# Malware o Software malicioso



El malware suele ser representado con símbolos de peligro.

# 1 - Introducción

**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. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

El software se considera malware en función de los efectos que, pensados por el creador, provoque en un computador. El término *malware* incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.

Malware no es lo mismo que software defectuoso; este último contiene bugs peligrosos, pero no de forma intencionada.

Los resultados provisionales de Symantec publicados en el 2008 sugieren que «el ritmo al que se ponen en circulación códigos maliciosos y otros programas no deseados podría haber superado al de las aplicaciones legítimas». Según un reporte de F-Secure, «Se produjo tanto malware en 2007 como en los 20 años anteriores juntos».

Según Panda Security, durante los 12 meses del 2011 se han creado 73.000 nuevos ejemplares de amenazas informáticas por día, 10.000 más de la media registrada en todo el año 2010. De éstas, el 73 por ciento son troyanos y crecen de forma exponencial los del subtipo downloaders.

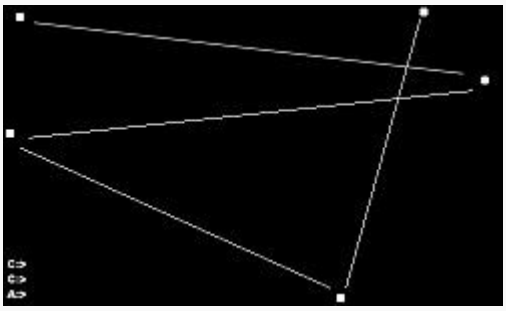
Algunos de los primeros programas infecciosos, incluido el Gusano Morris y algunos virus de MS-DOS, fueron elaborados como experimentos, como bromas o simplemente como algo molesto, no para causar graves daños en las computadoras. En algunos casos elprogramador no se daba cuenta de cuánto daño podía hacer su creación. Algunos jóvenes que estaban aprendiendo sobre los virus los crearon con el único propósito de demostrar que podían hacerlo o simplemente para ver con qué velocidad se propagaban. Incluso en1999 un virus tan extendido como Melissa parecía haber sido elaborado tan sólo como una travesura.

El software diseñado para causar daños o pérdida de datos suele estar relacionado con actos de vandalismo. Muchos virus son diseñados para destruir archivos en disco duro o para corromper el sistema de archivos escribiendo datos inválidos. Algunos gusanos son diseñados para vandalizar páginas web dejando escrito el alias del autor o del grupo por todos los sitios por donde pasan. Estos gusanos pueden parecer el equivalente informático del grafiti.

Sin embargo, debido al aumento de usuarios de Internet, el software malicioso ha llegado a ser diseñado para sacar beneficio de él, ya sea legal o ilegalmente. Desde 2003, la mayor parte de los virus y gusanos han sido diseñados para tomar control de computadoras para su explotación en el mercado negro. Estas computadoras infectadas "computadoras zombis" son usadas para el envío masivo de spampor correo electrónico, para alojar datos ilegales como pornografía infantil, o para unirse en ataques DDoS como forma de extorsión entre otras cosas.

Hay muchos más tipos de malware producido con ánimo de lucro, por ejemplo el spyware, el adware intrusivo y los hijacker tratan de mostrar publicidad no deseada o redireccionar visitas hacia publicidad para beneficio del creador. Estos tipos de malware no se propagan como los virus, generalmente son instalados aprovechándose de vulnerabilidades o junto con software legítimo como aplicaciones P2P.

## 2 - Malware infeccioso: virus y gusanos



Virus de ping-pong.

Los tipos más conocidos de malware, virus y gusanos, se distinguen por la manera en que se propagan, más que por otro comportamiento particular.

El término *virus informático* se usa para designar un programa que, al ejecutarse, se propaga infectando otros softwares ejecutables dentro de la misma computadora. Los virus también pueden tener un payload que realice otras acciones a menudo maliciosas, por ejemplo, borrar archivos. Por otra parte, un gusano es un programa que se transmite a sí mismo, explotando vulnerabilidades en una red de computadoras para infectar otros equipos. El principal objetivo es infectar a la mayor cantidad posible de usuarios, y también puede contener instrucciones dañinas al igual que los virus.

Nótese que un virus necesita de la intervención del usuario para propagarse mientras que un gusano se propaga automáticamente. Teniendo en cuenta esta distinción, las infecciones transmitidas por correo electrónico o documentos de Microsoft Word, que dependen de su apertura por parte del destinatario para infectar su sistema, deberían ser clasificadas más como virus que como gusanos.

# 3 - Malware oculto: Backdoor o Puerta trasera, Drive-by Downloads, Rootkits y Troyanos

Para que un software malicioso pueda completar sus objetivos, es esencial que permanezca oculto al usuario. Por ejemplo, si un usuario experimentado detecta un programa malicioso, terminaría el proceso y borraría el malware antes de que este pudiera completar sus objetivos. El ocultamiento también puede ayudar a que el malware se instale por primera vez en la computadora.

## 3.1 Puertas traseras o Backdoors

Un *backdoor* o *puerta trasera* es un método para eludir los procedimientos habituales de autenticación al conectarse a una computadora. Una vez que el sistema ha sido comprometido (por uno de los anteriores métodos o de alguna otra forma), puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro. Las puertas traseras también pueden instalarse previamente al software malicioso para permitir la entrada de los atacantes.

Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, intentando permanecer ocultos ante una posible inspección. Para instalar puertas traseras los crackers pueden usar troyanos, gusanos u otros métodos.

Se ha afirmado, cada vez con mayor frecuencia, que los fabricantes de ordenadores preinstalan puertas traseras en sus sistemas para facilitar soporte técnico a los clientes, pero no ha podido comprobarse con seguridad.

Un malware en Skype está siendo el problema reciente en la seguridad, debido a que a mayo del 2013, existían ya 750 mil afectados siendo el 67% en Latinoamérica. El código malicioso afecta al equipo y se propaga entre los contactos a través de este mismo medio de comunicación.

## 3.2 Drive-by Downloads

Google ha descubierto que una de cada 10 páginas web que han sido analizadas a profundidad puede contener los llamados *drive by downloads*, que son sitios que instalan spyware o códigos que dan información de los equipos sin que el usuario se percate.

A estas acciones Niels Provos y otros colaboradores de Google Inc le denominaron, en un artículo, "El fantasma en la computadora". Por ello, se están realizando esfuerzos para identificar las páginas que pudieran ser maliciosas.

El término puede referirse a las descargas de algún tipo de malware que se efectúa sin consentimiento del usuario, lo cual ocurre al visitar un sitio web, al revisar un mensaje de correo electrónico o al entrar a una ventana pop-up, la cual puede mostrar un mensaje de error. Sin ser su verdadera intención, el usuario consiente la descarga de software indeseable o de malware, y estas vulnerabilidades se aprovechan.

El proceso de ataque Drive-by Downloads se realiza de manera automática mediante herramientas que buscan en el sitio web alguna vulnerabilidad. Una vez encontrada, insertan un scriptmalicioso dentro del código HTML del sitio violado. Cuando un usuario visita el sitio infectado, éste descargará dicho script en el sistema del usuario, y a continuación realizará una petición a un servidor Hop Point, donde se solicitarán nuevos scripts con exploits encargados de comprobar si el equipo tiene alguna vulnerabilidad que pueda ser explotada, intentando con ellas hasta que tienen éxito, en cuyo caso se descargará un script que descarga el archivo ejecutable (malware) desde el servidor.

En la mayor parte de los navegadores se están agregando bloqueadores antiphishing y antimalware que contienen alertas que se muestran cuando se accede a una página web dañada, aunque no siempre dan una total protección.

## 3.3 Rootkits

Las técnicas conocidas como rootkits modifican el sistema operativo de una computadora para permitir que el malware permanezca oculto al usuario. Por ejemplo, los rootkits evitan que un proceso malicioso sea visible en la lista de procesos del sistema o que sus ficheros sean visibles en el explorador de archivos. Este tipo de modificaciones consiguen ocultar cualquier indicio de que el ordenador esta infectado por un malware. Originalmente, un rootkit era un conjunto de herramientas instaladas por un atacante en un sistema Unix donde el atacante había obtenido acceso de administrador (acceso root). Actualmente, el término es usado mas generalmente para referirse a la ocultación de rutinas en un programa malicioso.

Algunos programas maliciosos también contienen rutinas para evitar ser borrados, no sólo para ocultarse. Un ejemplo de este comportamiento puede ser:

> *"Existen dos procesos-fantasmas corriendo al mismo tiempo. Cada proceso-fantasma debe detectar que el otro ha sido terminado y debe iniciar una nueva instancia de este en cuestión demilisegundos. La única manera de eliminar ambos procesos-fantasma es eliminarlos simultáneamente, cosa muy difícil de realizar, o provocar un error el sistema deliberadamente."*

Uno de los rootkits más famosos fue el que la empresa Sony BMG Music Entertainment. Secretamente incluyó, dentro de la protección anticopia de algunos CD de música, el software “Extended Copy Protection (XCP) y MediaMax CD-3”, los cuales modificaban a Windows para que no lo pudiera detectar y también resultar indetectable por los programas anti-virus y anti-spyware. Actuaba enviando información sobre el cliente, además abrió la puerta a otros tipos de malware que pudieron infiltrarse en las computadoras, además de que si se detectaba, no podía ser eliminado, pues se dañaba el sistema operativo.

Mikko Hypponen, jefe de investigación de la empresa de seguridad, F-Secure con sede en Finlandia, consideró a este rootkit como uno de los momentos fundamentales de la historia de los malware.

### 3.4 Troyanos


Captura de pantalla del Troyano “Beast"

El término troyano suele ser usado para designar a un malware que permite la administración remota de una computadora, de forma oculta y sin el consentimiento de su propietario, por parte de un usuario no autorizado. Este tipo de malware es un híbrido entre un troyano y una puerta trasera, no un troyano atendiendo a la definición.

A grandes rasgos, los troyanos son programas maliciosos que están disfrazados como algo inocuo o atractivo que invitan al usuario a ejecutarlo ocultando un software malicioso. Ese software, puede tener un efecto inmediato y puede llevar muchas consecuencias indeseables, por ejemplo, borrar los archivos del usuario o instalar más programas indeseables o maliciosos.

Los tipos de troyanos son: backdoors, banker, botnets, dialer, dropper, downloaders, keylogger, password stealer, proxy.

Los troyanos conocidos como *droppers* son usados para empezar la propagación de un gusano inyectándolo dentro de la red local de un usuario.

Una de las formas más comunes para distribuir spyware es mediante troyanos unidos a software deseable descargado de Internet. Cuando el usuario instala el software esperado, el spyware es puesto también. Los autores de spyware que intentan actuar de manera legal pueden incluir unos términos de uso, en los que se explica de manera imprecisa el comportamiento del spyware, que los usuarios aceptan sin leer o sin entender.

## 4 - Malware para obtener beneficios

Durante los años 80 y 90, se solía dar por hecho que los programas maliciosos eran creados como una forma de vandalismo o travesura. Sin embargo, en los últimos años la mayor parte del malware ha sido creado con un fin económico o para obtener beneficios en algún sentido. Esto es debido a la decisión de los autores de malware de sacar partido

monetario a los sistemas infectados, es decir, transformar el control sobre los sistemas en una fuente de ingresos.

## 4.1 Mostrar publicidad: Spyware, Adware y Hijacking

Los programas spyware son creados para recopilar información sobre las actividades realizadas por un usuario y distribuirla a agencias de publicidad u otras organizaciones interesadas. Algunos de los datos que recogen son las páginas web que visita el usuario y direcciones de correo electrónico, a las que después se envía spam. La mayoría de los programas spyware son instalados como troyanos junto a software deseable bajado de Internet. Otros programas spyware recogen la información mediante cookies de terceros o barra de herramientas instaladas en navegadores web. Los autores de spyware que intentan actuar de manera legal se presentan abiertamente como empresas de publicidad e incluyen unos términos de uso, en los que se explica de manera imprecisa el comportamiento del spyware, que los usuarios aceptan sin leer o sin entender.

Por otra parte los programas adware muestran publicidad al usuario de forma intrusiva en forma de ventana emergente (pop-up) o de cualquier otra forma. Esta publicidad aparece inesperadamente en el equipo y resulta muy molesta. Algunos programas shareware permiten usar el programa de forma gratuita a cambio de mostrar publicidad, en este caso el usuario consiente la publicidad al instalar el programa. Este tipo de adware no debería ser considerado malware, pero muchas veces los términos de uso no son completamente transparentes y ocultan lo que el programa realmente hace.

Los hijackers son programas que realizan cambios en la configuración del navegador web. Por ejemplo, algunos cambian la página de inicio del navegador por páginas web de publicidad o páginapornográfica, otros redireccionan los resultados de los buscadores hacia anuncios de pago o páginas de phishing bancario. El pharming es una técnica que suplanta al DNS, modificando elarchivo hosts, para redirigir el dominio de una o varias páginas web a otra página web, muchas veces una web falsa que imita a la verdadera. Esta es una de las técnicas usadas por los hijackers o secuestradores del navegador de Internet. Esta técnica también puede ser usada con el objetivo de obtener credenciales y datos personales mediante el secuestro de una sesión.

## 4.2 Robar información personal: Keyloggers y Stealers

Cuando un software produce pérdidas económicas para el usuario de un equipo, también se clasifica como crimeware o software criminal, término dado por Peter Cassidy para diferenciarlo de los otros tipos de software malicioso. Estos programas están encaminados al aspecto financiero, la suplantación de personalidad y el espionaje.

Un ejemplo de cómo un hardware PS/2 keylogger está conectado.

Los keyloggers y los stealers son programas maliciosos creados para robar información sensible. El creador puede obtener beneficios económicos o de otro tipo a través de su uso o distribución en comunidades underground. La principal diferencia entre ellos es la forma en la que recogen la información.

Los keyloggers monitorizan todas las pulsaciones del teclado y las almacenan para un posterior envío al creador. Por ejemplo al introducir un número de tarjeta de crédito el keylogger guarda el número, posteriormente lo envía al autor del programa y este puede hacer pagos fraudulentos con esa tarjeta. Si las contraseñas se encuentran recordadas en el equipo, de forma que el usuario no tiene que escribirlas, el keylogger no las recoge, eso lo hacen los stealers. La mayoría los keyloggers son usados para recopilar contraseñas de acceso pero también pueden ser usados para espiar conversaciones de chat u otros fines.

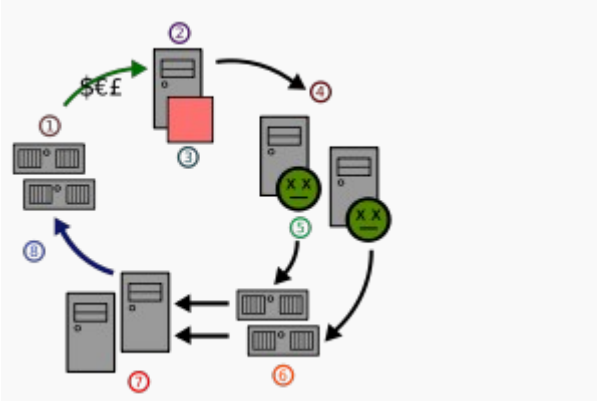
Los stealers también roban información privada pero solo la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas recordadas, por ejemplo en los navegadores web o en clientes de mensajería instantánea, descifran esa información y la envían al creador.

## 4.3 Realizar llamadas telefónicas: Dialers

Los dialers son programas maliciosos que toman el control del módem dial-up, realizan una llamada a un número de teléfono de tarificación especial, muchas veces internacional, y dejan la línea abierta cargando el coste de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos, salva pantallas, pornografía u otro tipo de material.

Actualmente la mayoría de las conexiones a Internet son mediante ADSL y no mediante módem, lo cual hace que los dialers ya no sean tan populares como en el pasado.

## 4.4 Ataques distribuidos: Botnets




**Ciclo de spam**
(1): Sitio web de Spammers
(2): Spammer
(3): Spamware
(4): equipos infectados
(5): Virus o troyanos
(6): Servidores de correo
(7): Usuarios
(8): Tráfico Web.

Las botnets son redes de computadoras infectadas, también llamadas "zombis", que pueden ser controladas a la vez por un individuo y realizan distintas tareas. Este tipo de redes son usadas para el envío masivo de spam o para lanzar ataques DDoS contra organizaciones como forma de extorsión o para impedir su correcto funcionamiento. La ventaja que ofrece a los spammers el uso de ordenadores infectados es el anonimato, que les protege de la persecución policial.

En una botnet cada computadora infectada por el malware se loguea en un canal de IRC u otro sistema de chat desde donde el atacante puede dar instrucciones a todos los sistemas infectados simultáneamente. Las botnets también pueden ser usadas para actualizar el malware en los sistemas infectados manteniéndolos así resistentes ante antivirus u otras medidas de seguridad.

## 4.5 Otros tipos: Rogue software y Ransomware

Los rogue software hacen creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.

### 4.5.1 Los Ransomware

También llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un "rescate" para poder recibir la contraseña que permite recuperar los archivos.

InfoSpyware reporta en su blog que a partir de mayo del 2012, han existido 2 nuevas variantes del llamado "virus de la policía" ó "Virus Ukash", que es producido por el troyano Ransom.ab, que con el pretexto de que se entró a páginas de pornografía infantil, se les hace pagar una supuesta multa para poder desbloquear sus equipos, actualmente también utilizando la propia cámara Web del equipo hacen unas supuestas tomas de vídeo que anexan en su banner de advertencia, para asustarlos más al hacerlos pensar

que están siendo observado y filmado por la policía, siendo Rusia, Alemania, España y Brasil los países más afectados ó la versión falsa del antivirus gratuito "Microsoft Security Essentials" que dice bloquear el equipo por seguridad y que para poder funcionar adecuadamente se ofrece un módulo especial que se tiene que pagar.

La Brigada de Investigación Tecnológica de la Policía Nacional de España, junto con Europol e Interpol, desmantelaron en febrero del 2013, a la banda de piratas informáticos creadores del "Virus de la Policía", responsables de estafar alrededor de 1 millón de euros al año.

A pesar de de ello, han surgiendo nuevas versiones y variantes, pero con las características propias de las policías de países de Latinoamérica, siendo los países afectados Argentina, Bolivia, Ecuador, Uruguay y México, en este último saca la imagen de la desaparecida Policía Federal Preventiva .

## 5 - Grayware o greynet

Los términos *grayware* (o *greyware*) y *graynet* (o *greynet*) (del inglés *gray* o *grey*, "gris") suelen usarse para clasificar aplicaciones o programas de cómputo que se instalan sin la autorización del departamento de sistemas de una compañía; se comportan de modo tal que resultan molestos o indeseables para el usuario, pero son menos peligrosos que los malware. En este grupo se incluyen: adware, dialers, herramientas de acceso remoto, programas de bromas (*Virus joke*), programas para conferencias, programa de mensajería instantánea, spyware y cualesquiera otros archivos y programas no bienvenidos que no sean virus y que puedan llegar a dañar el funcionamiento de una computadora o de una red. El término *grayware* comenzó a utilizarse en septiembre del 2004.

## 6 - Vulnerabilidades usadas por el malware

Existen varios factores que hacen a un sistema más vulnerable al malware: **homogeneidad**, **errores de software**, **código sin confirmar**, **sobre-privilegios de usuario** y **sobre-privilegios de código**.

Una causa de la vulnerabilidad de redes, es la homogeneidad del software multiusuario. Por ejemplo, cuando todos los ordenadores de una red funcionan con el mismo sistema operativo, si se puede comprometer ese sistema, se podría afectar a cualquier ordenador que lo use. En particular, Microsoft Windows tiene la mayoría del mercado de los sistemas operativos, esto permite a los creadores de malware infectar una gran cantidad de computadoras sin tener que adaptar el software malicioso a diferentes sistemas operativos.

La mayoría del software y de los sistemas operativos contienen bugs que pueden ser aprovechados por el malware. Los ejemplos típicos son los desbordamiento de búfer (buffer overflow), en los cuales la estructura diseñada para almacenar datos en un área

determinada de la memoria permite que sea ocupada por más datos de los que le caben, sobre escribiendo otras partes de la memoria. Esto puede ser utilizado por el malware para forzar al sistema a ejecutar su código malicioso.


Las memorias USB infectadas pueden dañar la computadora durante el arranque.

Originalmente las computadoras tenían que ser booteadas con un disquete, y hasta hace poco tiempo era común que fuera el dispositivo de arranque por defecto. Esto significaba que un disquete contaminado podía dañar la computadora durante el arranque, e igual se aplica a CD y memorias USB con la función AutoRun de Windows la que ya ha sido modificada. Aunque eso es menos común ahora, sigue siendo posible olvidarse de que el equipo se inicia por defecto en un medio removible, y por seguridad normalmente no debería haber ningún disquete, CD, etc., al encender la computadora. Para solucionar este problema de seguridad basta con entrar en la BIOS del ordenador y cambiar el modo de arranque del ordenador.

En algunos sistemas, los usuarios no administradores tienen sobre-privilegios por diseño, en el sentido que se les permite modificar las estructuras internas del sistema, porque se les han concedido privilegios inadecuados de administrador o equivalente. Esta es una decisión de la configuración por defecto, en los sistemas de Microsoft Windows la configuración por defecto es sobre-privilegiar al usuario. Esta situación es debida a decisiones tomadas por Microsoft para priorizar la compatibilidad con viejos sistemas sobre la seguridad y porque las aplicaciones típicas fueron desarrollados sin tener en cuenta a los usuarios no privilegiados. Como los exploits para escalar privilegios han aumentado, esta prioridad está cambiando para el lanzamiento deWindows Vista. Como resultado, muchas aplicaciones existentes que requieren excesos de privilegios pueden tener problemas de compatibilidad con Windows Vista. Sin embargo, el control de cuentas de usuario (UAC en inglés) de Windows Vista intenta solucionar los problemas que tienen las aplicaciones no diseñadas para usuarios no privilegiados a través de la virtualización, actuando como apoyo para resolver el problema del acceso privilegiado inherente en las aplicaciones heredadas.

El malware, funcionando como código sobre-privilegiado, puede utilizar estos privilegios para modificar el funcionamiento del sistema. Casi todos los sistemas operativos populares, y también muchas aplicaciones scripting permiten códigos con muchos privilegios, generalmente en el sentido que cuando un usuario ejecuta el código, el sistema no limita ese código a los derechos del usuario. Esto hace a los usuarios

vulnerables al malware contenido en archivos adjuntos de correos electrónicos, que pueden o no estar disfrazados. Dada esta situación, se advierte a los usuarios de que abran solamente archivos solicitados, y ser cuidadosos con archivos recibidos de fuentes desconocidas. Es también común que los sistemas operativos sean diseñados de modo que reconozcan dispositivos de diversos fabricantes y cuenten con drivers para estos hardwares, algunos de estos drivers pueden no ser muy confiables.

### 6.1 Eliminando código sobre-privilegiado

El código sobre-privilegiado se remonta a la época en la que la mayoría de programas eran entregados con la computadora. El sistema debería mantener perfiles de privilegios y saber cuál aplicar según el usuario o programa. Al instalar un nuevo software el administrador necesitaría establecer el perfil predeterminado para el nuevo código.

Eliminar las vulnerabilidades en los drivers de dispositivos es probablemente más difícil que en los software ejecutables. Una técnica, usada en VMS, que puede ayudar es solo mapear en la memoria los registros de ese dispositivo.

Otras propuestas son:

- Varias formas de virtualización, permitiendo al código acceso ilimitado pero solo a recursos virtuales.
- Varias formas de aislamiento de procesos también conocido como sandbox.
- La virtualizacion a nivel de sistema operativo que es un método de abstracción del servidor en donde el kernel del sistema operativo permite múltiples instancias de espacio de usuario llamadas contenedores, VEs, SPV o jails, que pueden ser parecidas a un servidor real.
- Las funciones de seguridad de Java.

Tales propuestas, sin embargo, si no son completamente integradas con el sistema operativo, duplicarían el esfuerzo y no serían universalmente aplicadas, esto sería perjudicial para la seguridad.

## 7 - Programas anti-malware

Como los ataques con malware son cada vez más frecuentes, el interés ha empezado a cambiar de protección frente a virus y spyware, a protección frente al malware, y los programas han sido específicamente desarrollados para combatirlos.

Los programas anti-malware pueden combatir el malware de dos formas:

1. Proporcionando protección en tiempo real (real-time protection) contra la instalación de malware en una computadora. El software anti-malware escanea

todos los datos procedentes de la red en busca de malware y bloquea todo lo que suponga una amenaza.

2. Detectando y eliminando malware que ya ha sido instalado en una computadora. Este tipo de protección frente al malware es normalmente mucho más fácil de usar y más popular. Este tipo de programas anti-malware escanean el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en la computadora. Al terminar el escaneo muestran al usuario una lista con todas las amenazas encontradas y permiten escoger cuales eliminar.

La protección en tiempo real funciona idénticamente a la protección de los antivirus: el software escanea los archivos al ser descargados de Internet y bloquea la actividad de los componentes identificados como malware. En algunos casos, también pueden interceptar intentos de ejecutarse automáticamente al arrancar el sistema o modificaciones en el navegador web. Debido a que muchas veces el malware es instalado como resultado de exploits para un navegador web o errores del usuario, usar un software de seguridad para proteger el navegador web puede ser una ayuda efectiva para restringir los daños que el malware puede causar.

## 8 - Métodos de protección

Siguiendo algunos sencillos consejos se puede aumentar considerablemente la seguridad de una computadora, algunos son:


Protección a través del número de cliente y la del generador de claves dinámicas

- Tener el sistema operativo y el navegador web actualizados.
- Tener instalado un antivirus y un firewall y configurarlos para que se actualicen automáticamente de forma regular ya que cada día aparecen nuevas amenazas.
- Utilizar una cuenta de usuario con privilegios limitados, la cuenta de administrador solo debe utilizarse cuándo sea necesario cambiar la configuración o instalar un nuevo software.
- Tener precaución al ejecutar software procedente de Internet o de medio extraíble como CD o memorias USB. Es importante asegurarse de que proceden de algún sitio de confianza.

- Una recomendación en tablet, teléfono celular y otros dispositivos móviles es instalar aplicaciones de tiendas muy reconocidas como App Store,Google Play o Nokia Store, pues esto garantiza que no tendrán malware. Existe además, la posibilidad de instalar un antivirus para este tipo de dispositivos.
- Evitar descargar software de redes P2P, ya que realmente no se sabe su contenido ni su procedencia.
- Desactivar la interpretación de Visual Basic Script y permitir JavaScript, ActiveX y cookies sólo en páginas web de confianza.
- Utilizar contraseñas de alta seguridad para evitar ataques de diccionario.

Es muy recomendable hacer copias de respaldo regularmente de los documentos importantes a medios extraíbles como CD, DVD o Disco duro externo, para poderlos recuperar en caso de infección por parte de algún malware, pero solamente si se esta 100% seguro que esas copias están limpias.

**Nota:** El método de restauración de sistema de windows, podría restaurar también archivos infectados, que hayan sido eliminados anteriormente por el antivirus, por tanto es necesario, desactivar ésta función antes de desinfectar el sistema, y posteriormente reactivarla.