas de software especializadas en antivirus. A continuación mencionaremos algunas de las conocidas en esta parte del hemisferio americano, aunque tal vez ya existan otras:

Proveedores:

- Trend Micro
- Norton Antivirus
- Norman Virus Control
- Norman Thunderbye
- Panda Antivirus Platinum
- VirusScan 4.01, Dr. Solomons
- F-Secure
- AVP,
- Sophos
- Command Antivirus

Casi todas estas casas fabricantes de software antivirus tienen el mismo nivel de efectividad, arriba del 90 por ciento. Cada vez que hay un concurso para analizar cual de ellas detecta más virus, sale una ganadora diferente, por lo que no conviene estar cambiando de software antivirus con mucha frecuencia.

Recomendamos seleccionar aquel que proporcione un mejor servicio.

Algoritmos utilizados

Existen varios métodos para identificar si un archivo tiene un virus, a estos métodos se les llama algoritmos para la detección de virus.

Varios de los fabricantes de software antivirus utilizan una mezcla de los algoritmos, los más utilizados se mencionan a continuación.

- **Verificación de patrones**

  Con el propósito de encontrar un virus específico, este software tiene que tener un patrón (*signature*) específico del mismo.

Si el patrón que busca no es encontrado significa que no tiene virus. Es decir: No patrón, no checa (*no signature, no match*).

Para acelerar la detección, algunos proveedores tienen el servicio de actualización en vivo (*live updating*), esto tiene el inconveniente de que si todavía no se encuentra la vacuna, tenemos que esperar.

- **Algoritmo heurístico**

Las casas fabricantes de antivirus usan el método heurístico para revisar archivos y programas buscando por código sospechoso que tradicionalmente se encuentra en los virus y no en un programa legítimo.

La heurística avanzada busca por secuencia de bytes por ejemplo:

- Programas que hacen cambios al Registry serán marcados como posibles virus, o
- Programas que pueden borrar o modificar archivos “xxxx.*”

La palabra heurístico viene del griego “encontrar”. En el dominio informático equivale a un programa que es capaz de resolver problemas con métodos alternativos, con el propósito de reducir el tiempo de procesamiento.

- **Filtro del contenido**

Este es una versión más flexible del método de verificación de patrones.

Un programador puede escoger una variedad de formas diferentes de ejecutar la misma instrucción, ejemplo:

- Para modificar el Registry, el método de verificación de patrones solamente busca por una secuencia de bytes para hacer esa instrucción,
- En el método de filtro de contenido, guarda una lista de maneras en que un programador podría hacer esa misma función.

Este método requiere de tener criterios adicionales para no dar falsos positivos cuando alguien este instalando un software.

- **Caja de arena**

Este método es lo que en inglés se llama *Dynamic Sandboxing*.

Se basa en ejecutar el código en un ambiente protegido. La caja de arena crea un espacio protegido dentro de la PC, donde el código sospechoso podrá ejecutarse.

Ya que el código malicioso no podrá hacer nada sin interactuar con el sistema operativo, estas cajas de arena vigilarán todas las llamadas al

sistema hechas por ese código y compararlas con las políticas, si se advierte alguna violación, el usuario será alertado.

Ejemplos

- Acceso a archivos: ¿el código lee, escribe o borra archivos?
- Network: ¿el código busca por dispositivos conectados en la red?
- Sistema operativo: ¿el código modifica o cambia algún parámetro del sistema operativo?
- Registry: ¿el código se auto-escribe en el Registry de manera que estará siempre activo?
- Direcciones IP: ¿se tiene alguna dirección IP codificada dentro del código?, etc.

- **Análisis de comportamiento**

Una nueva forma de detección es el software que revisa el comportamiento total del sistema, no busca por amenazas específicas.

Esta solución es presentada por http://www.okena.com/index.html empresa hawaiana, que lo lanzó al inicio del 2001.

Okena combina la heurística estática y dinámica con el análisis del comportamiento.

El software reside en el corazón de Windows y checa cada comando, cada operación con el Registry o con la red y reacciona a cualquier desviación con la normalidad.

Historias de Horror

Entre otras, las siguientes podrían ser algunas de las historias de horror en lo que respecta a los virus computacionales:

- El Back Orifice activó la fecha del Mundial de Futbol de Francia en 1998.
- El LoveLetter afectó a miles de empresas.
- Cuki trojan fue de los primeros.
- Palm.Liberty: es el primer caballo de Troya (Trojan horse) en la plataforma para Palm Top en OS. Fue descubierto a finales de agosto del 2000.
- El 25 de enero del 2003, ISS descubrió un nuevo gusano bautizado como “Slammer”, que se estaba extendiendo por medio de los servidores SQL de Internet.

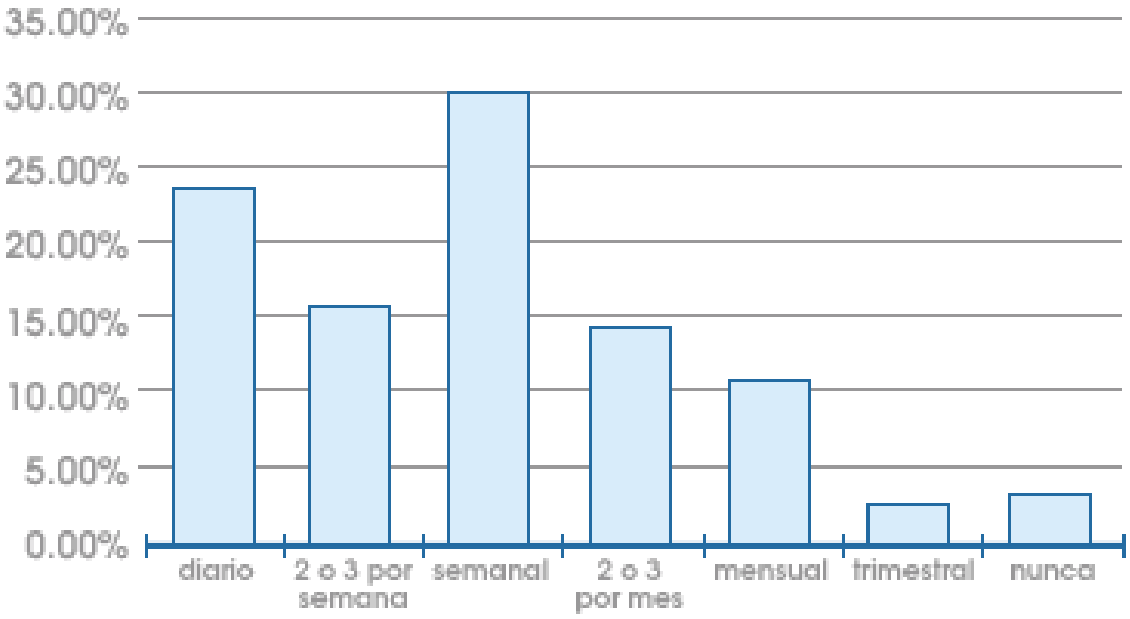
Un error común

Mucha gente cree que con hecho de tener instalado el software antivirus ya está protegido, eso es inexacto, ya que no toman en cuenta que se debe actualizar el archivo con los últimos virus encontrados.

En McAffe es el archivo DAT, en Norton es el “virus definition file”, así como en sus equivalentes en otros softwares, se deben mantener actualizados al menos cada semana.

En la gráfica que aparece en seguida se puede apreciar la frecuencia con que los usuarios comunes actualizan la lista de antivirus.

La recomendación es que se active la opción de actualización automática de la lista de antivirus (LiveUpdate Automático), para que el mismo paquete sea el que busque si existen actualizaciones pendientes por incorporar, y efectúe la actualización.



Recomendaciones

- Configurar correctamente el software antivirus. Activar las opciones de: auto protección, análisis del e-mail, bloqueo de scripts, análisis completo del disco duro diario.

- No inscribirse a páginas de dudosa reputación.
- Si se recibe un correo electrónico de procedencia desconocida con un archivo anexo, no abrirlo, de preferencia borrar el mensaje.
- No utilizar disquetes. En caso necesario primero se deberá revisar con un antivirus actualizado (algunas empresas destinan una PC desconectada de la red para revisar todos los disquetes que entren a la oficina).
- Evitar al máximo compartir archivos.
- No participar en cartas cadena (esta es una precaución adicional).
- Mantener actualizado el software antivirus (archivo con la lista de virus).

¿Qué hacer en caso de infectarse?

En caso de que alguna PC se sospeche que está infectada, se recomienda seguir el siguiente procedimiento:

1. Avisar al área de soporte técnico de informática, para que se valide si se trata de un virus o un mal funcionamiento de la PC.
2. Actualizar la vacuna, en caso de que este desactualizada.
3. Eliminar el virus, tal vez haya sido necesario contactar al proveedor del antivirus para utilizar una vacuna de emergencia.
4. En caso extremo recuperar el respaldo de la información.
5. Vacunar TODOS los disquetes.
6. Identificar la fuente del contagio.
7. Obtener tendencias de los incidentes con virus, identificando las áreas de la organización donde se presentan más virus. Analizar la procedencia de los mismos.

Referencias bibliográficas:

1. Qué es un virus computacional, recuperado del sitio de Internet http://personales.com/costarica/paraiso/softhard/virus.htm