EL VIRUS INFORMATICO Y LOS ANTIVIRUS

¿QUÉ ES UN VIRUS INFORMÁTICO?

Un virus informático es un programa de computadora, tal y como podría ser un procesador de textos, una hoja de cálculo o un juego. Un virus informático ocupa una cantidad mínima de espacio en disco, se ejecuta sin conocimiento del usuario y se dedica a autor replicarse.

CLASIFICACIÓN:

Dependiendo del lugar donde se alojan, la técnica de replicación o la plataforma en la cual trabajan, podemos clasificarlos:

VIRUS DE SECTOR DE ARRANQUE (BOOT).

Utilizan el sector de arranque, el cual contiene la información sobre el tipo de disco, es decir, numero de pistas, sectores, caras, tamaño de la FAT, sector de comienzo, etc.

VIRUS DE ARCHIVOS.

Infectan archivos y tradicionalmente los tipos ejecutables COM y EXE.

VIRUS DE ACCION DIRECTA.

Son aquellos que no quedan residentes en memoria y que se replican en el momento de ejecutarse un archivo infectado.

VIRUS DE SOBREESCRITURA.

Corrompen el archivo donde se ubican al sobrescribirlo.

VIRUS DE MACRO.

Estos programas usan el lenguaje de macros WordBasic, gracias al cual pueden infectar y replicarse a través de archivos MS-Word (DOC). En la actualidad esta técnica se ha extendido a otras aplicaciones como Excel y a otros lenguajes de macros

VIRUS BAT.

Este tipo de virus empleando ordenes DOS en archivos de proceso por lotes consiguen replicarse y efectuar efectos dañinos como cualquier otro tipo virus.

VIRUS DEL MIRC.

Consiste en un script para el cliente de IRC Mirc. Cuando alguien accede a un canal de IRC, donde se encuentre alguna persona infectada, recibe por DCC un archivo llamado "script.ini".

FUNCIONAMIENTO:

Para poder defendernos bien de las amenazas de los virus debemos contar con las herramientas necesarias para hacerle frente: antivirus, Antispyware, removedor de troyanos, firewall (son los mas destacados).

Tipos de virus y formas de combatirlos

Los virus son programas cuya finalidad es causar algún tipo de daño sobre un ordenador. Un virus es solamente un programa, lo que pasa que un programa con malas intenciones. La mayoría de los virus se desarrollan en entornos de Microsoft, siendo lo virus para Linux y Mac mucho menos comunes y de alcance menor, eso si, eso no quiere decir que lo usuarios de Mac y Linux estén exentos de Virus, ya que cada vez salen más tipo de virus, y por ejemplo algún tipo de Pishing es indiferente al sistema operativo y puede hacer mucho daño.Los virus adquirieron ese nombre por la capacidad de propagación que algunos tipos demuestran. Algunos infectan tu lista de contactos de correos, como los virus en la vida real.

Con este artículo pretendo mostrar los tipos de virus que hay de una manera no muy técnica para que todo el mundo pueda entender de una manera sencilla cómo funcionan y las técnicas utilizadas para su propagación.

La forma más sencilla y más común de propagación de un virus es el mail. La mayoría de los virus necesitan que el usuario ejecute un link o la orden para que el virus se instale,

para ello, los creadores de los virus estudian los habitos de los usuarios para saber la manera más sencilla.Por ejemplo, hacer que el virus se ejecute a través de un link a un archivo de humor, erotismo. Es bastante común mandar virus escondidos en documentos como documentos de PowerPoint, etc.

Lo malo de esto es que el usuario hay muchas veces que no se entera, y envía ese mismo mail a sus contactos pensando que

es algo de humor cuando en realizad está ayudando a propagar el virus. Otra posibilidad es la de que el virus tenga la capacidad de reproducirse, lo que significa que al ser infectado, él mismo está programado para enviarse a todos tus contactos, con un link atractivo para que el resto de usuarios caiga igual y así se van infectando todos.Esta es la manera con la que virus tan conocidos como el "I LOVE YOU" se propagaron tan rápidamente.
Otra de las maneras en la que los virus se pueden propagar es mediante la red, es decir, en páginas en Internet que el link o el ejecutable te introduce un virus pareciendo que hacen otra cosa. Por ejemplo, la típica página de cracks o de descarga de software gratuita que saben que la gente demanda mucho, y que aprovechan para infectarte cuando clickeas sobre el link que necesitas descargar. Yo aconsejo no bajar nunca de páginas de este tipo.
También las redes P2P es un método directo de propagación de virus. Se suele tener la costumbre de ir a la carpeta descargas y ejecutar archivos comprimidos, ejecutables y demás tipo de archivos con posibilidad de estar infectados sin ningún control. Lo que yo aconsejo es analizar siempre un archivo antes de ejecutarlo. También es bueno no descargar si se puede archivos .exe, .bat, etc. Hay que intentar descargar archivos de ISO o imágenes de archivos, analizándolos previamente también.

Los virus se pueden clasificar de muchas maneras, pero quiero hacerlo por tipo de virus y por su procedencia:

- ***Los caballos de Troya:*** Estos infectan a una máquina haciéndose pasar por software no malicioso. Este se encarga de abrir una puerta en nuestra máquina, que permite a un servidor pirata externo descargar un código malicioso. Los caballos de Troya casi nunca contiene software malicioso, y por eso son mas difícil de localizar o de que el antivirus lo detecte. El caballo de Troya solo abre las puertas para que otro ordenador se encargue de infectar nuestro ordenador. Por ejemplo, imaginar un sitio web que para descargar la música necesites instalar un pequeño programa, este programa será el que te abra las puertas al servidor de virus.

- ***Rootkit:*** Este tipo de virus son fragmentos de software malicioso que se pega directamente en el corazón de tu sistema operativo, y una de sus funciones puede ser la de tapar las pruebas para que un caballo de Troya pueda infectar un equipo. Este tipo de virus suelen ser muy perjudiciales ya que al infectar archivos del sistema, la mejor solución suele ser reinstalar el sistema operativo.

- ***Un gusano:*** Este tipo de virus es una forma de programa maligno que tiene la capacidad de propagarse por si mismo. El gusano aprovecha un fallo de seguridad para instalarse en el ordenador y luego escanea la red en busca de otros ordenadores con el mismo fallo de seguridad. Por esta razón, un gusano es capaz de propagarse en cuestión de horas. Por eso, siempre es aconsejable mantener tu equipo actualizado para evitar fallos de seguridad que aprovechan los virus. Hay gusanos de muchos tipos, uno de los más comunes es aquel que hace que la RAM de tu ordenador se consuma hasta que desborda.
- ***Keyloggers:*** La función de un keylogger, como su palabra indica, es recoger todo lo que se teclea. Se encarga de guardar en un archivo todo lo que se teclea por lo que si estás acostumbrado a teclear la clave del banco por teclado. Este tipo de virus puede guardar tu clave y mandársela a alguien que no creo que haga buen uso de ella. Suelen ir incrustados dentro de otros virus y existen métodos de protección ante este tipo de virus. Por ejemplo, el teclado de la pantalla de acceso a bancos.
- ***Hijackers:*** Son pequeños programas o scripts que alteran el funcionamiento de tu navegador y crean molestos cambios como pop-ups emergentes, instalación de barras de herramientas, acceso restringido a webs, etc. Son más molestos que peligrosos, pero pueden ayudar a la propagación de otros virus.
- ***Spyware:*** es un tipo de software malicioso que se encarga de espiar ti actividad dentro del ordenador, suelen estar dentro de otro tipo de software y pueden reportar a una dirección todo tu actividad. Pueden tener muchos usos, desde mala intención de uso de contraseñas y demás, hasta ser la mejor manera de saber ámbitos de utilización de ordenadores, es decir, puede ser distribuido por una empresa para saber que es lo que los usuarios utilizan y demandan sin que se enteren (Es un poco rebuscado pero ocurre).
- ***Spam:*** El spam es cualquier correo no deseado que su única finalidad es la publicidad o la propagación de virus. El spam no es un virus en si, sino que puede ser puente para virus o se puede utilizar para bloquear servidores que al final tiene un fin malo. El Spam utiliza servidores con fallos de seguridad para mandar millones de correos a la red, que pueden contener links a virus o publicidad. El 95 % del correo mundial es Spam, y es uno de los grandes problemas de internet. Muchos virus consiguen infectar ordenadores para que actuen como Zombies, bien sea, en este caso para enviar Spam o para infectar a otros equipos, por lo que resulta muy dificil conseguir saber el origen de la infección.

Otros Tipos de virus:

- ***Virus de Office:***

  El programa de Microsoft ha sido el blanco de muchos virus, unos más molestos que otros. Estos virus se alojan en los archivos con extensiones DOT, DOC y XLS, que corresponden a las plantillas del WORD, los documentos de Word y los de Excel. Generalmente se valen de una Macro (secuencia de comandos automatizada) para llevar a cabo su labor. Se detecta la presencia de estos virus cuando Word le pregunta si desea Abrir el Documento con Macros.

  Generalmente causan que el programa se ponga lento. Entre los virus de Office, se encuentran el RCH, el Ethan,el Buendia, Melissa, etc.

  Generalmente no causaran un daño mayor al equipo o a sus programas, salvo el propio WORD y el EXCEL.

  Solución:
  Los antivirus reconocen estos virus y los eliminan de los archivos infectados.

  Siempre trate de revisar los discos de 3 1/2 que le lleguen, pedrera un minuto pero mantendrá limpio el equipo.

  Sea muy cuidadoso al llevar archivos de Word o Excel de un lugar a otro, y si encuentra un archivo infectado, hágale saber al encargado de la sala de la cual proviene el archivo de la existencia de virus en los equipos.

  Una forma rápida de reparar el Word, es copiar el archivo Normal.dot que se encuentra en la Carpeta C:\Archivos de Programa\Microsoft Office\Plantillas desde un equipo en buen estado, y reemplazarlo en el equipo infectado. Generalmente el Normal.dot infectado es mucho más pesado que el que esta en buen estado. Esto nos servirá para generar archivos sin virus, pero en el caso de abrir un archivo con virus, volveremos a infectar el programa.

- ***Virus de sistema:***

  Estos virus infectan archivos de sistema, con las extensiones EXE, y COM. generalmente tienen otra forma de actuar, ya que necesitan que el archivo se ejecute y es ahí donde el virus se expande e infecta otros archivos.

  Los efectos de estos virus son diversos, desde bloquear el funcionamiento del equipo, hasta el daño fatal de la placa madre del equipo. Muchos de ellos se activan en fechas especificas, conmemorando algún evento(bombas lógicas), como el Chernobil, que se activa a final de Abril, y que ataca el disco duro provocando la perdida total de datos y el borrado de la BIOS(sistema básico del equipo), en el peor de los casos.

  Solución:
  · Evite el instalar programas de fuentes poco confiables, como CD's grabados por desconocidos, CD's de programas piratas, Archivos que le lleguen por IRC (chat) o por e-mail

  · Revise periódicamente su equipo con un antivirus. Dependiendo del uso que se le de al equipo, una revisión cada dos o tres semanas será suficiente.

- ***Troyanos:***

  Los Troyanos o Caballos de Troya, son virus específicos que tienen la función de abrir entradas al equipo.

  La comunicación en internet se hace a través de puertos de comunicación, así el 23 es el puerto de Mail, el 80 el de transmisión de paginas web, etc. Un troyano abre un puerto y generalmente instala un servidor (programa para recibir instrucciones y ejecutar acciones en SU equipo). El modo de operación es el siguiente:

  Por algún método nos llega el troyano (generalmente por mail, Chat o icq), escondido en algún programa simpático o pícaro, lo ejecutamos y se inicia. El troyano se instala, copia su servidor, e instala la aplicación para que se inicie con Windows, y se oculta. La próxima vez que se inicie Windows, el servidor se iniciara. Entonces si alguien que tenga el cliente (programa para aprovechar la puerta abierta) podrá entrar a nuestro equipo y aprovechar las funciones del Servidor.

Entre los troyanos más conocidos están: BackOriffice, el Netbus, etc.

Solución.

· El troyano actúa sólo si estamos conectados a Internet. Por si solo no es operativo, necesita de un cliente (equipo externo que accede a él) que ocupe sus funciones. Entonces, si sospecha de un troyano, desconéctese de Internet, y proceda a buscarlo con un antivirus.

· Mantenga un antivirus al día o alguno especifico como el Cleaner, para sacar el troyano.

· UN caso especial son los Gusanos o worms. Se contagian de la misma forma que los troyanos, y se previenen del mismo modo. Entre ellos están el Navidad, el Emanuel, etc.

- ***Hoaxes, Virus que no lo son:***

Muchas veces nos llegan correos avisándonos de peligrosos virus recién descubiertos, que han causado estragos en otras partes del mundo, pero muchos de ellos no pasan de ser sólo falsas alarmas.

Ellos son los hoaxes. Dentro del mundo informático, existe lo que se llama ingeniería social, que aquí se aplica para causar temor a las personas que reciben esta falsa alarma. No crea demasiado en aquellos mensajes que le avisan de un virus y no le entregan un link directo con información para solucionarlo.

Una vez vistos los tipos más comunes de virus, quiero dar una serie de consejos sobre como proteger tu sistema:

1. Tener un buen antivirus instalado en tu ordenador.
2. Tener también un firewall para evitar intrusiones.
3. Mantener siempre tu sistema antivirus y el sistema operativo siempre actualizado. Esto les pone más dificil las cosas a virus nuevos o a los que aprovechan agujeros o vulnerabilidades del sistema.
4. No abrir o ejecutar links a mails que no te fias, y a los que sí te fias, no ejecutes archivos con extensiones como: .exe, .bat, .com, .vbs, a no ser que sepas que son fiables.
5. Analizar siempre antes cualquier archivo nuevo que entre en tu ordenador. A veces es engorroso, pero es una muy buena costumbre, sobretodo si utilizas redes P2P.

6. No navegar por páginas raras y no fiables, y tener un buen sistema antispyware para detectar ese tipo de software malicioso.
7. Mantener siempre tu navegador actualizado y si puede ser Firefox mejor (Consejo personal).
8. Si utilizas la banca por Internet, es decir, si gestionas tus cuantas desde Internet a través de tu banco, debes tener especial atención al Pishing, con lo que no introduzcas directamente nunca tu usuario y contraseña, hazlo mediante el teclado que se muestra en la página, esto evita que algunos virus puedan conocer tu contraseña, pero no todos. Esto es importante por que pueden hacer mucho daño, no a tu ordenador, sino a tu dinero.
9. No des nunca tus datos bancarios más que en la página de tu banco, y asegurándonos que es la página de siempre, ya que muchos métodos de phising utilizan páginas que parecen las verdaderas para que les introduzcas tus datos, además, tu banco jamas te pedira que confirmes tus datos por mail, con lo que cualquier correo que te llegue de ese tipo, hay que eliminarlo.

LOS ANTIVIRUS

Los **antivirus** son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos *(a veces denominados malware).*

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado.

Actualmente a los antivirus se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

Los virus, gusanos, spyware,... son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen la características de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información.

Una característica adicional es la capacidad que tienen de propagarse. Otras características son el robo de información, la pérdida de esta, la capacidad de suplantación, que hacen que reviertan en pérdidas económicas y de imagen.

Daños y perjuicios

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como pérdida de productividad, baja en el rendimiento del equipo, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir *replicándose* en otras partes del sistema de información. Las redes en la actualidad ayudan a dicha propagación.

Los daños que los virus dan a los sistemas informáticos son:

- Pérdida de información (evaluable según el caso)
- Horas de contención (Técnicos de SI, Horas de paradas productivas, tiempos de contención o reinstalación, cuantificables según el caso+horas de asesoría externa)
- Pérdida de imagen (Valor no cuantificable)

Hay que tener en cuenta que cada virus es una situación nueva, por lo que es difícil cuantificar a priori lo que puede costar una intervención. Tenemos que encontrar métodos de realizar planificación en caso de que se produzcan estas contingencias.

Métodos de contagio

Existen dos grandes grupos de *contaminaciones*, los virus donde el usuario en un momento dado ejecuta o acepta de forma inadvertida la instalación del virus, o los gusanos donde el programa malicioso actúa replicándose a través de las redes.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o no previstos. Dichos comportamientos son los que nos dan la traza del problema y tienen que 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*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software pirata o de baja calidad, que pueda contener junto con el software uno o varios programas maliciosos.

Un antivirus tiene tres principales funciones y componentes:

- **VACUNA** es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en **tiempo real**.
- **DETECTOR**, que es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de **control** y **reconocimiento** exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura.
- **ELIMINADOR** es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas.

Tipos de vacunas

- ***CA:Sólo detección:*** son vacunas que solo detectan archivos infectados sin embargo no pueden eliminarlos o desinfectarlos.

- ***CA:Detección y desinfección:*** son vacunas que detectan archivos infectados y que pueden desinfectarlos.

- ***CA:Detección y aborto de la acción:*** son vacunas que detectan archivos infectados y detienen las acciones que causa el virus.

- ***CA:Detección y eliminación de archivo/objeto:*** son vacunas que detectan archivos infectados y eliminan el archivo u objeto que tenga infección.

- ***CB:Comparación directa:*** son vacunas que comparan directamente los archivos para revisar si alguno esta infectado

- ***CB:Comparación por signatura:*** son vacunas comparan las signaturas de archivos sospechosos para saber si están infectados.

- ***CB:Comparación de signatura de archivo:*** son vacunas que comparan las signaturas de los atributos guardados en tu equipo.

- ***CB:Por métodos heurísticos:*** son vacunas que usan métodos heurísticos para comparar archivos.

- ***CC:Invocado por el usuario:*** son vacunas que se activan instantáneamente con el usuario.

- ***CC:Invocado por la actividad del sistema:*** son vacunas que se activan instantáneamente por la actividad del sistema

FUNCIONAMIENTO DE LOS ANTIVIRUS

Un programa antivirus no es más que un sistema que analiza información de muy diverso tipo y, en caso de que se encuentre infectada, procede a su desinfección.

DIFERENTES ANTIVIRUS:

Norton Antivirus, AVG, Panda Security, NOD32, Bit defender.
FUNCION DE UN FIREWALL: Es un programa que sirve para filtrar lo que entra y sale de un sistema conectado a una red.
FUNCIONAMIENTO DE UN REMOVEDOR DE TROYANOS: Se trata de un software diseñado específicamente para combatir los troyanos, que, a diferencia de los antivirus, suele llevar incluidas herramientas especiales para la lucha contra ellos
FUNCION DE UN ANTISPYWARE: Se encarga de combatir programas que recopilan información de un ordenador y después transmite esa información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador, a ese tipo de programas se los denomina spyware.
La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras

• Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.
• La manipulación de programas: consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.
• Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
• Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Se basa en el principio de que 10,66 es igual a 10,65 pasando 0,01 centavos a la cuenta del ladrón n veces.

2. Manipulación de los datos de entrada

• Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
• Como instrumento: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

3. Daños o modificaciones de programas o datos computarizados

• Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
• Acceso no a autorizado a servicios y sistemas informáticos: estos acceso se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.

• Reproducción no autorizada de programas informáticos de protección legal: esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.
Adicionalmente a estos tipos de delitos reconocidos, el XV Congreso Internacional de Derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información.

Tipos de antivirus

El mundo de internet se ha poblado de virus de cualquier tipo, que pueden afectar de una manera u otra el funcionamiento de nuestro sistema. Por lo tanto se hace indispensable utilizar un programa que detecte los posibles virus y los elimine de la forma más segura posible. Además este programa debe contener herramientas indispensables para, por ejemplo, estar siempre actualizado, mantener un control constante de virus, etc.

A continuación los resultados que ha dado cada programa cuando fueron atacados por virus y además los análisis en general que hemos hechos sobre estos.

McAfee Virus Scan

Este es un software hecho por Network Asóciate y que sin duda posee características detacables en cuanto a su función. Es uno de los más populares antivirus y bastante querido por los profesionales de éste ámbito.

Las últimas versiones han demostrado ser muy profesionales en cuanto a diseño y estructura del programa.

Sus herramientas más detacables son:

El sistema de monitorización en segundo plano es bastante bueno y no relentiza la computadora.

Posee herramientas que monitorizan el correo electrónico de forma segura, incluso tenemos la posibilidad de agregar un botón propio de VirusScan a Outlook o Eudora con el cual podremos activar la revisión.

Posee también un calendario en donde podremos ver cuándo fueron las últimas veces que escaneamos el sistema.

El programa posee una seguridad muy buena, ya que hace copias de los archivos más imporantes del sistema y los almacena de forma segura.

Como todo buen antivirus, posee una herramienta para actualizaciones por Internet. Pero igualmente el número de virus que posee en un base de datos es relativamente bajo.

Norton Antivirus 2000

Este antivirus es un producto de Symantec y es realmente muy conocido. Siempre destacado por su diseño, este posee una de las interfaces mejores del mercado y una distribución de la información muy buena. Esto hace que manejar el programa se haga sencillo y rápido.

El sistema de escaneo de unidades es muy bueno.

Como la mayoría de los antivirus, posee una muy buena actualización a través de Internet.

Posee una herramienta para crear discos de rescate y emergencia realmente muy buena.

El antivirus posee un programa que se instala que es muy buena para la detección de virus a través del e-mail. Este instala un proxy para correo electrónico que descarga los mensajes que nos llegan, verifica la existencia de virus y al terminar podremos leerlos. Detecta todo tipo de virus (comprimidos o no) en los mensajes de correo.

Posee un sistema inteligente de detección de virus. Aunque los virus no se encuentren en su base de datos, al ser ejecutados rápidamente se da cuenta de su accionar extraño y los detecta.

Panda Antivirus Platinum

También es uno de los mejores antivirus del mercado. Posee una base de virus grande comparándola con Norton y McAfee. Por lo tanto en cuanto a detección de virus directamente es prácticamente el mejor.

El monitoreo de programas en segundo plano usa los recursos de nuestro sistema y puede volverlo algo lento.

Tiene la posibilidad de elegir entre dos tipos de interfaces: simple y avanzada. Para tener un mejor control de los virus, preferimos la avanzada.

También posee programas para la detección de virus por correo electrónico, o archivos bajados de Internet (www y ftp). Crea discos de salvación muy buenos también.

En cuanto a la interface, existen opiniones ambiguas. A nuestro parecer, posee un diseño muy profesional y fácil de manejar.

Antiviral Toolkit Pro

Puede detectar los virus en memoria sin arrancar con un disco de emergencia, lo que sus competidores no poseen.

Detecta todo tipo de virus, incluso en archivos comprimidos. A la hora de manejarlo, es muy sencillo y uno se adapta fácilmente a él.

Posee una herramienta de actualización muy buena a través de internet.

También puede introducirse como plugins en los programas de correo electrónico.

Su aplicación de monitorización en segundo plano es muy útil y no relentiza el sistema cuando trabajamos con archivos pequeños.

Un antivirus es una aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en los sistemas informáticos, como las computadoras.

Inicialmente los antivirus se encargaban de eliminar los diferentes tipos de virus, sin mayores complicaciones en el vocabulario. A medida que fueron creándose más y más tipos de virus, cambiando las técnicas de difusión/ataque/ocultación, comenzaron a salir "antivirus especializados" en determinados tipos de virus o en determinados medios de difusión, diversificando el vocabulario.

Actualmente la mejor forma de clasificar a todos los códigos malignos es con el nombre de **malware** o **programas malignos**, término que incluye virus, espías, troyanos, gusanos, dialers, etc.

También la mejor forma de llamar genéricamente a los antivirus, antiespías, antiintrusos, cortafuegos, etc. es: herramientas, aplicaciones o sistemas de seguridad informática.

Por lo tanto, ¿qué tipo de herramientas de seguridad informática existen?: sencillamente, todas las aplicaciones "anti", como ser:

Algunos antivirus populares

* Kaspersky Anti-virus.
* Panda Security.
* Norton antivirus.
* McAfee.
* avast! y avast! Home
* AVG Anti-Virus y AVG Anti-Virus Free.
* BitDefender.
* F-Prot.
* F-Secure.
* NOD32.
* PC-cillin.
* ZoneAlarm AntiVirus.

Otros: ClamXav, Comodo AntiVirus, Norman, PC Tools AntiVirus, Protector Plus, Quick Heal Antivirus, Rising AntiVirus, Sophos Anti-Virus, Windows Live OneCare, BullGuard, Cisco Security Agent.