Términos y conceptos

Estos términos son usados en los documentos de información de SATINFO que edita en la web y en las noticias que se envian por e-mail a los asociados que se han dado de alta (totalmente gratuito) a este servicio.

BASADO EN LA DOCUMENTACION EDITADA EN LA WEB DEL MINISTERIO DE CIENCIA Y TECNOLOGIA, ADAPTADA A LOS VIRUS EXISTENTES EN REVISION DE FECHA FEBRERO 2003

-A-

ACCESO REMOTO: (ACCESO COMPARTIDO)
Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

ACTIVE-X (Controles Active-X):
Los denominados controles Active-X son componentes adicionales que se pueden incorporar a las páginas web, para dotar a éstas de mayores funcionalidades (animaciones, vídeo, navegación tridimensional,...etc). Están escritos en un lenguaje de programación (Visual Basic, C, o C++) que no es el propio de las páginas web (HTML) y podrían estar infectados o realizar operaciones no deseadas.

AGUJERO DE SEGURIDAD:
Fallo de un programa, mediante cuyo aprovechamiento los creadores de virus o hackers consiguen la introducción de los procesos víricos o realizar intrusismo en el sistema.

ALGORITMO DE CIFRADO:
Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños. Ver DES, 3DES, Blowfish Y PGP

ALGORITMO DE CIFRADO BLOWFISH:

Blowfish es un codificador simétrico de bloques. Toma una clave de longitud variable, entre 32 y 448 bits.

ALGORITMO DE CIFRADO DES Y JDES

Algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmo DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

ALGORITMO DE CIFRADO PGP

Sistema comercial de cifrado de seguridad usado mundialmente

ANÁLISIS HEURISTICO:
Se trata de un análisis adicional que solamente algunos programas antivirus pueden realizar, para detectar virus que en ese momento son desconocidos.

ANTIVIRUS:
Son todos aquellos programas que permiten analizar memoria y unidades de disco en busca de virus. Una vez el antivirus ha detectado alguno de ellos, informa al

usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus. Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos.

ARMOURING: (ANTIDEBUGGING)
Mediante esta técnica el virus impide ser examinado. Para conocer más datos sobre cada uno de ellos, éstos son abiertos como ficheros que son, utilizando programas especiales que permiten descubrir cada una de las líneas del código (lenguaje de programación en el que están escritos). En un virus que utilice esta técnica, no se podrá leer el código.

ASCII:
ASCII (American Standard Code for Information Interchange) significa código estándar (americano) para el intercambio informático. Es un convenio adoptado para asignar a cada carácter un valor numérico.

Este código utiliza como unidad el byte, como un byte está compuesto de 8 bits, la cantidad de caracteres representables (número de combinaciones posibles con 8 bits) es de 28=256.

El código ASCII se divide en dos grupos.

·Las primeras 128 combinaciones (números 0-127) corresponden a lo que se llama código ASCIL estándar, aquí se incluyen los caracteres alfabéticos, numéricos, caracteres especiales y códigos de control (0.31).

. Las combinaciones restantes (128-255) corresponden al ASCIH extenso. Incluyen los caracteres de dibujo de recuadros, caracteres sombreados, algunas letras griegas, algunos símbolos científicos y caracteres especiales de diferentes idiomas (por ejemplo la ç del catalán o la ñ del castellano).

ATRIBUTOS:
Los ficheros y directorios tienen asignadas unas determinadas características que se denominan atributos. Estas pueden ser: sólo lectura, modificado, oculto, de sistema.

AUTOCIFRADO:
Es una capacidad de algunos virus para esconderse de posibles programas antivirus. Los programas antivirus se encargan de encontrarlos buscando determinadas cadenas de caracteres (firma del virus), identificativas de cada uno de ellos. Para evitar este mecanismo de búsqueda, algunos virus consiguen codificar o cifrar estas cadenas de texto de forma diferente en cada nueva infección. Esto supone que en la nueva infección, el antivirus no encontrará la cadena que busca para detectar a un virus en concreto, pues éste la habrá modificado. No obstante, existen otros mecanismos alternativos para detectarlos.

-B-

BACKDOOR: (PUERTA TRASERA)
Es una puerta abierta por un proceso específico, generalmente virus, gusano o troyano, mediante el cual se tiene acceso remoto al control de procesos del sistema afectado.

BACKGROUND:
Se dice que una aplicación funciona "en background" cuando está trabajando sin afectar a la actividad del usuario (en segundo plano).

BIOS:
Es la abreviatura de Basic Input / Output System e identifica al software o conjunto de programas que arrancan el ordenador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. El programa del BIOS, se encuentra siempre en la memoria principal, pero no en la RAM (Random Access Memory) pues al apagar el ordenador se borraría, sino en la ROM (Read Only Memory - Memoria de Sólo Lectura), cuyo almacenamiento es permanente, grabado en un chip PROM, EPROM, EEPROM o FLASH EPROM.

BOMBA LOGICA:
Es un prgrama que en función del cumplimiento de unas condiciones, tiene una activación automática (fecha de activación, número de veces de ejecución, etc).

BOOT / MASTER BOOT:
Todos los discos (disquetes y discos duros) tienen una sección muy importante, denominada "sector de arranque". En ella se almacena la información acerca de las características del disco, además de poder albergar un programa con el que es posible arrancar el ordenador, mediante la utilización de ese disco. Cuando se habla del Boot se puede hacer referencia al sector de arranque de un disquete o de un disco duro, mientras que el término Master Boot Record (MBR) hace referencia al sector de arranque maestro o Tabla de Particiín de un disco duro.

BULO (HOAX):
Se trata de una información, generalmente por mensaje de correo electrónico, que avisa de un virus no existente aumentando el temor a los virus e invitando a su difusión, además de recomendar, en algún caso, el borrado de ficheros.

-C-

CADENA:
Es una consecución de carácteres de texto, dígitos numéricos, signos de puntuación o espacios en blanco consecutivos. Alguna de las técnicas empleadas por los antivirus para la detección de virus es buscar determinadas cadenas de códigos, que éstos actualizan habitualmente.

CARA:
Es una parte de un disco de almacenamiento, siendo la agrupación de todos los sectores a los que la cabeza de lectura/escritura puede acceder.

CHAT:
Se trata de conversaciones escritas entre varios ordenadores. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo. Son muy usadas las siglas IRC para referirse a esta técnica (INTERNAL RELAY CHAT). Un programa muy usado para ello es el mIRC.

CHECKSUM: (CheckSummer)
Método o sistema para calcular un valor asociado a determinados archivos que habitualmente no cambian para protegerlos. CheckSummer recalculará periódicamente dicho número y si se detecta que ha cambiado, será un indicio de infección. En ocasiones el Checsum se obtiene a través de combinación de varios métodos diferentes de cálculo.

CIFRADO POLIMORFICO:
Es una de las características que, algunos de los virus existentes, utilizan para que los antivirus no los encuentren. Con ello, el virus se cifra, codifica o "encripta" automáticamente cuando realiza una infección. En cada infección realizará este

cifrado de forma diferente, de tal forma que en cada ocasión sus cadenas o códigos son diferentes. El problema que el antivirus encuentra es que no siempre tiene que buscar los mismos códigos o cadenas de caracteres pues el virus en cada infección los hará diferentes.

CILINDRO:
Es el conjunto de todos los sectores a los que pueden acceder todas las cabezas de lectura/escritura, sin que éstas se desplacen.

CLAVE (del Registro):
El Registro de sistema (Registry) es un elemento en el que se guardan las especificaciones de configuración del ordenador, mediante valores o claves. Estas claves cambiarán de valor, y/o se crearán, cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos o no desados.

CLUSTER:
Con este término se identifica una sección física dentro de un disco de almacenamiento. Agrupa uno o varios sectores del disco que se encuentran consecutivos o adyacentes.

CIFRAR:
Proceso para transformar la información escrita texto legible a texto codificado.

-D-

DESINFECCIÓN:
Es la acción que realizan los programas antivirus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan la información infectada.

DEBUG:
Programa que permite la edición y creación de otros programas escritos en lenguajes como Ensamblador (no lenguajes de alto nivel). También hace posible la investigación del código interno en cualquier fichero.

DIRECTORIO, CARPETA:
Éstos dos términos hacen referencia al mismo concepto. Se trata de divisiones (no físicas) en cualquier tipo de disco donde son almacenados determinados ficheros. Forman parte de una manera de organizar la información del disco, guardando los documentos como si de una carpeta clasificadora se tratase.

DISCO DE ARRANQUE: DISCO DE SISTEMA O DISCO DE INICIO)
Es un disco que contiene archivos de inicio, ocultos y especiales para que funcione el equipo. Normalmente es específico del sistema operativo y de la versión. El usuario medio dispone de varios tipos de discos de arranque, que pueden ser desde un disco de arranque en un disquete normal a un disco de arranque de urgencia o un CD arrancable. Reviste importancia utilizar un disco de arranque cuando se desinfecta un equipo, ya que para poder eliminar algunos virus, debe arrancarse con un sistema libre de virus, para lo cual es idóneo el uso de un disquete de arranque.

Algunos sistema operativos le llaman disco de inicio a un disco de arranque o de sistema que además contenga otros ficheros de interés.

DOS (MS/DOS):
Estas siglas significan Disk Operating System (DOS). Se refieren al sistema operativo (S.O.) anterior a Windows, que en su momento, creó la empresa Microsoft.

-E-

EICAR:
El Instituto Europeo de investigación de antivirus informáticos ha creado una cadena de caracteres en la que todos los antivirus deben detectar un patrón para comprobar su correcta instalación y funcionamiento. No se trata de ningún virus, sino sólo de una cadena de detección inocua.

EN FASE DE PROPAGACIÓN (IN THE WILD):
Este término se refiere a una famosa lista, Wildlist, en la que se reflejan los virus que, en la actualidad o en ese periodo de tiempo, se encuentran en su apogeo. Esto no significa que los virus de esta lista sean los que se activan en esas fechas, sino los más extendidos en ese momento, o los más nombrados. Por decirlo de otra forma, son los virus más populares del momento. Por ese motivo, puede darse el caso de que uno o varios de ellos dejen de estar en la lista por una temporada y al cabo de un tiempo vuelvan a aparecer en ella.

EXCEPCIONES:
Una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso lo que el programa antivirus consigue es realizar la búsqueda concreta de un determinado virus.

EXPLORAR: (SCAN)
Buscar virus bajo demanda o al acceso.

EXPLORACIÓN BAJO DEMANDA:
Programa antivirus que el usuario ejecuta manualmente en busca de virus (Ver además Resident Scanner y Heuristic Scanner).

EXPLORACIÓN HEURÍSTICA:
Método de exploración antivirus que busca virus nuevos y desconocidos.

EXPLORADOR RESIDENTE:
Programa antivirus que busca virus al acceso en segundo plano (background), protegiendo al sistema de forma simultánea con el uso del PC

-F-

FALSA ALARMA: (FALSO POSITIVO)
Los análisis heurísticos, que se utilizan para detectar virus nuevos, previamente no descubiertos, pueden detectar virus donde no los hay. No es frecuente su uso, pero hay que recordar su existencia y obrar en consecuencia según las circunstancias.

FAT:
También denominada Tabla de Asignación de Ficheros (File Allocation Table), representa una sección del disco en la cual se almacenan las direcciones donde se encuentran los ficheros contenidos o guardados en dicho disco. Estas tablas (se crean normalmente dos iguales en cada disquete o partición de disco duro en FAT12/16/32, para evitar posibles pérdidas de datos si fallara una de ellas) se

encuentran localizada tras el Boot o sector de arranque de los disquetes o particiones de discos duros.

FICHERO, ARCHIVO, DOCUMENTO:
Estos tres términos tienen el mismo significado y hacen referencia a la información que se encuentra en un soporte de almacenamiento informático. Es el trabajo real que realiza cada usuario (textos, imágenes, bases de datos, hojas de cálculo,...,etc.). Cada uno de ellos se caracteriza por tener un nombre identificativo. El nombre puede estar seguido de un punto y una extensión, generalmente compuesta por tres carácteres que identifican el tipo de fichero del que se trata. Algunas extensiones comunes son: EXE y COM (ficheros ejecutables, programas), TXT y DOC (ficheros de texto). Actualmente, en Windows 32 bits, pueden tener 4 letras, como por ejemplo HTML, así como en cualquier sistema también 0, 1 y 2 letras, cabiendo el uso de "dobles extensiones", truco utilizado por algunos virus que presentan el nombre seguido por dos "extensiones

FICHEROS DE PROCESO POR LOTES (.BAT o BATCH):
Los ficheros de proceso por lotes o ficheros Batch se caracterizan por tener extensión BAT. Son ficheros de texto que contienen comandos de MS/DOS, uno por cada línea escrita. Cuando se ejecuta este tipo de ficheros, cada una de las líneas en él escritas se van ejecutando de forma secuencial. Un fichero muy importante de este tipo es el AUTOEXEC.BAT, el cual se encuentra en los sistema operativos clásicos MS-DOS, WINDOWS95, 98, Me. etc, en la raíz del disco duro y se ejecuta automáticamente cuando el ordenador arranca, cargando una serie de controladores y programas.

FICHEROS INI:
Archivos en los que los programas almacenan instrucciones o configuraciones que se utilizan durante su funcionamiento. Los creadores de virus a menudo utilizan los archivos WIN.INI, SYSTEM.INI y WININIT.INI.

FICHEROS SCR:
Son los denominados ficheros de Script. Su extensión es SCR y sirven para determinar los parámetros ("condiciones") con los que se deben ejecutar unos determinados programas. Permiten iniciar un programa con unas pautas fijadas de antemano. También los virus los pueden utilizar para contener ficheros ejecutables tipo EXE, como por ejemplo una de las variantes del W32/Opaserv, que se esconde en el fichero MARCO!.SCR

FICHEROS ZIP, RAR Y AUTOEXTRAIBLES:
Archivo ZIP y RAR son archivos que se han empaquetado y comprimido en uno solo, y a los que, en función de la utilidad empleada, se les ha dado la extensión del nombre de la utilidad. Estos archivos pueden contener ficheros infectados, por lo que se debe configurar el antivirus para que analice los archivos comprimidos en busca de virus.

· Archivos autoextraibles son archivos empaquetados que, al ejecutarse, se desempaquetan. La mayoría de los archivos transferidos a través de Internet están comprimidos para ahorrar espacio en disco y reducir el tiempo de transferencia. El programa de autoextracción puede extraer virus o Caballos de Troya. Estos tipos de virus pueden ser eficaces ya que el análisis de archivos comprimidos es una técnica más bien nueva que utilizan la mayoría de los principales paquetes de programas antivirus. El contagio de un virus no se produce con sólo descargar un archivo autoextraible, hay que ejecutarlo. Analice siempre los archivos nuevos antes de utilizarlos.

-G-

GUSANO:
Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos y generalmente no infectan ficheros..

-H-

HEXADECINAL:
Hex- es un prefijo que quiere decir 6 y -decimal es un sufijo que significa 10, por tanto representa números de base 16. Puesto que hay más de 10 dígitos, los valores del 10 al 15 se representan con las letras A a F, respectivamente. Esta representación se utiliza en programación informática.

HOAX (BULO):
Se trata de un mensaje de correo electrónico que avisa de un virus NO existente aumentando el temor a los virus e invitando a su difusión. Algunas veces estos bulos pueden recomendar el borrado de ficheros. No hacer nigún caso, y en caso de duda preguntar al técnico en virus si realmente es un bulo o no.

-I-

INFECCIÓN:
Es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro ordenador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

INTERRUPCION:
Es una señal mediante la cual se consigue hacer una pausa momentánea en las labores que se encuentra ejecutando la C.P.U. del ordenador (CENTRAL PROCESS UNIT = microprocesador). Cuando ésta tiene lugar, la CPU abandona las operaciones que estaba realizando y pasa a ejecutar las acciones u operaciones que requiere el tipo de interrupción requerida. Respecto a cada una de ellas, existe un nivel de jerarquías para aceptar unas antes que otras o para que unas permitan interrumpir a las otras. Cuando se han realizado las acciones correspondientes a la interrupción aceptada, la CPU sigue con la tarea que abandonó en su momento.

IRC:
Mediante el IRC se pueden mantener conversaciones escritas, en tiempo real, entre varios usuarios conectados a un canal de comunicaciones disponible en Internet

-J-

JAVA:
Se trata de un popular lenguaje de programación muy utilizado en Internet.

-M-

MACRO / VIRUS DE MACRO:
Una macro es una secuencia de operaciones o instrucciones que definimos en un programa (por ejemplo, Word, Excel, o Access) paraque se realicen de forma automática y secuencial. Estos son "microprogramas" que pueden ser infectados por los virus. Los documentos de Word, las bases de datos o las hojas de cálculo etc., no son programas y por ello no deberían ser infectados por ningún virus. No

obstante, en cada uno de los ficheros creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas.

MALWARE:
Son programas que se diseñan intencionadamente para llevar a cabo acciones no autorizadas, y a menudo perjudiciales o indeseables, como virus, gusanos y troyanos.

MULTIPARTITE:
Es una propiedad que caracteriza a determinados virus avanzados. Estos podrán realizar infecciones utilizando combinaciones de técnicas que otros tipos de virus utilizan en exclusiva. Pueden ser capaces de infectar al mismo tiempo documentos , ficheros ejecutables EXE o COM y sectores de arranque en disquetes y/o discos duros.

-O-

OCULTAMIENTO u OCULTACION (STEALTH):
Los virus que utilizan esta técnica intentan pasar desapercibidos ante los ojos del usuario, no levantando ninguna sospecha sobre la infección que ya ha tenido lugar. Los virus residentes son los que más la utilizan, aunque no es exclusivamente este tipo de virus quienes la aplican.

-P-

PAYLOAD:
Son acciones que tiene programado ocasionar el virus al sistema infectado en función de contadores, tiempo, etc.

PISTA:
Es una sección concéntrica inapreciable al ojo humano, que se encuentra en cualquier tipo de disco o soporte de grabación. Permite almacenar la información organizada en pistas o tracks, dentro del disco. Es el grupo de sectores a los que se puede acceder en una operación del lectura, sin desplazar la cabeza lectora del disco a otra posición.

PLANTILLA (PLANTILLA GLOBAL):
Es un determinado fichero que una aplicación concreta utiliza para iniciar su sesión de trabajo con unos valores o parámetros establecidos por defecto. Por ejemplo, el procesador de textos Microsoft Word (que forma parte de Microsoft Office) tiene asociada una plantilla cuyo fichero se denomina NORMAL.DOT.

POLIMORFICO / POLIMORFISMO:
Basándose en la técnica de autocifrado, el virus se codifica o cifra de manera diferente en cada infección que realiza (su firma variará de una infección a otra). Si sólo fuese así estaríamos hablando de un virus que utiliza el cifrado, pero adicionalmente el virus codificará también el modo (rutina o algoritmo) mediante el cual realiza el cifrado de su firma. Todo esto hace posible que el virus cree ejemplares de sí mismo, diferentes de una infección a la siguiente, cambiando de "forma" en cada una de ellas. Para su detección, los programas antivirus emplean técnica de simulación de descifrado.

PUERTA TRASERA: (BACKDOOR)
Es el camino abierto por un proceso específico, generalmente virus, gusano o troyano, mediante el cual se tiene acceso remoto al sistema afectado.

PROGRAMAS (FICHEROS .EXE y .COM):
Los ficheros, documentos o archivos se componen de un nombre (cuyo número de caracteres antiguamente se limitaba a 8) y una extensión (que puede no existir). Esta extensión especifica el tipo de fichero. Si es EXE o COM, el fichero será un programa ejecutable. De esta forma si hacemos doble clic sobre él o escribimos su nombre, se realizarán determinadas acciones.

-R-

REDIRECCIONAR:
Esta acción permite aplicar un nuevo destino. En el caso de los virus, se puede hablar de éste término cuando un virus es capaz (por ejemplo) de hacer que el sistema en lugar de acceder a una dirección en la que debería encontrar determinados componentes, es obligado por el virus a saltar o acceder a otra dirección diferente.

REFERENCIAS, ENLACES, SALTOS, LINKS:
Cada uno de estos cuatro conceptos se puede definir también como un hyperenlace. Con ello nos referimos a determinados elementos (texto, imágenes, botones) y/o secciones de un documento HTML (una página Web), que pinchando en ellos con el puntero del ratón, el usuario se conectará (saltará o accederá) a otra página diferente o a una sección de la misma página en la que ya se encontraba.

REGISTRO DE WINDOWS (REGISTRY):
También denominado Registro de Sistema es un fichero en el cual se almacenan todos los valores de configuración e instalación de los programas que se encuentran instalados en el sistema operativo. Esta configuración se rige por claves, subclaves, valores y datos que se pueden consultar y modificar, y que la mayoría de programas lo modifican de forma automática al instalarse.

RENOMBRAR:
Es la acción por la cual un usuario, una aplicación o un programa (en nuestro caso, serán los programas antivirus) eliminan el nombre antiguo de un fichero, asignándole otro a éste.

REPLICA :
Se define como réplica la acción por la cual los virus se propagan o hacen copias de sí mismos, con el único objetivo de realizar posteriores infecciones.

RESIDENTE / VIRUS RESIDENTE (TSR):
Un virus que posea esta propiedad, será del tipo denominado "virus residente". Su característica es la de colocarse en secciones concretas de la memoria para, desde allí, atacar o infectar a todos los programas (ficheros EXE o COM) que se ejecuten. El virus se instala en la memoria del ordenador y desde ella está continuamente comprobando si se ejecuta algún programa. Cuando esto ocurre, infecta el programa ejecutado. (TSR: TERMINATE and STAY RESIDENT)

-S-

SECTOR:
Es un término que define una sección de un disco. Para verlo más claro podríamos decir que un sector es una "porción de tarta" ficticia que define una determinada zona del disco. De esta forma la estructura del mismo se encuentra dividida y permite el mejor almacenamiento y organización de la información. Se trata de la unidad mínima de información a la que se puede acceder en una operación de lectura/escritura, la cual tiene un tamaño de 512 Bytes.

SECTOR DE ARRANQUE:
Todo disco duro o disquete tiene un sector de arranque que el PC lee cuando se enciende. Este sector contiene todos los códigos necesarios para cargar los archivos de sistema DOS.

SECTOR DE PARTICIÓN:
Todo disco duro tiene un sector de partición que es leído después del arranque de la BIOS del PC. Contiene datos sobre el disco tales como el número de sectores, cilindros y cabezales de cada parte partición y la ubicación de las particiones.

SISTEMA DE CIFRADO:
Colección completa de algoritmos que tienen su propia denominación en Función de las claves que utilizan para encriptar. (Ver Blowfish, DES y PGP).

SISTEMA OPERATIVO (S.O.) (O.S. = OPERATING SYSTEM):
Existen dos términos muy utilizados en informática. Estos son los conceptos de hardware y software. El primero de ellos se refiere a todo lo que es físico y tangible en el ordenador, como unidades de disco, tarjetas gráficas, microprocesador, memoria,...etc. Por otro lado está el software que se define como el conjunto de programas (o información) con la que puede trabajar el hardware (ficheros, directorios, programas ejecutables, bases de datos, controladores,...etc.). Pues bien, el sistema operativo pertenece al software y más concretamente es el conjunto de programas (y ficheros o archivos de otro tipo) que permite que se pueda utilizar el hardware. Se puede tener el mejor ordenador del mundo (el mejor hardware), pero si éste no tiene instalado un sistema operativo, no funcionará .Algunos ejemplos de sistemas operativos son: MS/DOS, UNIX, OS/2, Windows 95/98/Me/NT/2000/XP, Linux, etc.

SOBREESCRITURA:
Los virus de sobreescritura se caracterizan por no respetar la información contenida en los ficheros que infecta, haciendo que estos queden inservibles posteriormente. Pueden encontrarse virus de sobreescritura que además son residentes y otros que no lo son. Aunque la desinfección es posible, no existe posibilidad de recuperar los ficheros infectados, siendo la única alternativa posible la eliminación de éstos.

TUNNELING:
Se trata de una técnica especialmente diseñada para imposibilitar la protección antivirus en cualquier momento. Mientras el análisis permanente, o residente, del programa antivirus que se encuentre instalado, intenta realizar detecciones, el virus actúa en su contra. Todas las operaciones que se realizan sobre cualquiera de los archivos son inspeccionadas por el antivirus mediante la interceptación de las acciones que el sistema operativo lleva a cabo para hacerlas posible. De la misma manera, el virus interceptará estas peticiones o servicios del sistema operativo, obteniendo las direcciones de memoria en las que se encuentran. Así el antivirus no detectará la presencia del virus. No obstante, existen técnicas antivirus alternativas que permiten la detección de virus que realicen este tipo de operaciones.

-T-

TEXTO CODIFICADO:
Se dice que un texto está escrito en ciphertext cuando es necesario decodificarlo para poder leerlo.

TEXTO SIMPLE:
Se dice que un texto está escrito en plaintext cuando puede ser leído sin tener que realizar ninguna operación, es decir, no está codificado.

TROYANO:
Son programas que llegan a un ordenador de forma aparentemente normal y no producen necesariamente efectos visibles o apreciables (por lo menos en ese momento), pero llevan una activación propia. Al activarse puede causar efectos en nuestro sistema, a través de los cuales se pueden producir acciones peligrosas.

-V-

VACUNACION:
Mediante esta técnica el programa antivirus almacena información sobre cada uno de los ficheros. En caso de haberse detectado algún cambio entre la información guardada y la información actual del fichero, el antivirus avisa de lo ocurrido. Existen dos tipos de vacunaciones: Interna (la información se guarda dentro del propio fichero, de tal forma que al ejecutarse él mismo comprueba si ha sufrido algún cambio) y Externa (la información que guarda en un fichero especial y desde él se contrasta la información).

VARIANTE DE UN VIRUS:
Se conoce como variante de un virus ya existente a otro virus básicamente igual al primero pero con algún pequeño cambio en su programación o efecto.

VBS: (VISUAL BASIC)
Lenguaje de programación de alto nivel muy empleado por los creadores de virus. Incluso hay programas en Internet que permiten crear virus de Visual Basic Script a la carta, pudiendo utilizarlos personas sin conocimientos informáticos.

VIRUS:
Programa que está diseñado con la capacidad de replicarse añadiéndose sin conocimiento del usuario a otros programasy con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

VIRUS DE ARCHIVO:
Virus que infecta los archivos ejecutables de los programas. Al abrir un programa infectado, primero se ejecuta el virus y luego se abre la aplicación. Cuando se ejecuta el virus se copia a sí mismo en otros archivos o en otro disco.

VIRUS DE COMPAÑÍA:
Virus que crea un archivo para esconderse cuyo nombre es igual al del original, cambiando la extensión del original por otra, a veces inoperativa, como en el caso del KLEZ.H.

En ocasiones juegan con las extensiones EXE y COM, siendo ejecutados bajo MS-DOS primero los archivos con la extensión .COM, antes que los de extensión .EXE.

VIRUS DE MACRO:
Virus que infecta las macros de Word y Excel, principalmente, de modo que cuando se abre un archivo que tenga una macro infectada, infectará el sistema.

VIRUS DE SECTOR DE ARRANQUE Y DE PARTICIÓN:
Los virus de esta categoría infectan el sector de arranque y sector de partición. La mayoría de los PCs están configurados para intentar arrancar de la unidad a: antes que del disco duro, por lo que si se ha introducido un disquete con el BOOT infectado en la disquetera en el momento de arrancar, el PC se infectará.

VIRUS DE SOBRE-ESCRITURA:
Virus que sobrescriben cada archivo que infectan: el programa maligno copia su propio código sobre el archivo de modo que los programas dejan de funcionar.

VIRUS GUSANO:
Los virus que se propagan generando uno o varios ficheros sin infectar los ya existentes en los ordenadores.

VIRUS MULTIPARTITON:
Virus que utiliza una combinación de técnicas para expandirse infectando archivos ejecutables, sector boot y partición.

VIRUS TROYANO:
Cuando un virus entra en un ordenador y su misión es causar efectos tras llegar a una determinada fecha o coincidir con datos preprogramados, se le denomina troyano, en referencia al histórico caballo de Troya