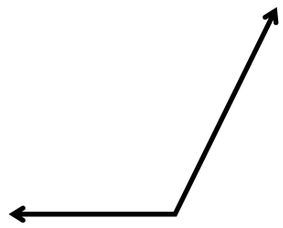
VIRUS INFORMÁTICOS

Breve aproximación a su problemática

¿Qué es un virus informático ?

La definición más simple y completa que hay de los virus informáticos se fundamenta en cuatro características, que se refuerzan y dependen mutuamente. Según su definición un virus es un programa (*software*) que cumple con las siguientes pautas:

- Es **Dañino.**
- Se **Autoreproductor.**
- Es **subrepticio y oculto** (no sabemos si está o no y cuando se activará)
- Es **muy pequeño** (en bytes)



Asimismo estos “programas” casi nunca incluyen el nombre del autor, ni el registro, ni el copyright, ni la fecha de creación. Al ser indudablemente un programa, está demás decir que fue creado por un programador, persona, ser humano, bastante especial por cierto, que se dedica a practicar de algo tan antiguo como la malicia humana.

Todos los virus informáticos están diseñados para reproducirse y evitar su detección. Como cualquier otro programa informático, un virus debe ser ejecutado para que funcione: es decir, la computadora debe cargar el virus desde la memoria de la misma y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus. La carga activa puede trastornar o modificar archivos de datos, presentar un determinado mensaje, provocar fallos en el sistema operativo y otros muchos efectos.

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: 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 internautas novatos.
- Joke: Al igual que los hoax, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a errar es posible que salga una ventana que diga: OMFG!! No se puede cerrar!

UN POCO DE HISTORIA

En 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera (se copiara). Esta teoría se comprobó experimentalmente en la década de 1950 en los Bell Laboratories, donde se desarrolló un juego llamado Core Wars en el que los jugadores creaban pequeños programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él.

En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término "virus" para describir un programa informático que se reproduce a sí mismo.

En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. Pronto les siguió un sinnúmero de virus cada vez más complejos.

El virus llamado Brain, que apareció en 1986, y en 1987 ya se había extendido por todo el mundo, fue de orígen paquistaní.

En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática.

El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990.

En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.

ESPECIES DE VIRUS

Existen al menos cinco categorías de virus:

1. Parásitos
2. De sector de arranque inicial o “boot sector”
3. De vínculo
4. De archivo de datos.
5. Spyware / Adaware / Malware

1- Los virus parásitos infectan archivos ejecutables o programas de la computadora. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser de acción directa o residentes. Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta. Un virus residente se oculta en la memoria de la computadora e infecta los programas cuando se ejecutan programas. Casi en desuso

2- Los virus del sector de arranque inicial (o virus de arranque o boot sector) residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan la PC. Estos virus suelen difundirse mediante el intercambio físico de discos flexibles. Con el tiempo el virus puede dañar los archivos de arranque y la PC se colgará cada vez que intentemos arrancar. Ejemplos de este tipo de virus : Predator2, Natas, Chile, Diablo, etc. Prácticamente desaparecidos

3- Los virus de vínculo modifican la forma en que el sistema operativo encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa deseado. Un virus de vínculo puede infectar todo un directorio de una computadora, y cualquier programa ejecutable al que se acceda en dicho directorio desencadena el virus.

4- Otros virus infectan programas que contienen lenguajes de macros potentes (lenguajes de programación que permiten al usuario crear nuevas características y herramientas) que pueden abrir, manipular y cerrar ficheros de datos. Estos virus, llamados virus de archivos de datos, están escritos en lenguajes de macros y se ejecutan automáticamente cuando se abre el programa legítimo. Son independientes de la máquina y del sistema operativo. Los más comunes son los que infectan archivos de Word y Excel.

5- Spyware / Adaware / Malware: **Malware** (del inglés ***mal****icious soft****ware***), también llamado **badware**, **código maligno**, **software malicioso** o **software malintencionado**, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término *malware* es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

¿Qué daños pueden producir los virus informáticos ?

¿Qué tipo de daños producen los virus informáticos ? Una vez que la máquina ha sido infectada, pueden ocurrir varias cosas:

- Que el virus afecte el sector de “booteo” (arranque) y tome el control cada vez que la PC arranca. Esto implica una segura infección de cada disquete que se introduzca en esa máquina.
- Que el virus infecte archivos ejecutables (.exe, .com) y que cada vez que éstos se ejecutan, el virus proceda a infectar otros archivos.
- Que el virus infecte archivos ejecutables y los dañe de algún modo, haciendo imposible su ejecución, y por lo tanto el no funcionamiento del programa.
- Que el virus se aloje en la memoria RAM y produzca efectos colaterales extraños como ser “crashes” o colgadas del sistema sin sentido aparente, disminución de la velocidad habitual de la PC, errores de lectura, fallas generales en los pendrives, etc.

- Que el virus produzca un daño grave en nuestra información: Borrado de archivos, formateo del disco rígido, etc.

Todo virus informático, como sus hermanos biológicos, tiene la función de autoreproducirse y de contagiar a otros huéspedes (computadoras.) Esta es la única forma de expandirse a otras máquinas. Si éstos virus, que tienen como finalidad causar algún daño, fueran fácilmente detectables, no estaríamos hablando de esto ahora.

Es por ello que los programas virus tienen que ser necesariamente **subrepticios,** o sea, funcionar en forma oculta, solapada, subterránea, y sin que se note su accionar y existencia.

Finalmente, para poder trabajar en forma oculta y poder reproducirse sin que el usuario lo note de inmediato, estos “programas” son casi siempre, muy pequeños en tamaño.

De todas maneras por muy pequeños que sean siempre que se infectan archivos éstos cambian de tamaño. Esto hace que los programas antivirus puedan controlar –como herramienta de seguridad- , el tamaño de los archivos más importantes del sistema.

¿Cómo se produce la infección ?

Las posibilidades si bien no son muchas, merecen su consideración. Seguramente infectaremos nuestra máquina si :

- Arrancamos nuestra PC con algún disco (rígido o disquete) infectado.
- Ejecutamos algún archivo (.exe, .doc, .com, etc.) infectado.
- “Bajamos” de Internet, vía módem u otro medio, algún archivo infectado y sin saberlo, lo abrimos.
- Abrimos algún documento de Word o Excel que contenga alguna "macro", que es otro lugar donde se alojan los virus.
- Nos llega algún mensaje de correo electrónico con un archivo “adjunto” que nos invita a abrirlo porque es un tema muy importante (como el gusano Melissa, I Love you, NetSky, BugBear, etc.etc.)

Métodos de propagación

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, más comúnmente: *Haz 2 clics y gana 2 tonos para móvil gratis.*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software modificado o de dudosa procedencia.

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 buffer y puertos de red para infiltrarse y contagiar el equipo, causar inestabilidad en el sistema, mostrar mensajes de error, reenviarse a otras máquinas mediante la red local o Internet y hasta reiniciar el sistema, entre otros daños. En las últimas versiones de Windows 2000, XP y Server 2003 se ha corregido este problema en su mayoría.

Medidas de prevención :

Siempre es bueno y saludable que cuando trabajemos frente a una PC, tengamos en cuenta algunas de estas posibles medidas de prevención para evitar males mayores :

- ✓ Conocer la procedencia de todo el software que tenemos en nuestra máquina.
- ✓ Tomar el hábito de revisar (scanear) todo disquete nuevo que vayamos a utilizar.
- ✓ Tratar de no arrancar desde pendrives a no ser que sea absolutamente imprescindible.
- ✓ Dentro de lo posible, adquirir software original.

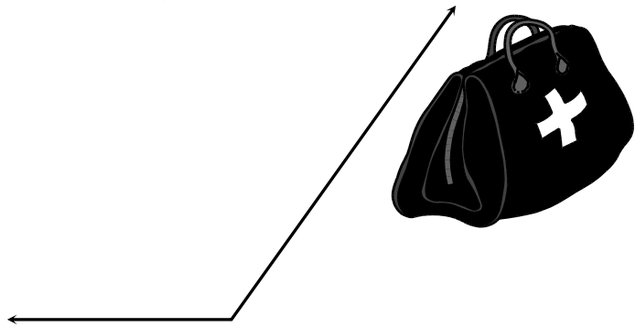
- ✓ Revisar con sumo cuidado los archivos de Word o Excel que vengan junto con mensajes de correo electrónico vía Internet.

- ✓ Contar con uno o mejor dos, programas antivirus. Si utlizamos una red o navegamos en Internet esto es imprescindible.

SOFTWARE ANTIVIRUS

Como era de suponer, existen también los programas que combaten a los virus informáticos. Está bien claro que no existe un único producto que pueda aniquilar el problema de los virus, y de acuerdo con muchas opiniones, nunca lo habrá.
Sin embargo hay algunos productos que se destacan por su performance a la hora de detectar y limpiar virus informáticos y sus variantes. Entre ellos podemos citar :

AVG
Kaspersky
Avast
Mcafee
Norton Antivirus
Avira
Eset
Panda Antivirus



Obviamente cada uno de ellos posee prestaciones y orientaciones diferentes y tienen versiones para todos los Sistemas Operativos. Algunos se especializan en la detección y otros en las tareas de remoción y limpieza.

Las actualizaciones de estos productos son un tema central dado la cantidad de virus nuevos que aparecen por mes). Es por eso que casi todos ellos, en su versión original, permiten descargar de Internet las actualizaciones necesarias para estar bien protegido todo el tiempo.

Hay cosas que no ocurren:

- ✓ No hay forma de infectar mi máquina si solo navego por la Web (en sitios seguros…) y no instalo nada de lo que me piden.

- ✓ Los virus no se reproducen por la corriente eléctrica (¿te imaginás?)

- ✓ Un virus no puede "destruir" hardware (no hay forma de que se derrita el teclado). Aunque se han detectado algunos extraños virus que afectan el BIOS de la PC (un componente de la memoria ROM)

¿Qué nos depara el futuro ?

Indudablemente el tema de Internet ha dado un nuevo empuje a la propagación de virus, en especial el correo electrónico que tiene la capacidad de colocar archivos adjuntos junto a los mensajes invitando al usuario a abrir ese “regalito”. En la actualidad la mayoría de los ataques pasan por los molestos spywares y propagandas no deseadas (adaware), programas y barras que se instalan si no somos cuidadosos la hacer click.