

VIRUS: INTRODUCCIÓN

Uno de los cambios más sorprendentes del mundo, hoy en día, es la rapidez de las comunicaciones ya que se permite el intercambio de información independientemente del lugar físico en que nos encontremos. Ya no nos sorprende la transferencia de información en tiempo real o instantáneo.

Se dice que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizan el comercio en forma electrónica, para ser más eficientes. Pero al unirse en forma pública, se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

Cada vez es más frecuente encontrar noticias referentes a que redes de importantes organizaciones han sido violadas por criminales informáticos desconocidos. A diario se reciben informaciones de ataques a redes informáticas: los archivos son alterados, los computadores se vuelven inoperantes, se ha copiado información confidencial sin autorización, etcétera.

Los administradores de sistemas deben gastar horas y, a veces, días enteros volviendo a cargar o reconfigurando sistemas comprometidos, con el objeto de recuperar la confianza en la integridad del sistema. No hay manera de saber los motivos que tuvo el intruso. Aquella gente que irrumpe en los sistemas sin autorización, aunque sea solamente para mirar su estructura o hacer una pequeña broma, causan mucho daño.

HISTORIA DE LOS VIRUS

A) ANTES DE INTERNET:

Los virus, en sus comienzos, se originaron partiendo de una investigación científica relativa a los conceptos de inteligencia artificial y vida artificial, y hasta el momento en que mentes maliciosas decidieron hacer uso de la idea para causar daños en sistemas informáticos, no eran más que meros experimentos universitarios. En 1950 Jonh Von Neumam desarrolló, por primera vez, el concepto de programas autorreplicantes que son programas que hacen que programas y datos se almacenen conjuntamente en la memoria y que posibilitaba que ese código fuera alterado.

En 1960, en los laboratorios de Bell, se desarrolla un juego llamado Core Wars (Guerras del Núcleo), en el que dos programas luchaban entre sí por un espacio de memoria común y cuyo vencedor era el que conseguía más memoria. Los programas debían sobrevivir utilizando técnicas de ataque, ocultamiento y reproducción similares a las de los actuales virus informáticos.

En los años 70 se elaboran los primeros programas que se autorreproducían. Aparecieron los primeros gusanos, que, en un principio, no tenían un carácter destructivo sino experimental. La función de los gusanos era generar múltiples copias de ellos mismos a lo largo de una red de computadoras.

En los años 80 aparecen los primeros virus experimentales y la primera definición de virus informático. En 1985 surgen los virus para MS-DOS y se propagaban por los disquetes. En 1986 aparece el primer virus dañino (Brain) que nació en Pakistán. En 1987 aparecieron los primeros virus que fueron ampliamente difundidos (Charlie, Lehigh y Viernes 13). En 1988 se produjo el primer ataque de un gusano a una red que entonces era ARPAnet, precursora de Internet; este gusano se difundía a través de correo electrónico y la erradicación del mismo costó 1 millón de dólares. Ese mismo año aparecieron ya los pri-

meros programas antivirus. Un año más tarde aparecen virus con nuevas técnicas de ocultamiento y los programas antivirus desarrollan nuevas técnicas, como la heurística.

B) DESPUÉS DE INTERNET:

Los gusanos de Internet o "i-worms" han sido, una vez más, los protagonistas en este año que acaba. Si bien estos últimos meses hemos vivido una evolución tanto en el enfoque como en las técnicas utilizadas por estos especímenes que sin duda marcarán el futuro más inmediato en este terreno.

Dejando a un lado el gusano de Morris, que data de 1988, el comienzo de la nueva era de gusanos para Windows e Internet suele situarse en los primeros meses de 1999. En enero de ese año surgía Happy99, un gusano que nos felicitaba con fuegos artificiales la llegada del nuevo año mientras aprovechaba para distribuirse adjunto en mensajes de correo electrónico. Dos meses más tarde, en marzo de 1999, aparecería Melissa que, además de provocar una infección masiva en pocos días, sería el precursor de una nueva ola de gusanos.

Mientras que Happy99 era un binario cuyas interioridades y diseño sólo las apreciaría un programador experto, Melissa nos descubría como cualquier usuario, con unos conocimientos básicos de lenguaje de macros o script, podía crear o plagiar en pocas líneas un gusano que se distribuyera a los contactos de la libreta de direcciones de Outlook del sistema infectado. Comenzaba una revolución. En Hispasec nos adelantamos a Happy99 y Melissa con la noticia "Una nueva generación de virus informáticos ha llegado" publicada el 14 de diciembre de 1998, título bajo el cual se describía un complejo virus que se distribuía adjunto a través del correo electrónico. Win32.Parvo estaba escrito íntegramente en ensamblador por GriYo, del conocido grupo español 29A, destacados por la sofisticación y constante innovación en sus creaciones. La noticia terminaba con la frase: "Este virus es el pionero en este tipo de transmisión, pero sospechamos que no es más que el comienzo de lo que será una larga lista de virus de nueva generación."

Para los más puristas hay que puntualizar que meses antes habían aparecido ya algunos especímenes que utilizaban el correo electrónico para distribuirse, como el virus de macro para Word "ShareFun", que ya en 1997 se distribuía a través de Microsoft Mail, "Red-Team" que infectaba ejecutables de Windows y utilizaba el cliente Eudora para adjuntarse a los e-mails, o el virus de macro "Antimarc" para Word97 que se distribuía a través del mIRC y el Outlook Express.

Las novedades del presente año vienen por parte de la nueva corriente de gusanos que logran infectar sistemas de forma automática, sin necesidad de que el usuario abra o ejecute un archivo, para ello emplea principalmente vulnerabilidades del cliente de correo. Por otro lado, la incorporación de estas técnicas de hacking al mundillo de los virus ha provocado la aparición de especímenes que explotan agujeros de seguridad en los servidores, una vez infectados son utilizados como plataformas de distribución masiva aprovechando su mayor disponibilidad y ancho de banda.

Sin embargo, aun hoy día, no podemos olvidar la generación "Melissa", gusanos muy simples que logran infectar a los clientes gracias a su mejor arma, la ingeniería social (engañar al usuario). Desde el ya mítico y romántico "ILoveYou", a sucedáneos con reclamos más visuales como el "AnnaKournikova" que nos invadió a principios de año, pasando por los típicos gusanos que se hacen pasar por felicitaciones navideñas.

En el 2001, dentro de los gusanos que tienen en la ingeniería social su mejor arma, destaca en el primer puesto "SirCam", al que le bastó con incorporar frases tipo "hola como estas? Te mando este archivo para que me des tu punto de vista", para que muchos usuarios abrieran el gusano y se infectaran. "SirCam" también incorpora la doble extensión en el nombre de archivo, característica común entre los gusanos para intentar ocul-

tar su verdadera extensión y hacerse pasar por formatos inofensivos como gráficos o simple texto.

También merecen mención especial gusanos que, aunque se distribuyen e infectan de forma similar a los anteriores, son mucho más sofisticados y complejos en su diseño e incorporan importantes innovaciones. Ya en 1999 hizo aparición "Babylonia", programado por Vecna del grupo 29A, capaz de autoactualizarse por Internet por medio de "plug-ins". Del mismo autor surgiría a finales del 2000 "Hybris", un gusano al que los usuarios apodaron como el del "enanito" o "Blancanieves" por hacer referencia al cuento del mismo nombre, que ha conseguido mantener un alto número de infecciones durante todo el presente año. Entre las características más sofisticadas de "Hybris" destaca la autoactualización con "plug-ins" cifrados con algoritmo RSA y una llave de 128 bits que recoge de los grupos de noticias de Internet.

Otro gusano que ha hecho furor en el 2001 ha sido "Magistr", que además de incorporar payloads (efectos) muy dañinos, destaca por su capacidad de construir tanto el asunto como el cuerpo del mensaje donde viaja de forma arbitraria recogiendo frases y párrafos entre los documentos que encuentra en los sistemas infectados. Esta característica, además de impedir reconocer la llegada del gusano por los signos más evidentes como puede ser un texto fijo en el asunto del mensaje, provoca un importante efecto de ingeniería social, ya que las frases o párrafos que se incluyen en el e-mail suelen tener en muchas ocasiones relación con la actividad del remitente.

Pero sin duda la novedad de este año ha sido la proliferación de gusanos que aprovechan vulnerabilidades en los sistemas para lograr infectarlos de forma automática, sin necesidad de que el usuario abra o ejecute el archivo que porta el código vírico. No obstante, no debemos olvidar que el primer espécimen que incorporó esta funcionalidad fue "BubbleBoy", un gusano escrito en VBS (Visual Basic Script) por Zulu, capaz de activarse de forma automática con tan sólo leer el mensaje donde se adjuntaba gracias a una vulnerabilidad del cliente de correo Outlook. La noticia en la que se analizaba a "BubbleBoy", el 5 de noviembre de 1999, terminaba con la frase: "BubbleBoy supone el germen de lo que desde Hispasec vaticinamos como una auténtica avalancha de "strains" y demás mutaciones o variantes de este i-worm, que ha marcado un pasado y un futuro, un ayer y un mañana, en el terreno de la virología informática."

Uno de los últimos exponentes de esta corriente se ha hecho notar apenas unas semanas, nos referimos a "BadTrans.B", un gusano que explota una vulnerabilidad conocida de Internet Explorer a través de la cual es posible forzar la ejecución automática de un binario adjunto en un mensaje de correo (.EML). Para lograrlo modifica la cabecera MIME que hace referencia al archivo de forma que simula ser un formato confiable. Esto provoca que Internet Explorer lo abra sin preguntar al usuario. Esta vulnerabilidad es heredada por los clientes de correo Outlook y Outlook Express, ya que utilizan el componente de Internet Explorer para visualizar los mensajes HTML. Otro grupo destacado de gusanos en este año que se acaba son aquellos que explotan vulnerabilidades en los servidores de Internet para lograr infectarlos de forma automática y aprovecharlos como pasarela para buscar nuevos sistemas víctimas. Aunque el mundo Linux se vio afectado por gusanos como "Ramen", la palma en este terreno se la ha llevado el servidor Internet Information Server de Microsoft, cuyas vulnerabilidades ha provocado un gran número de infecciones por parte de gusanos como "Code Red". El más sofisticado en este terreno ha sido "Nimda", que aprovecha vulnerabilidades tanto en clientes (IE) como en servidores (IIS), a la postre el gusano que más quebraderos de cabeza ha provocado. "Nimda" puede atacar a los usuarios de Windows por tres vías diferentes: por correo electrónico, al visitar una página Web o al estar en una red local compartiendo recursos con otro ordenador infectado. Además, tiene una cuarta vía de infección que afecta a los servidores Windows basados en Internet Information Server.

DEFINICION DE VIRUS

Encontrar una definición de virus informáticos es una tarea un poco complicada. En general podemos decir que un virus informático es un pequeño programa diseñado para alterar el funcionamiento de un computador.

Un concepto más completo de virus informático sería el de que es un pequeño programa capaz de autoreproducirse. Está diseñado para dañar sistemas informáticos, alterando su forma de trabajar o dañando información almacenada en el disco duro, sin el conocimiento o permiso del afectado. En términos más técnicos, un virus se define como una porción de código de programación cuyo objetivo es implementarse a si mismo en un archivo ejecutable y multiplicarse sistemáticamente de un archivo a otro. Además los virus están diseñados para realizar una acción concreta en los sistemas informáticos. Esta acción puede ir desde la simple aparición de un mensaje en la pantalla, hasta la destrucción de toda la información contenida en el sistema.

La combinación de código potencialmente dañino, con la habilidad de reproducirse y evolucionar es lo que hace peligroso a los virus para los computadores. Cuando un virus se instala en una máquina, puede ejecutar cualquier instrucción que su autor haya programado, la cual puede iniciarse en una fecha determinada, después de utilizar el programa infectado un número de veces o al azar.

CICLO DE VIDA

Los virus informáticos, de igual modo que los biológicos, tienen un ciclo de vida. En primer lugar hay una creación que se produce cuando una persona con conocimientos de programación, trabaja en su gestación por varias semanas y termina creando un nuevo virus que se encuentra programado para reproducirse rápidamente y hacer daño en algún momento determinado especificado por el programador.

La gestación es con el propósito de futuras reproducciones. Usualmente esto se hace infectando un programa y luego distribuyéndolo por la Red. Al hilo de esto está la reproducción, es decir, su replicación por un largo tiempo antes de que sea activado.

Los virus poseen rutinas de destrucción de datos que se activarán cuando ciertas condiciones sean dadas. Algunos virus se activan en una fecha determinada.

La fase de descubrimiento no se tiene porque producir después de la activación, pero usualmente sucede así. Esto se produce cuando alguien da la noticia de un nuevo virus. Generalmente pasa a manos de la National Computer Security Association (NCSA) que se documenta y luego se distribuye a los diseñadores de antivirus.

Después del descubrimiento, los diseñadores de software modifican sus productos para incluir la detección del nuevo virus. Si los suficientes diseñadores de antivirus son capaces de detectarlo y limpiarlo, así como los suficientes usuarios adquieren antivirus apropiado para combatirlo, el virus puede estar cerca de ser extinguido. A pesar de que ningún virus ha desaparecido por completo, algunos han cesado por largo tiempo de aparecer en la comunidad informática.

TIPOS DE VIRUS

En materia de clasificación no hay una unanimidad de la misma. Se ha optado por la presente por ser la mas comprensible y menos técnica. La clasificación está realizada en función de cómo actúan los virus informáticos.

A) VIRUS DE MACROS:

Una macro es un conjunto de instrucciones para ser llevadas a cabo por un programa de computadora. Estas instrucciones se emplean típicamente para hacer tareas. Un virus de macro es una macro, el cual se enmascara como un legítimo archivo, generalmente de Microsoft Word. Este virus utiliza la macro para replicarse y realizar algún tipo de daño. La lista de instrucciones que contiene este virus de macro puede copiar y borrar archivos, realizar modificaciones a los archivos, insertar otros virus y ejecutar programas incluyendo el virus que ha insertado. Los virus de macro no son directamente ejecutables, sino que deben ser leídos, interpretados y ejecutados. Hoy en día los virus de macro son los más peligrosos y extendidos, y gracias a Internet han cobrado mayor relevancia si cabe. Actualmente, un 64% de los desastres informáticos están causados por virus de macro, lo que les convierte en la mayor amenaza contra la seguridad informática del mundo.

B) CABALLOS DE TROYA:

Son aquellos que se introducen en el sistema bajo una apariencia totalmente diferente a la de su objeto final, esto es, que se presentan como información perdida sin ningún sentido. Al cabo del tiempo, esperando a la indicación programada, se activan, comienzan a ejecutarse y a mostrar sus verdaderas intenciones. En general, estos virus son destructores de la información contenida en los discos.

C) GUSANOS:

Son programas que constantemente viajan a través de un sistema informático interconectado sin dañar necesariamente el hardware o el software de los sistemas que visitan. La función principal es viajar en secreto a través de equipos anfitriones recopilando cierto tipo de información programada para enviarla a un equipo determinado al cual el creador del virus tiene acceso.

Fotografía de la actividad de gusanos en la red

Se publica un interesante artículo sobre la actividad de los gusanos recientes en Internet. Sus autores son Dug Song, Rob Malar y Robert Stone y, durante dos meses han monitorizado los intentos de propagación de los gusanos en auge: tres variantes de redCode y dos variantes de Nimda. Los resultados son impresionantes.

Habiendo analizado las conexiones en una red que se corresponde con el 1/256 del espacio de direcciones de Internet, se observan más de 2.500 millones de intentos de conexión, con picos de 2000 intentos por segundo. Extrapolando esos datos a todo Internet se detectan unas 6.4 billones (un billón es un millón de millones) de intentos de conexión, con un tráfico mínimo -en el mejor de los casos- de 60 terabytes. Aún sin contar la contaminación en sí de otras máquinas, que genera un tráfico extra importante, el simple escaneo de direcciones IP a la caza de servidores web (que pueden ser vulnerables o no), consume una cantidad de recursos impresionante. Algunos de los resultados que extrapolo personalmente de este trabajo son:

- Una máquina anónima conectada a Internet experimentará un escaneo por parte de alguno de esos gusanos cada hora, aproximadamente.
- El no tener una IP oficial o publicada en un DNS no ofrece ninguna protección, ya que estos escaneos se realizan de forma aleatoria sobre el espacio de direcciones IP.
- Por lo tanto, una máquina que no esté protegida y bien configurada *NO* debe conectarse a Internet hasta que se asegure convenientemente.
- En una red con 256 direcciones públicas (una clase C estándar), se recibe un escaneo cada 14 segundos.

Aunque los resultados mostrados en el artículo son inconsistentes en algunos aspectos, las conclusiones generales que se pueden obtener de él son muy interesantes y merecen un instante de reflexión.

DAÑOS OCASIONADOS POR LOS VIRUS

Los virus informáticos no afectan en general directamente al hardware de la computadora sino a través de los programas que lo controlan; en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco duro, tiempo de procesamiento, memoria. En general los daños que pueden causar los virus se refieren a hacer que el PC se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desordenar datos en el disco duro, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Para realizar la clasificación que vamos a enumerar se ha tenido en cuenta que el daño es una acción de la computadora no deseada por el usuario y que está provocada por un virus y, además esta enumeración está realizada en función del tiempo necesario para reparar dicho daño:

- **Daños triviales.**- Daños que no ocasionan ninguna pérdida grave de funcionalidad de nuestro sistema y que originan una pequeña molestia al usuario. Deshacerse del virus implica, generalmente, segundos o minutos. Un ejemplo de este tipo de daños lo encontramos con el virus "Form" el cual, el día 18 de cada mes hacía sonar un pitido cuando pulsábamos cualquier tecla.
- **Daños menores.**- Daños que ocasionan una pérdida de la funcionalidad de las aplicaciones que poseemos. En el peor de los casos tendremos que reinstalar las aplicaciones afectadas lo que nos puede llevar de media hora a una hora. Un ejemplo de virus que ocasionan este daño sería el famoso "Viernes 13" o "Jerusalem". Este lo que hace es, todos los viernes 13, borrar todos los programas que se han utilizado después de que el virus haya infectado nuestro sistema.
- **Daños moderados.**- Los daños que el virus provoca son formatear el disco duro, mezclar los componentes de la FAT o sobrescribe en el disco duro. Para solucionar esto utilizaremos la última copia de seguridad que hemos hecho y reinstalaremos el sistema operativo. Este proceso nos puede llevar de una a dos horas.
- **Daños mayores.**- Algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que, ni aún restaurando la última copia de seguridad que tengamos, volvamos al último estado de los datos. El día que detectemos la presencia del virus y queramos restaurar el último backup nos daremos cuenta que éste también está infectado. Puede que lleguemos a encontrar una copia de seguridad no infectada, pero será tan antigua que hayamos perdido una gran cantidad de archivos que fueron creados con posterioridad al backup no infectado. Un ejemplo de este tipo de virus es el "Dark Avenger".
- **Daños severos.**- Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuando los datos son correctos o han cambiado, pues no hay unos indicios claros de cuando se ha infectado nuestro sistema.
- **Daños ilimitados.**- El virus lo que hace es que personas no autorizadas para ello puedan entrar en nuestro sistema. El daño no lo ocasiona el virus, sino esa tercera persona que, gracias a él, puede entrar en nuestro sistema. Un ejemplo es el virus "Cheeba".

MEDIOS PARA DEFENDERSE DE LOS VIRUS

Los consejos que a continuación se van a desarrollar están pensados para empresas que posean una red local o global y que dispongan de una conexión a Internet. No obstante hay alguna medida que se puede extrapolar para el caso de particulares o de empresas que no posean una red o una conexión a Internet o ambas cosas._

En primer lugar hay que poseer una cierta seguridad informática. Ésta se consigue con la realización de copias de seguridad frecuentes. El software se puede comprar de nuevo, pero la información sólo la puede proteger el usuario y la pérdida de la misma le puede ocasionar graves daños. En caso de tener computadores portátiles habrá que hacer backups de todos ya que éstos pueden contener información confidencial y valiosa.

Evitar la infección. Esto se consigue teniendo un programa antivirus y actualizándolo con la mayor frecuencia posible, ya que un antivirus sin actualizar no sirve como defensa ante los virus de nueva generación.

Recordar que un e-mail puede incorporar un virus en una macro. Al abrir un mensaje que incluya macros, hay que asegurarse de que están desactivado antes de continuar. Se deben tener configurados los programas para que avisen al usuario antes de abrir de un archivo que contenga macros. Además un e-mail puede incorporar un virus en un script de Visual Basic y en HTML (esto es parecido a las macros). Una manera de evitar contagios es desactivando la opción de ejecutar los scripts en el navegador o en el procesador de textos. Además si se recibe algún mensaje de alguien a quien no se conoce y ese mensaje contiene un fichero adjunto, no se debe abrir y se debe asegurar que el archivo no contiene ningún virus.

Proteger contra escritura el archivo "Normal.dot", ya que los virus de macro suponen hoy en día el mayor tipo de virus y la mayoría de estos virus atacan a este archivo. Al protegerlo contra la escritura se podrán detectar todos los intentos de sobreescritura. Esta medida no evita el hecho de infectarse con virus de macro, pero sí disminuye los problemas cuando ya se ha producido una infección.

Tener cuidado con los programas gratuitos de Internet ya que, al haber muchos programas y utilidades disponibles en este medio y se consiguen con el hecho de descargarlos, algunos pueden incluir virus. Si se utiliza algún programa de este tipo, hay que asegurarse de que está limpio antes de utilizarlo.

Distribuir archivos con la extensión ".rtf" en vez de archivos con la extensión ".doc", ya que los primeros no soportan macros y así se evita el contagio de este tipo de virus.

En caso de se sufra una infección de un virus lo primero de todo es evitar el pánico. Se deberá informar a los responsables de seguridad informática quienes comprobarán primero el Servidor y posteriormente las estaciones de trabajo. Cuando se descubra donde está el virus hay que aislar el PC portador y evitar el intercambio de disquetes y CD's con otros PC's. Se debe evitar el envío de mensajes y de archivos a través de la red o de Internet. Se comprobará que existen backups actualizados y, si no es así, se deberán hacerlos inmediatamente, aunque el PC esté infectado. También se comprobará que está instalada y, en caso contrario, instalarla, la versión más actualizada que exista del software antivirus. Por último pedir el asesoramiento de una empresa especializada en estos temas para que solucione el problema.

¿Qué es un HOAX?

Los hoax (mistificación, broma o engaño), son mensajes con falsas advertencias de virus, o de cualquier otro tipo de alerta o de cadena (incluso solidaria, o que involucra a nuestra propia salud), o de algún tipo de denuncia, distribuida por correo electrónico. Su común denominador, es pedirle que los distribuya "a la mayor cantidad posible de conocidos".

- Jamás reenvíe un mensaje de este tipo que llegue a su casilla. Esta clase de alarmas, suelen ser **TOTALMENTE FALSAS**, o basadas en hechos erróneos, pero lo que es peor activan un tipo de "contaminación" muy diferente.

Se registró la circulación de cadenas de mails con información errónea sobre virus, al indicar que se elimine un archivo ejecutable de la carpeta Windows. Estos mails son denominados **HOAX**.

¿Qué evitamos al no reenviarlas?

1. La propagación de una noticia inexistente que puede causar problemas a usuarios inexpertos.
2. La divulgación de las direcciones de correo electrónico de nuestros conocidos, amigos, familiares y contactos de negocios que son enviados y reenviados hasta que alguien las elimine del mensaje original.
3. La proliferación de información 'basura' por internet.

¿Que es un Joke?

Los **Jokes** no son virus sino más bien bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus.

Se trata de programas que simulan los efectos de virus destructivos -por ejemplo la eliminación de los ficheros de disco duro-. Ante este tipo de programas lo mejor es no perder la calma y comprobar que en realidad no han producido los efectos destructivos que el programa simulaba.

PÁGINAS WEB CONSULTADAS

- <http://www.albanet.com.mx/>
- <http://www.antivirus.com.ar/>
- <http://www.bbc.co.uk/>
- <http://www.cibernauta.com/>
- www.ctv.es/USERS
- <http://www.derecho.org/>
- <http://www.edata.es/>
- <http://www.el-mundo.es/>
- <http://www.e-new.com/>
- <http://www.gratisweb.com/>
- <http://www.kriptopolis.com/>
- <http://www.monografias.com/>
- <http://www.noticias.com/>
- <http://www.sinvirus.com/>
- <http://www.virusprot.com/>

GLOSARIO DE TÉRMINOS

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. Este tipo de objetos se ejecutan automáticamente al abrir la página web donde éstos se encuentran. No obstante, es posible configurar las opciones de seguridad del navegador para que esta ejecución no tenga lugar. Para eliminar los controles ActiveX que contengan código malicioso bastará con borrar éstos.

Análisis Heurístico. Se trata de un análisis adicional que solamente algunos programas antivirus pueden realizar, para detectar virus que en ese momento son desconocidos. Se caracteriza por analizar los archivos, obteniendo información de cada uno de ellos (tamaño, fecha, y hora de creación, posibilidad de residir en memoria, etc). Esa información es analizada por el programa antivirus, quien decide si puede tratarse de un virus o no.

Antivirus. son todos aquellos programas que permiten analizar memoria y unidades de disco en busca de virus (por ejemplo F-Prot, AVP, Panda Antivirus). Una vez el antivirus ha detectado alguno de ellos, informa al usuario procediendo a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.

Archivo de Identificadores de Virus. Se trata de una base de datos que contiene las referencias utilizadas para la detección de los virus en la computadora objeto del análisis.

Armouring. 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). Pues bien, en un virus que utilice la técnica de Armouring no se podrá leer el código.

ASCII (Código ASCII). se trata del código con el que se codifican los caracteres (texto, números, signos de puntuación,...etc). Cada uno de ellos tendrá asignado un código de 8 bits (bit: unidad mínima de información, 0 o 1)

Atributos. los ficheros y directorios tienen asignadas características que se denominan atributos. Estas pueden ser: sólo lectura, modificado, oculto, de sistema

Autoencriptación. 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), que los identifican. 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.

Backdoor (BCK, puerta trasera). Se trata de una característica que incorporan ciertos programas que permite el acceso remoto a los equipos afectados mediante la apertura de una "puerta trasera".

BIOS. es la abreviatura de Basic Input / Output System e identifica al software o conjunto de programas que arrancan la computadora (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. El BIOS se encuentra siempre en la memoria principal, pero no en la RAM (Random Access Memory) pues al apagar la computadora

se borraría, sino en la ROM (Read Only Memory - Memoria de Sólo Lectura), cuyo almacenamiento es permanente.

BOOT, MASTER BOOT (Sector de Arranque). 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 la computadora, mediante la utilización de ese disco. Cuando se habla del Boot se hace referencia al sector de arranque de un disquete, mientras que el término Master Boot (MBR) hace referencia al sector de arranque de un disco duro.

Cadena. es una consecución de caracteres 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 texto (o código) que éstos incluyen 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 en Internet. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto de personas, al mismo tiempo.

Cifrado / Encriptado. 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 realizar 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 Windows (Registry) es un elemento en el que se guardan las especificaciones de configuración de la computadora, 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.

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.

Virus de Compañía . este tipo de virus no se añade a otros programas sino que utiliza otras técnicas para asociarse a otros programas. Por ejemplo, en caso de existir un fichero ejecutable con un determinado nombre y extensión EXE, el virus se encargará de crear otro fichero con el mismo nombre pero con extensión COM haciéndolo invisible (oculto) al usuario para evitar levantar sospechas. Este fichero que crea será el propio virus y el sistema operativo, al encontrarse con dos ficheros que llevan el mismo nombre, ejecutará en primer lugar el de extensión COM, siendo éste el virus que en ese preciso instante realizará la infección. Tras realizarse la ejecución del fichero COM correspondiente al virus, éste devuelve el control al sistema operativo para que ejecute el fichero EXE. De esta forma el usuario no tendrá conocimiento de la infección que en ese preciso instante ha tenido lugar. Este tipo de virus también es conocido con el nombre de *Spawning*.

Contraseña. algunos virus protegen los documentos infectados con contraseñas con el fin de hacer que éstos sean inaccesibles. Esta contraseña podrá ser una cadena de texto o incluso un número generado de modo aleatorio.

Denegación de Servicio (DOS). se trata de un tipo de ataque en el que se priva a un usuario o organización de ciertos servicios que deberían estar disponibles en circunstancias normales. Generalmente estos servicios se centran en el cese del normal funcionamiento de redes o sistemas de correo electrónico. Por otra parte, este tipo de ataques es capaz de dañar archivos en los computadores afectados. Aunque estos ataques suelen ser malintencionados, también es posible que ocurran de modo accidental.

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 (assembler) (no lenguajes de alto nivel). También hace posible la investigación del código interno en cualquier fichero.

Dropper. Se trata de ficheros ejecutables que contienen virus en su interior. Cuando estos ficheros son ejecutados, el "dropper" libera los virus que contiene. Cuando se analiza este tipo de ficheros con un programa antivirus, el trabajo de análisis no detectará ningún virus ya que el código del virus no se crea hasta que el usuario ejecuta el dropper.

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.

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. Esta tabla se encuentra localizada en el Boot o sector de arranque del disco.

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, compuesta por tres caracteres 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),..., etc.

Ficheros de Proceso por Lotes (.BAT, ficheros 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 va ejecutando de forma secuencial. Un fichero muy importante de este tipo es el AUTOEXEC.BAT, el cual se encuentra siempre en la raíz del disco duro y se ejecuta automáticamente cuando la computadora arranca, cargando una serie de controladores y programas.

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.

Gusano. es 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.

Gusano de Script, de mIRC. se trata de archivos ejecutables que modifican el fichero SCRIPT.INI para hacer posible la distribución del gusano a través de los canales de IRC. Este tipo de gusanos funcionan a través de programas como mIRC o Pirch.

Gusano de Visual Basic Script. este tipo de gusanos utilizan el IRC o Outlook para enviar copias de ficheros infectados a otros usuarios.

Gusano de Win32. este tipo de gusanos se propaga a través de las API de Windows, funciones MAPI o clientes de correo electrónico como Microsoft Outlook. Estos gusanos son capaces de enviarse a sí mismos como un fichero adjunto a todas las direcciones a las que el usuario afectado envíe un mensaje de correo.

Hoax. Los llamados Hoax no son virus sino falsos mensajes de alarma sobre virus in-existent. Estos se envían por correo electrónico con la intención de extender falsos rumores por Internet. Los mensajes no suelen estar fechados, con lo que se pretende que los mensajes siempre parezcan recientes. En ocasiones, los Hoax pretenden engañar a los usuarios mediante el uso de palabras técnicas. Por otra parte, suele ser frecuente la inclusión del nombre de ciertas agencias de prensa (CBS...) en el encabezamiento de estos mensajes. Con todo esto se pretende dar un aspecto verídico a los mensajes.

Host. Este término se refiere a un computador que actúa como fuente de información. Este término se puede referir a casi cualquier tipo de computador; desde un computador central que actúa como host para sus terminales, hasta un servidor que actúa como host para sus clientes. También se puede decir que un computador puede actuar como host para sus periféricos. Finalmente, los clientes en las redes también son considerados host ya que actúan como fuente de información en la red.

In The Wild (lista). este término se refiere a una famosa lista en la que se reflejan los virus que, en la actualidad o en ese lapso, 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.

Infección. es la acción que realiza un virus al introducirse, empleando cualquier método, en nuestro computador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas.

Interrupción. es una señal mediante la cual se consigue hacer una pausa momentánea en las labores que se encuentra ejecutando el microprocesador. Cuando ésta tiene lugar el micro 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 un tipo de interrupción aceptada, el microprocesador continúa con la tarea que abandonó en su momento.

IRC. es una de las posibilidades que permite Internet. Mediante el IRC se pueden mantener conversaciones escritas, en tiempo real, entre varios usuarios conectados a un canal de comunicaciones disponible en Internet.

Java. se trata de uno de los lenguajes de programación con el que se pueden crear páginas Web.

Java Applets (Applets de Java). los Applets de Java con pequeños programas incluidos en algunas páginas HTML. Estos programas se pueden ejecutar automáticamente al abrir la página HTML en cuestión. Los creadores de virus pueden aprovecharse de esta circunstancia para realizar ataques a otros sistemas. En muchos casos, es posible configurar los navegadores para que estos pequeños programas no se ejecuten de modo automático.

Jokes. Los Jokes no son virus sino más bien bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus. Se trata de programas que simulan los efectos de virus destructivos -por ejemplo la eliminación de los ficheros de disco duro-. Ante este tipo de programas lo mejor es no perder la calma y comprobar que en realidad no han producido los efectos destructivos que el programa simulaba.

Macro (Virus de macro). una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son "microprogramas" que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo de, 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. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas.

Malware. Malware es un término general utilizado para referirse a programas que contengan código malicioso, ya sean virus, troyanos o gusanos.

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.

Ocultamiento u Ocultación (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. Cuando un virus infecta un archivo, suele dejar signos evidentes de su actuación, como aumento de tamaño del archivo infectado, modificación de la fecha y hora de creación, secciones marcadas como defectuosas, y otras. Los virus que utilizan stealth evitan que estas pistas se visualicen, para lo cual vigilará peticiones de información que intercepta ofreciendo información falsa.

PE (Portable Executable). El término PE (Portable executable) se refiere a al formato estándar de archivos ejecutables de Win32.

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 de lectura, sin desplazar la cabeza lectora del disco a otra posición.

Plantilla (Plantilla Global). una 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.

Payload. este término se refiere a los efectos secundarios que cualquier virus puede producir cuando ya ha pasado cierto tiempo desde el momento de la infección.

Polimórfico / Polimorfismo. basándose en la técnica de autoencriptación, 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 la encriptación, pero adicionalmente el virus cifrará 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.

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 hiperenlace. Con ello nos referimos a determinados elementos (texto, imágenes, botones) y/o secciones de un documento HTML (una página Web). 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). el denominado Registro de Windows (Registry) es un fichero en el cual se almacenan todos los valores de configuración e instalación de los programas que se encuentran instalados y de la propia definición del sistema operativo. Esta configuración se rige por claves, subclaves y valores que se pueden consultar y modificar y que la mayoría de programas modifican de forma automática (en algún aspecto) al instalarse.

Réplica. 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. 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 de la computadora y desde ella está continuamente comprobando si se ejecuta algún programa. Cuando esto ocurre, infecta el programa ejecutado.

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.

Sistema Operativo (S.O.). 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 la computadora, 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 computador del mundo (el mejor hardware), pero si éste no tiene instalado un sistema operativo, no funcionará (ni siquiera se podrá encender). Algunos ejemplos de sistemas operativos son: MS/DOS, UNIX, OS/2, Windows 95/98/2000/NT,...etc.

Sobreescritura. los virus de sobreescritura se caracterizan por no respetar la información contenida en los ficheros que infecta, haciendo que estos queden inservibles poste-

riormente. 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.

Script (Virus de Script). los virus de script están escritos en lenguajes de programación como VBScript y JavaScript. Estos virus utilizan el Scripting Host de Windows para activarse e infectar otros archivos. Los virus se activarán de modo automático al hacer doble clic en los ficheros VBS y JS infectados.

Sobrepasamiento (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.

Troyano. los troyanos no se replican o no hacen copias de sí mismos. En realidad son programas que llegan a un computador de forma totalmente normal y no producen efectos realmente visibles o apreciables (por lo menos en ese momento). Pueden llegar acompañados de otros programas y se instalan en nuestro computador. Al activarse puede dejar huecos en nuestro sistema, a través de los cuales se producen intrusiones.

Vacunación. 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. Una variante es una versión modificada de un virus original. Estas modificaciones pueden ser tan simples como un cambio en los mensajes de texto que pueda mostrar el virus, o más complejas como la incorporación de nuevas líneas de código.