Virus y malwares.

Gran cantidad de virus, troyanos, spywares y todo tipo de malwares circulan en la web. Estos cambian la página de inicio de Internet Explorer, provocan la aparición de pantallas no deseadas, y ni hablar del riesgos de que nos hackeen, espíen, etc.

¿Qué es un virus informático?

Un **virus informático** es un software malicioso 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.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

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

Tipo de virus.

- **Virus de archivo.-** Son aquellos que infectan archivos, como su nombre indica.
    - **Virus residentes.-** Se ejecutan cada vez que encendemos el ordenador y se ocultan en la RAM de forma permanente, controlando todas las operaciones que se realizan con el ordenador, teniendo la capacidad de infectar todos los archivos que abramos, cerremos, copiemos, ejecutemos, etc.
    - **Virus de acción directa.-** Estos virus se reproducen y actúan en el mismo momento de ejecutarse. Normalmente sólo afectan a los archivos que se encuentran en su misma carpeta o en las que se encuentren en el path.

- **Virus de sobre escritura.-**Estos virus lo que hacen es escribir dentro de un archivo reemplazando su contenido. no variando de tamaño y quedando inservibles, debiendo ser eliminados con la consiguiente pérdida de la información que contengan.

- **Virus de macro.-** Son virus específicos para programas que usen macros (como *Word, Excel, PowerPoint, CorelDraw*).

- **Virus de ejecutables.-** Afectan exclusivamente a ficheros ejecutables (.exe y .com), produciendo una serie de efectos indeseados. A este tipo pertenecen la mayoría de los virus existentes.

- **Virus de disco**.- Son virus que no afectan a archivos, si no a las mismas unidades de almacenamiento.

    - **Virus de boot.-** Son aquellos que infectan los sectores de arranque del disco duro (boot). Para que estos actúen es necesario que arranquemos el ordenador con un medio que tenga el boot (arranque) infectado, por lo que, a pesar de ser extremadamente peligrosos, ya que infectan una parte esencial del sistema, pudiendo llegar a dejarlo inservible, es relativamente fácil protegerse de ellos.

    - **Virus de FAT.-** Estos virus atacan la FAT, que es el sector de un disco donde se guarda la información de la ubicación en este de las diferentes carpetas y archivos. Estos virus pueden dejar inaccesibles ficheros o directorios enteros.

Hay también programas maliciosos que no se pueden considerar completamente virus, pero sí una especie de pseudo virus:

- **Bombas lógicas.-** No se reproducen ni son programas en sí mismos, si no que se trata de códigos ocultos dentro de otro programa con la finalidad de destruir información y causar el mayor daño posible cuando se cumple una condición. Pueden llegar a ser extremadamente peligrosas, ya que incluso pueden llegar a eliminar toda la información de un disco.

- **Hoax.-** Los Hoaxes, también conocidos como virus falsos, son mensajes difundidos normalmente por correo electrónico destinados a crear confusión entre los usuarios al hacer creer la existencia de un falso virus. La función destinada a estos suele ser la de que el que lo recibe lo reenvíe a su lista de contactos, intentando de paso causar con ello una sobrecarga de tráfico en los servidores de correo.

- **Gusanos.-** Los gusanos (*worms*) no son virus propiamente dichos, ya que su cometido no es el de infectar ficheros, simplemente es el de reproducirse a una gran velocidad, llegando así a colapsar nuestro sistema. Su medio de propagación suele ser el correo electrónico, las redes y los chat. No infectan ningún fichero, pero pueden dejarnos totalmente bloqueado el ordenador.

¿Qué es un malware?

Es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.

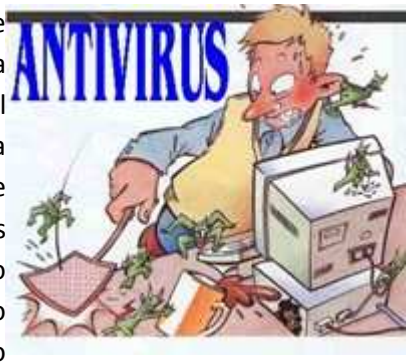
En el mundo de los **virus informáticos** hay una amplia variedad de tipos. Uno de los más activos y hasta cierto punto dañinos son los **virus espías** o **spyware**. Cada vez se utiliza más el término **malware** para definir al conjunto de este tipo de programas.
Un **spyware** o **virus espía** es un tipo de malware que tiene por finalidad la recopilación y envío de información sobre los propietarios o usuarios de un ordenador o sistema sin su conocimiento y consentimiento. Es un tipo de malware sumamente extendido (probablemente el que más) que además de enviar a terceros información personal de nuestro ordenador ralentiza este, siendo junto con el adware la principal causa de este problema.

Hay que aclarar que no todos los programas destinados a recopilar información sobre el usuario o el sistema son programas espía o spyware. Reciben esta denominación tan sólo cuando actúan **sin el conocimiento y consentimiento del usuario**.

- **Adware** .- Es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad al computador después de instalado el programa o mientras se está utilizando la aplicación.

- **Spyware**.- Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

- **Troyano**.- Un Troyano es un programa malicioso que se oculta en el interior de un programa de apariencia inocente. Cuando este último es ejecutado, el Troyano realiza la acción o se oculta en la máquina del usuario que lo ha ejecutado. Habitualmente se utiliza para espiar a personas, permite a terceros extraer información o tomar el control de nuestro ordenador, monitorear lo que alguien está haciendo en cada momento, (capturando sus pulsaciones o enviando capturas de pantalla del escritorio).



Vista la diferencia que hay entre un virus en general y un spyware en particular, las diferencias entre un programa antivirus y un programa antimalware son:

- Un **programa antivirus** es un programa diseñado para detectar los diferentes tipos de virus que hay, pero sin hacer una especial incidencia en los spyware. Ver **'Comparativa antivirus Feb-2009**'

Característica	Avast	Avast	AVG	AVG Free	McAfee	Norton	ESET	Panda

		Free				**(Symantec)**	**NOD32**	**Security**
Anti-Virus	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí
Anti-spyware	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí
Link Scanner	✗ No	✗ No	✓ Sí	✓ Sí	✗ No	✗ No	✗ No	✓ Sí
Anti-Rootkit	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí
Web Shield	✓ Sí	✓ Sí	✓ Sí	⚠ Limitado	✗ No	✓ Sí	✓ Sí	✓ Sí
ID Protection	✓ Sí	✗ No	✓ Sí	✗ No	✓ Sí	✓ Sí	✗ No	✓ Sí
Firewall	✗ No	✗ No	✓ Sí	✗ No	✓ Sí	✓ Sí	✓ Sí	✓ Sí
Anti-Spam	✓ Sí	✗ No	✓ Sí	✗ No	✗ No	✗ No	✗ No	✓ Sí
Sistemas x64	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✗ No	⚠ Limitado	✓ Sí	✓ Sí
Español	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí	✓ Sí
Soporte técnico	✓ Sí	✗ No	✓ Sí	Solo FAQ	30 días	✓ Sí	✓ Sí	✓ Sí
Mac y Linux	✓ Sí	✗ No	Linux	Linux	✗ No	Mac	Linux	Linux
Consumo de Recursos	Muchos al arrancar	Muchos al arrancar	Pocos	Pocos	Termino Medio	Muchos	Pocos	Pocos
Version	4.8	4.8	9.0	9.0	2009	2009	?	2010

- Un programa **anti-spyware** es un tipo de antivirus, pero diseñado específicamente para detectar, detener y eliminar spyware, lo que hace que su efectividad contra este tipo determinado de virus sea muy alta.
    - Spyware Doctor
    - Ad-Aware SE Personal
    - Malwarebytes' Anti-Malware
    - SUPERAntiSpyware
    - SpyBot Search & Destroy
    - **Sin Espias Antispyware**

- Spy Sweeper
- Pc Tools Spyware Doctor

Top Virus

Top 10 Virus Informáticos

- **CREEPER (1971)**: el primer programa gusano corrió en un equipo DEC 10 bajo el sistema operativo TOPS TEN.
- **ELK CLONER (1985)**: el primer virus para computadores personales, concretamente para los sistemas Apple II. Creado por un estudiante, el virus infectaba el sistema operativo, se copiaba en los discos flexibles y desplegaba uno o dos versos de un poema. El virus no tuvo mucha notoriedad ni provocó grandes preocupaciones, sin embargo, pocos se dieron cuenta de que iniciaría una generación de ciber criminales y, en paralelo, una industria de seguridad de la información.
- **El INTERNET WORM (1985)**: escrito por una persona de la Universidad Cornell que paralizó Internet.
- **PAKISTANI BRAIN (1988)**: el primer virus que infectó el PC de IBM y fue escrito por dos hermanos de Pakistán. Este fue el primer virus que recibió amplia cobertura de los medios, aunque los virus ya se conocían en la ciencia ficción.
- **JERUSALEM FAMILY (1990)**: se contabilizaron casi cincuenta variables de este virus, que se cree salió de la Universidad de Jerusalén.
- **STONED (1989)**: es el virus que más se propagó en la primera década de los virus. Stoned infectaba el sector de arranque/.mbr que contaba el número de reinicios desde la infección original y mostraba la frase “your computer is now stoned”.
- **DARK AVENGER MUTATION ENGINE (1990)**: fue escrito en 1988, pero se utilizó a principios de los noventa en virus como POGUE y COFFEESHOP. Este Motor de Mutación fue el primer Polimorfo real que se usó a nivel masivo y cambió para siempre la forma en que funcionan los virus.
- **MICHEANGELO (1992)**: una variante de STONED, con una carga destructiva. El 6 de marzo, este virus borró los primeros 100 sectores de un disco duro, dejándolo inútil. Provocó uno de los primeros pánicos mediáticos alrededor de los virus de equipos informáticos.
- **WORLD CONCEPT (1995)**: el primer macro virus para Microsoft Word. Word Concept escribía la frase, “That’s enough to prove my point”. Inició la segunda era de los virus y fue importante en el sentido de que llevó los virus a un nivel de hackers mucho menos avanzado.
- **CIH/CHERNOBYL (1998)**: El virus Chernobyl fue el virus más destructivo jamás

visto, hasta entonces. Atacando los días 26 de cada mes (dependiendo de la versión involucrada), borraba el disco duro, y eliminaba el flash ROM BIOS de la computadora en cuestión.

Top 10 Virus 2009

- **Win32/Conficker:** como de costumbre, una vulnerabilidad en Windows – en este caso en el subsistema RPC – ha permitido la proliferación de uno de los virus más problemáticos del año. Hablamos del popular **Conficker** que, utilizando una característica de **Windows** (XP en particular) consiguió infectar a un gran número de ordenadores. Para evitar la infección por este virus debemos descargar el parche desarrollado por **Microsoft** el pasado mes de octubre.

- **INF/Autorun:** Esta "simpatico" virus de ordenador infecta el PC mediante la creación de un archivo "**autorun.inf**". Esto se realiza de forma automática cuando un dispositivo extraíble se conecta al ordenador. Ergo, se puede evitar desactivando esta función automática

- **Win32/PSW.OnLineGames:** un buen troyano dedicado a complicar la vida de todos los amantes de los videojuegos. Su función es la de robar información privada, números de tarjetas de crédito y contraseñas.

- **Wind32/Agent:** copia archivos en la carpeta temporal de la computadora infectada, este virus se inicia automáticamente cada vez que se inicie sesión en **Windows** y roba toda la información sensible. Un buen **anti-malware** es la mejor arma para cazar y eliminar este tipo de virus.

- **Win32/FlyStudio:** cambia la configuración del navegador para redirigir a sus víctimas a sitios poco recomendables, llenos de publicidad…

- **INF/Conficker:** increíble pero cierto, este virus explota la función automática de Windows para arrancar y descargar otros programas maliciosos. Una vez más, la mejor solución es desactivar la función de arranque automático de CD / DVD y de dispositivos extraíbles.

- **Win32/Pacex.Gen:** se trata de un montón de programas maliciosos que crea el mismo puede robar las contraseñas y la información sensible de la víctima.

- **WMA/TrojanDownloader.GetCodec:** Este virus edita archivos de audio que encuentre en el sistema, convirtiéndolos en "**wma**", que, al abrirse en **Windows Media Player**, hace que este programa descarge un códec falso lleno de código malicioso. La mejor solución es evidar la descarga de codecs por parte de **Windows Media Player**.

- **Win32/Qhost:** se introduce en la carpeta "**System32**" de **Windows**, permitiendo que el equipo pueda ser manejado a distancia. Además, cambia la **configuración de DNS** para redirigir los navegadores a sitios poco recomendados.

- **Win32/Autorun:** si tenéis en cuenta el nombre creo que es bastante evidente lo

que hace….ejecutarse automáticamente al introducir elementos extraibles / CD / DVD.