SEGURIDAD INFORMATICA.

Seguridad de la Información.

Dando por bueno que la seguridad trata de la protección de los bienes, parece natural establecer cuáles son los bienes informáticos a proteger. En una primera panorámica podríamos decir que éstos son: el hardware; el software y los datos. De estos bienes, los más expuestos a todo tipo de riesgos, y también los que más rápidamente se devalúan, son los datos. Están expuestos a más riesgos, puesto que son accedidos por más personas: usuarios; analistas; programadores, que los restantes bienes y sometidos a las mismas amenazas no intencionadas que los demás. Son los que más rápidamente se devalúan, pues su tiempo de vida útil suele ser corto y pierden su valor más rápidamente que el hardware, cuyo tiempo de vida útil se suele estimar en torno a 2 o 3 años y el software que en algunos casos (p. ej., los de gestión y control) con los mantenimientos oportunos, se mantiene operativo durante más de 5 años.
Naturalmente podríamos listar otros bienes a proteger como: personal informático; materiales fungibles; suministros de potencia y aire acondicionado; sistemas de transmisión de datos; etc., pero, por un lado, son bienes no intrínsecamente informáticos (aunque imprescindibles para el desarrollo de la función informática) y, por otro, su protección viene dada por los mismos mecanismos que los de los tres bienes enunciados anteriormente.

Las amenazas que se ciernen sobre los sistemas informáticos tienen orígenes diversos. Así, si consideramos las amenazas externas, el hardware puede ser físicamente dañado por agua, fuego, sabotajes, y otros. Las mismas causas pueden dañar los medios magnéticos de almacenamiento externo. La información contenida en éstos, también puede verse afectada por campos magnéticos intensos y, frecuentemente, por errores de operación. Las líneas de comunicación pueden ser interferidas o "pinchadas", etc.

Otros tipos de amenazas provienen de usuarios o empleados infieles. Así, los primeros pueden usurpar la personalidad de usuarios autorizados y acceder indebidamente a datos para su consulta o borrado, o, aunque algo más complicado, modificar en su provecho programas de aplicación.

Otras amenazas más sutiles provienen de inadecuados controles de programación. Así, el problema de residuos, es decir, de la permanencia de información en memoria principal cuando ésta es liberada por un usuario o, en el caso de dispositivos externos cuando ésta es incorrectamente borrada. Una técnica fraudulenta muy usada consiste en transferir información de un programa a otro mediante canales ilícitos y no convencionales (canales ocultos).

El comportamiento de las amenazas a la seguridad de la información arroja que la mayoría de los hechos son realizados por intrusos individuales. Un porciento menor corresponde a incidentes realizados por grupos organizados, otro porciento aun menor son delitos y la punta de la pirámide corresponde a casos de espionaje, (industrial, económico, militar...). Según la Oficina de Ciencia y Tecnología de la Casa Blanca las pérdidas anuales estimadas en USA por espionaje económico ascienden a $ 100 Miles de Millones de USD.

Las principales amenazas de Internet son:

- *Los ANEXOS a mensajes enviados por email infectados por virus.*
- *El intercambio de códigos de virus.*
- *Los FIREWALLS o Cortafuegos mal configurados.*
- *Los ataques a la disponibilidad de Recursos.*
- *Alteración de páginas Web.*
- *El "Repudio" y las estafas asociado al Comercio Electrónico.*
- *Las vulnerabilidades de los Sistemas Operativos y la no actualización de los PARCHES concernientes a la Seguridad de los mismos.*
- *La rotura de contraseñas.*
- *La suplantación de identidad*

- *El acceso a páginas pornográficas, terroristas, etc.*
- *El robo y la destrucción de información*
- *Pérdida de tiempo durante el acceso a sitios ajenos a la razón social de la entidad.*
- *El hecho de que herramientas de Hacking y Cracking se ofrecen como FREEWARE*

SEGURIDAD FISICA Y LÓGICA.

término seguridad física es el usualmente empleado para describir las medidas de protección externas ador, que tratan de proteger a éste y su entorno de amenazas físicas. Normalmente, se materializan mediante dispositivos eléctricos, electrónicos, etc.

De todas las medidas de protección ya esbozadas las físicas son, probablemente, las primeras que en todas las instalaciones informáticas se adoptan. Ello es debido a dos factores; por un lado, aunque la probabilidad de que se produzca un incendio o una inundación sean mucho menor que las probabilidades de ocurrencia de otras amenazas, ante una catástrofe como las citadas las pérdidas serían completas.

Por otro lado, estas medidas de protección son usualmente las más fáciles de tomar. Su costo no es excesivo (con la excepción de los sistemas de continuidad eléctrica) y su mantenimiento no ofrece especiales problemas.

Una primera medida de protección para las salas de Centros de Proceso de Datos (CPD), común a todas las amenazas expuestas es la ubicación geográfica adecuada de las mismas. Una segunda consideración, también general, es la correcta construcción de dicha sala y su situación idónea dentro del edificio.

Las siguientes medidas son ya específicas para cada tipo de amenaza, por lo que las expondremos bajo el riesgo que contribuyen a prevenir.

Inundaciones (intensas lluvias, desborde de ríos, penetraciones del mar, etc.)

La mejor medida es la adecuada ubicación de los equipos, en edificios alejados de zonas potencialmente peligrosas (cercanías de barrancos y cauces de ríos, zonas bajas de la costa, etc.). En todo caso estos sistemas conviene situarlos en plantas altas.

Inundaciones internas

Además de las medidas constructivas (no deben pasar conducciones de agua por los techos ni paredes, debe haber desagües en el piso real, el cual debe presentar una inclinación hacia estos, etc.) existen detectores de humedad, que situados en el piso real podrían avisar de la inundación. Además, se recomienda tapar con forros plásticos los equipos cuando no se usen (sobre todo los PC's).

Fuegos

Los sistemas de detección/extinción de incendios son de sobra conocidos. En la actualidad, el elemento extintor más usado es el halón, gas anticatalítico de la reacción química que produce el fuego y que en pequeña proporción no es inmediatamente tóxico.

Actualmente se investigan a marchas forzadas sustitutos, pues por el daño elevadísimo que producen a la capa de ozono, se acordó en la Convención de Montreal su total eliminación.

Caídas de tensión

En este epígrafe se consideran tanto las caídas propiamente dichas (cortes de más de pocos milisegundos), microcortes, transitorios, etc. Lo más eficaz contra estas anomalías del suministro es un sistema de alimentación ininterrumpida (SAI o UPS en inglés) en línea (los fuera de línea precisan de unos microsegundos, tiempo de conmutación, para actuar). De ser los tiempos prolongados se necesitaría un equipo electrógeno de respaldo.

Calor

La protección pasa por la instalación de alarmas que se disparan caso de subir o bajar la temperatura de la sala por encima o debajo de los límites permitidos.

Interferencias electromagnéticas

La solución óptima es el apantallamiento de la sala de ordenadores y en el caso de terminales el uso de aquéllos con certificación TEMPEST (enmascaramiento de pulsos electromagnéticos transientes). Para las líneas de comunicación (las más expuestas) el uso exclusivo de las apantalladas o, más seguro todavía, fibra óptica.

Atentados

Su prevención se consigue mediante estrictos controles de acceso a las áreas del ordenador y su entorno. En el caso de costosas o críticas instalaciones, los sistemas biométricos (mejor se debería decir bioantropométricos) son de gran fiabilidad. Entre estos se deben citar: reconocimiento de las huellas digitales, del patrón de las venas del fondo de ojo, de la forma de la mano, de la voz, etc. Además, se pueden instalar equipos de reconocimiento de materiales que entran en las instalaciones.

Hurtos

El problema actual más grave lo constituyen los ordenadores personales y sus partes componentes, cuya fácil portabilidad presenta un gran riesgo. Existen ya sistemas de anclaje muy efectivos y otros, que en conjunción con arcos en las salidas, permiten prevenir esta amenaza.

- MEDIDAS DE SEGURIDAD TECNICAS O LOGICAS.

Por lo que respecta a las medidas técnicas pretenden proteger tanto el software, sea de base o de aplicación, como los datos. Estas medidas pueden implementarse en dispositivos hardware o en productos software.

Para el desarrollo de estas medidas, se ha hecho necesaria una investigación académica muy intensa, principalmente en la última década y media, que ha dado lugar a modelos teóricos del máximo interés como pueden ser: modelos de control de accesos; modelos de control de flujo de información; desarrollo de criptosistemas de clave privada y pública; desarrollo de sistemas de firma digital y no-repudio en transmisión de datos.
A continuación expondremos muy someramente los temas más notables de estas medidas de protección.

-Criptología

A diferencia de las otras ramas del conocimiento que fundamentan la informática, todas ellas muy jóvenes, la criptografía (y por tanto la criptología) hunde sus orígenes, al menos, en la antigüedad clásica. Así, el escítalo lacedemonio era un instrumento criptográfico (un simple bastón con una tira de papel enrrollado) ya usado durante las guerras entre espartanos y atenienses, y el cifrado CESAR, empleado aún hoy en día para ejemplarizar los métodos criptográficos de sustitución, fue ideado por los romanos.

Por contra de los ejemplos anteriores, los métodos criptográficos son usados actualmente no sólo en temas relacionados con la guerra o el espionaje, sino que la sociedad de la información en la que vivimos, precisa de medios seguros de transportar y almacenar todo tipo de información, sea comercial, sanitaria, estadística o de cualquier otra clase, y así la criptografía ha experimentado en los últimos tiempos un fuerte desarrollo, que ha originado la aparición continua de nuevos y complejos algoritmos criptográficos, cuyos dos principales paradigmas son el RSA y el DES.

La palabra criptología deriva del griego Kriptos, oculto, y abarca tanto la criptografía, o sea, la protección de la información a través de su codificación mediante claves, como el criptoanálisis, es decir, la supresión de esa protección sin el conocimiento de la clave.

La criptografía asume generalmente que el criptoanalista tiene pleno acceso al criptograma. Así mismo, se acepta el principio enunciado por Dutchman A. Kerckhoff: "La seguridad del cifrado debe residir exclusivamente en el secreto de la clave". En otras palabras, el Principio de Kerckhoff establece que todo el mecanismo del cifrado, excepto el valor de la clave, es conocido por el criptoanalista.

Frecuentemente, los criptosistemas utilizan la misma clave para cifrar y para descifrar (o, si son distintas, del conocimiento de una se deduce la otra), son los criptosistemas de clave única o simétricos.

Por contra, otros métodos criptográficos usan dos claves distintas (no pudiéndose obtener a no ser que se posea una información adicional) para las operaciones citadas, denominándose criptosistemas de dos claves o asimétricos.

- Sistemas operativos

El principal problema en la construcción de sistemas informáticos seguros, es el diseño, desarrollo e implementación de sistemas operativos que satisfagan estrictas políticas de seguridad.

Para que un sistema operativo sea seguro debe ser diseñado de modo que: identifique y autentifique a todos los usuarios, controle el acceso a todos los recursos e informaciones, contabilice todas las acciones realizadas por usuarios (o procesos invocados por ellos), audite los acontecimientos que puedan representar amenazas a la seguridad, garantice la integridad de los datos, mantenga la disponibilidad de recursos e informaciones, etc. Todos estos aspectos han venido siendo estudiados con interés creciente en las dos últimas décadas, creándose modelos teóricos de gran importancia, que recientemente se han empezado a implementar en sistemas operativos comerciales.

Históricamente los primeros mecanismos de seguridad que se introdujeron en los sistemas operativos fueron la identificación y autenticación, esta última mediante contraseñas sólo conocidas por el usuario. Aunque este sistema sigue siendo el mayoritariamente usado, han empezado a aparecer otras formas de autenticación, entre ellas:

Identificación por hardware: el usuario o el terminal al que está conectado, posee un dispositivo hardware que identifica inequívocamente al mismo;
Características bioantropométricas del usuario, como pueden ser: huellas digitales; patrones de voz; imagen de la palma de la mano; mapa de las venas del fondo del ojo; etc.;
Conocimientos, aptitudes, hábitos del usuario; por ejemplo: características dinámicas de la firma (tiempo, aceleraciones, inclinaciones); estilo de pulsación del teclado; rasgos del uso del ratón; etc;
Información predefinida que posee el usuario: datos personales; culturales; aficiones; frases-contraseña; etc.;

Además, el modelo simple de contraseñas se ha venido perfeccionando, para evitar los riesgos que conlleva la utilización repetida de los mismos caracteres para acceder al sistema. Así, han aparecido los modelos de contraseña variable; de lista de contraseñas; basados en funciones

unidireccionales; los generadores de contraseñas, y otros muchos que aunque todavía no generalizados son usados en ciertas aplicaciones con estrictos requisitos de seguridad.

Mención aparte merece el cifrado de contraseñas, cada vez más usado para evitar que los ataques a la tabla de contraseñas del sistema puedan revelar las mismas.

- Redes de ordenadores

Por la aceptación que están obteniendo los estándares de la Organización Internacional de Estándares (ISO) sobre los "Open Systems Interconnection", y por la creciente influencia que ejercen, vamos a exponer la arquitectura de seguridad de dichas normas que, además, ejemplifica muy bien los conceptos básicos sobre los que se asientan todas las arquitecturas de seguridad.

En la arquitectura citada, hay cuatro capas de la torre de niveles OSI donde se pueden implementar los mecanismos de seguridad pertinentes. La implantación en uno u otro nivel dependerá de los requisitos de seguridad a satisfacer, que pueden clasificarse también en cuatro divisiones.

Así, un dispositivo de cifrado a nivel físico o a nivel de enlace es la solución si se desea conectar redes seguras, pero mediante enlaces inseguros. En efecto, aunque las redes de origen y de destino sean seguras, si el camino entre los nodos atraviesa alguna red insegura (por ejemplo, una red pública de datos), se precisa añadir mecanismos de seguridad en el nivel de transporte.

Sin embargo, si los ordenadores que desean comunicarse no tienen la certeza de que las redes a las que pertenecen sean seguras, se precisa que la seguridad se extienda extremo a extremo. Este tipo de seguridad se puede implementar en el nivel de red o de transporte. Ambas opciones están en consideración en los comités de normalización correspondientes.

Finalmente, algunos usuarios que sólo desean proteger algunas aplicaciones, o algunos campos de ciertas aplicaciones, necesitan implementar la seguridad en el nivel de aplicación, aunque a veces también se procede en el nivel presentación.

Los tres conceptos básicos de la arquitectura de seguridad de OSI son: amenazas a la seguridad, servicios de seguridad y mecanismos de seguridad.

Las primeras son acciones potenciales que pueden comprometer la seguridad de la información.

Se pueden clasificar en pasivas y activas.

Las amenazas pasivas consisten en el registro o detección de los datos mientras son transmitidos. Por no suponer alteración de los mismos son difíciles de detectar y de imposible recuperación, por lo que el único tipo de medidas de protección lo constituyen las preventivas. Las dos modalidades de estas amenazas son la lectura de datos y el análisis del tráfico. En este último caso el atacante se limita a leer las cabeceras de los paquetes, donde puede encontrar la identidad y situación de los nodos. También puede, a partir de aquí, obtener la frecuencia de los mensajes entre dos nodos lo que constituye, en ocasiones, una valiosa información.

Las amenazas activas se materializan mediante la conexión de un dispositivo a la línea de transmisión para alterar o borrar señales o generar otras nuevas. Pueden consistir en: la destrucción (o retraso) de todos los mensajes que circulan por una línea, la modificación del flujo de mensajes, sea borrando alterando, retrasando o reordenando algunos mensajes.

Por otra parte, un mecanismo de seguridad es una implementación hardware o software diseñada y construida para prevenir, detectar o recuperarse de la materialización de una amenaza. Cada servicio de seguridad es implementado mediante uno o varios mecanismos de seguridad.

Los mecanismos considerados en la norma OSI citada son: cifrado, firma digital, control de accesos, integridad de los datos, intercambio de autenticación, rellenado de trafico, control de rutas y notarización.

Finalmente, las normas OSI definen un servicio de seguridad como una función suministrada por un sistema de comunicación para mejorar su seguridad. Los servicios definidos son: confidencialidad, integridad, autenticidad, control de accesos y no repudio.

El uso de sistemas de interconexión abiertos (OSI), muy recomendable por su versatilidad y por su rápida implantación, incrementa las amenazas a la información con lo que el mantenimiento de la confidencialidad, integridad y disponibilidad es una tarea mucho más ardua.

- Evaluación y certificación de la seguridad

Finalmente, cabe resaltar que a la par que el interés se ha desplazado hacia estas medidas técnicas, se ha ido poniendo de manifiesto la necesidad de evaluar la calidad de las funciones de seguridad que los sistemas de información iban incorporando. Desgraciadamente, esta evaluación no puede realizarse mediante una métrica exacta; por lo que la verificación de estas funciones de seguridad debe hacerlas una institución neutral y digna de confianza. Además, el proceso de verificación debe ser transparente, lo que es sólo posible mediante una descripción detallada de los procesos que se han seguido y los correspondientes criterios de verificación.

PLAN DE SEGURIDAD INFORMATICA.

El Plan de Seguridad Informática constituye el documento básico para lograr la confidencialidad, integridad y disponibilidad de la información y la protección de los medios y los locales donde se utilice la técnica de computación.

En el desarrollo de este plan es necesario formular la política de seguridad, establecer una estructura de gestión de la seguridad informática, elaborar el sistema de medidas de seguridad informática, implantar el programa de seguridad informática y elaborar el plan de contingencia de la entidad.

Previo a la formulación de la política de seguridad, se deben considerar diferentes aspectos referentes a la información en la organización. Así, es imprescindible hacer un estudio de:

1º.-grado de criticidad de los diversos servicios respecto de la información y del valor de ésta para aquellos;
2º.-nivel de inversión en Tecnologías de la Información;
3º.-amenazas (sean accidentales o intencionadas) que sufre la información;
4º.-las vulnerabilidades de los sistemas y productos de T.I. existentes;
5º.-las medidas de seguridad ya implantadas.

Con este estudio previo se puede ya elaborar la política de seguridad. Ésta es el conjunto de principios y reglas generales que regulan la forma, propia de cada organización, de proteger las informaciones que maneja en todas las fases de su tratamiento.

Un factor determinante en la elaboración de esta política, y consecuentemente en el éxito del plan de seguridad, es la implicación de los máximos responsables de la institución. A no ser que éstos comprendan y se involucren en los objetivos de la política de seguridad su final feliz será incierto. La veracidad de esta afirmación resulta de considerar que la política de seguridad afecta a todos los servicios y niveles dentro de éstos, así como a los flujos de información entre diferentes servicios, de éstos al exterior y viceversa. Es decir, involucra a todo el sistema de información de la organización.

- POLITICA DE SEGURIDAD INFORMATICA.

La política de seguridad que nos ocupa puede contener principios específicos para algunos servicios en los que la seguridad de la información sea especialmente crítica. O también, puede incluir aspectos convenientes sólo a ciertos equipos, como pueden ser ordenadores personales.

Entrando ya en los contenidos de la política de seguridad, ésta debe comenzar postulando que la información es un activo más del organismo y cuáles son las características a priorizar de este activo: la confidencialidad (impedir la divulgación no autorizada); la integridad (impedir la modificación no autorizada) y la disponibilidad (impedir la retención no autorizada). Se deben tratar, al menos, los siguientes aspectos:

Organizativos:

Se deben definir las responsabilidades de los empleados, y el papel que desempeñan éstos, en la protección de la información y las líneas de dependencia funcionales a este respecto. Igualmente, se debe crear una estructura departamental específica, responsable de coordinar y controlar en todo el organismo la seguridad de la información.

De Personal:

Se deben contemplar aquí, sobre todo, los aspectos de concienciación y formación en seguridad.

Igualmente, se deben tratar los aspectos sancionadores, caso de incurrir en negligencias, las políticas de contratación y el empleo de personal externo cuando sea preciso. Todo ello bajo la perspectiva de la seguridad.

***De Procedimiento**:*

La política de seguridad se debe considerar como una referencia obligada en todo el ciclo de vida de los sistemas de información. Así, la seguridad de las T.I. debe ser tenida en cuenta en el desarrollo de todas las aplicaciones (estableciendo el modo de hacer esto), en la adquisición de equipos físicos y lógicos (incluyendo cláusulas específicas en los contratos), en la instalación y mantenimiento de éstos, etc.

Así mismo, se debe definir la manera de mantener y cambiar, en su caso, estos procedimientos.

Clasificación de la información:

La información debe ser clasificada de acuerdo con su sensibilidad e importancia para la organización, ya que no es posible esperar que los directivos y trabajadores mantengan un absoluto control sobre toda la información que manejan; así pues, es necesario que conozcan: primero, qué informaciones son consideradas más sensibles y, segundo, cómo se deben manejar y proteger estas informaciones.

La implantación de esta clasificación suele encontrar resistencia en el personal, que acusa el incremento de trabajo que supone. Es por tanto imprescindible una operación de "venta" a los empleados de este sistema; así como limitar al máximo las informaciones tipificadas en el más alto nivel.

Así mismo, se considerará la manera de desclasificar, etiquetar, almacenar, acceder, destruir y reproducir las informaciones según dicho nivel de clasificación.

Manejo de incidentes:

Se establecerá un registro de incidentes de la seguridad de la información, que capacite a los departamentos para analizar las tendencias, prever incidentes futuros y concentrar los recursos de seguridad de la manera más eficiente.

***Análisis de riesgos**:*

Se especificará el método para analizar los riesgos de la información, así como para definir riesgos máximos asumibles.

***Auditoría**:*

Se establecerá la extensión y periodicidad de las auditorías de seguridad internas y externas. En los reportes finales de las auditorías deberá siempre establecerse la elaboración de un Plan de Medidas para la solución de los problemas encontrados. Según la extensión y ambición con que se aborde la política de seguridad, se pueden afrontar más o menos temas, aunque los anteriores deberían considerarse los mínimos a contemplar.

- ESTRUCTURA DE GESTION.

Por lo que respecta a la determinación de la estructura de gestión, debe crearse una unidad (departamento, sección, grupo, etc.) específica encargada de gestionar la seguridad.

-SISTEMA DE MEDIDAS DE SEGURIDAD.

Se relacionarán las medidas necesarias para garantizar la seguridad de la información a partir de los objetivos planteados.

Las medidas que se definirán en el documento se clasificarán según su función, las cuales pueden ser de; Seguridad Física, Seguridad Técnica o Lógica, Administrativas u Organizativas, Seguridad de Operaciones, Legales y Educativas o de Concientización. Según su forma de actuar dentro del sistema de la Entidad y las mismas pueden ser de tipo preventivas, detectivas o correctivas, y partiendo de estas clasificaciones se ordenarán las medidas.

-PLAN DE CONTINGENCIA.

Se denomina Plan de Contingencia (también de recuperación de desastres o de continuación de negocios), a la definición de acciones a realizar, recursos a utilizar y personal a emplear caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización. Es decir, es la determinación precisa del quién, qué, cómo, cuándo y dónde, caso de producirse una anomalía en el sistema de información.

El Plan de Contingencia debe considerar todos los componentes del sistema: Datos críticos, equipo lógico de base, aplicaciones, equipos físicos y de comunicaciones, documentación y personal. Además, debe contemplar también todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: suministro de potencia; sistemas de climatización; instalaciones; etc. Finalmente, debe prever también la carencia, por cualquier motivo, de personal calificado para el correcto funcionamiento del sistema.

Se debe destacar, que previo al comienzo del trabajo, se debe obtener el pleno compromiso de los máximos responsables de la organización. Sin su apoyo el fracaso del plan está garantizado.

- PROGRAMA DE SEGURIDAD.

El programa de seguridad deberá desarrollar la política de seguridad y luego implementar y mantener este desarrollo. Se deberán identificar proyectos y productos, establecer calendarios, asignar prioridades, acordar recursos, y fundamentalmente, dictar procedimientos concretos. Estos

procedimientos serán administrativos, técnicos, físicos y de personal. Entre los primeros: clasificación de la información; privilegios de acceso; gestión de la configuración; registro de incidencias; uso de programas externos; control y etiquetado de documentos; almacenamiento y destrucción de soportes de información; gestión de cambios; mantenimiento de equipos y programas; metodología de análisis y evaluación de riesgos; manual de medidas de seguridad; plan de contingencia; etc. Entre los técnicos: controles de acceso lógico; normas de diseño, desarrollo y, sobre todo, mantenimiento de programas propios; tipo de técnicas criptográficas y casos en que procede su uso; etc. Entre los físicos: controles de acceso físico (personas y objetos); gestión de bienes; protección de fuegos, inundaciones y atentados; etc. Por lo que respecta a los de personal: contratación; plan de concienciación y formación; responsabilidades; infracciones y sanciones; etc.

Por último, el programa de seguridad debe contener las indicaciones oportunas que permitan su implantación y evaluación continuada (entre otros mediante auditorías y cuestionarios periódicos a ser cumplimentados por los responsables de los distintos servicios y secciones), que permitan la actualización del mismo, o incluso de la política de seguridad cuando sea preciso.

-PLAN DE FORMACION.

El plan de formación contendrá todas las acciones a desarrollar para la capacitación de todos los trabajadores de la organización en materias de protección y seguridad de la información de forma general y muy especialmente en relación con los puestos de trabajo en concreto. En esta formación se utilizarán diversos métodos como seminarios, cursos, conferencias, demostraciones prácticas y otros. El plan de formación y su aplicación serán objeto de aprobación y control por parte de las distintas instancias de la propia organización.

REGLAMENTO SOBRE SEGURIDAD INFORMATICA (Fragmento)

TITULO I

OBJETIVOS Y ALCANCE

ARTICULO 1: El presente Reglamento tiene por objeto establecer las medidas de Seguridad y Protección de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías informáticas y de comunicaciones, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información en ellas contenida; así como la Disciplina Informática, que regirá el trabajo con dichas tecnologías dirigida a preservar su integridad.

ARTICULO 2: A los efectos de este Reglamento el conjunto de las medidas de Seguridad y Protección de la Información, y de Disciplina Informática constituirán la Seguridad Informática, que comprende medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo o constituyan una amenaza para la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías informáticas y de comunicaciones; así como el correcto uso y conservación de las mismas.

ARTICULO 3: Este Reglamento será de aplicación en todos los Organos y Organismos de la Administración Central del Estado y sus dependencias, otras entidades estatales, empresas mixtas, y en todas aquellas empresas que operen en el territorio nacional, siendo de obligatorio cumplimiento por todas las personas que participen en la elaboración, uso, aplicación, explotación, y mantenimiento de las Tecnologías Informáticas y de Comunicaciones.

El responsable del cumplimiento de lo dispuesto en el párrafo anterior será el jefe máximo de cada entidad.

ARTICULO 4: La información que se procese, intercambia, reproduzca y conserve a través de los medios técnicos de computación se considera un bien de cada entidad.

ARTICULO 5: Se considerará información sensible a los efectos de esta norma aquella que sin ser clasificada pueda considerarse vital por las entidades para sus operaciones científicas, comerciales, económicas, entre otras, y cuya pérdida o modificación no autorizada altere o pueda alterar la capacidad de gestión de la misma, ocasione ó pueda ocasionar, pérdidas en valores, o pueda ser perjudicial para la integridad física o moral de una persona.

Su acceso, uso y divulgación inadecuada implicará la responsabilidad que corresponda.

INTRODUCCION A LOS VIRUS INFORMATICOS.

Los programas destructores de la información procesada en las computadoras han causado una gran alarma y pánico desde su aparición en el mundo informático hace unos años, lo cual es lógico si nos percatamos que estos programas, donde los virus informáticos son sus máximos exponentes, representan un grave y serio problema para la seguridad e integridad de la información almacenada en las máquinas computadoras.

Por su analogía con los Virus Biológicos, se les llama Virus Informáticos, a programas escritos por especialistas de computación que se reproducen a sí mismos y además ejecutan una acción o efecto secundario en los Sistemas que infectan, pero a diferencia de los Virus Biológicos, los Virus Informáticos son resultado del trabajo mal orientado del hombre, no de la obra de la naturaleza.

Los virus atentan contra la productividad del trabajo de las computadoras ya que afectan sus recursos principales: el tiempo de procesamiento y el espacio de memoria disponible del Sistema; tanto la memoria operativa (RAM), como la memoria externa de los discos duros y disquetes, y pueden ser capaces de alterar, destruir o borrar la información contenida en las computadoras, mutilando en segundos el esfuerzo de especialistas de meses o tal vez años, con la consecuente pérdida de recursos materiales y humanos.

El desarrollo creciente de las aplicaciones de la Informática ha incrementado su dependencia a los sistemas automatizados, los cuales se ven amenazados por la acción devastadora de los virus informáticos, que pueden poner en peligro actividades tan importantes como la salud (fundamentalmente en relación con el diagnóstico y tratamiento clínico), las investigaciones científicas, los controles económicos y financieros, la automatización industrial, los servicios de reservación de pasajes, hoteles y otras capacidades, el pago de la seguridad social, el cobro de servicios como el telefónico, la electricidad, el gas, además de otros que harían muy extensa esta relación; lo que causaría cuantiosos daños económicos y sociales.

DEFINICION Y TERMINOS DE PROGRAMAS DESTRUCTORES.

Existen diferentes versiones en cuanto al surgimiento de los programas destructores, sin embargo existen dos hechos que los medios especializados en informática, divulgan como los posibles creadores de estos programas.

El primer hecho es que John Von Neumann, en 1949 en su libro "Theory And Organization of Complicated Automata" describió algunos programas que se reproducían a sí mismos.

El segundo hecho y al parecer el que desencadenó en el mundo de las microcomputadoras a los programas destructores relata que varios científicos de los Laboratorios Bell, inventaron un juego, con el objetivo de entretenerse, inspirado en un programa escrito en Lenguaje Ensamblador, el cual tenía la capacidad de reproducirse cada vez que se ejecutaba.

El juego consistía en invadir la computadora del adversario con un código que contenía una serie de informaciones destinadas a destruir la información de la memoria de su adversario o impedir su correcto funcionamiento. Conscientes de la peligrosidad que el juego representaba, prometieron mantenerlo en secreto.

Sin embargo, en 1983 el Doctor Ken Thompson, en una alocución en la Association For Computing Machinery, da a conocer la existencia de esos programas con detalles de su estructura.
A partir de ese momento, muchos son los casos conocidos de autores de programas destructores, que como recreación o de forma maliciosa han causado el pánico y la histeria en el mundo informático.

Existen varias clasificaciones y definiciones de los mismos según su forma de actuar, nosotros preferimos la siguiente clasificación:

-Gusanos:

Los Gusanos son programas que pueden provocar efectos tan dañinos como los causados por los virus, pero se diferencian de éstos en su forma de transmitirse, pues no infectan otros programas con una copia de sí mismos, ni son insertados en otros programas por sus autores. Es decir, no necesitan de otros para propagarse.

Funcionan en grandes sistemas informáticos conectados mediante una red de comunicaciones, difundiéndose rápidamente a través de ésta. Estos programas hacen una gran utilización de los recursos de la red provocando un descenso en la velocidad de funcionamiento de la misma y bloqueos de los sistemas.

Los Gusanos más conocidos son:

- CHRISTMAS:

Actuó en una red de la IBM en Diciembre de 1987.

El mismo se manifestó a través de un mensaje que se observaba en la pantalla de la microcomputadora y que le pedía a los usuarios de la red que teclearan la cadena CHRISTMAS. Una vez tecleada la misma se observaba la figura correspondiente a un árbol de Navidades, y sin que el usuario se percatara, se ejecutaba un fichero Rexx que leía el directorio de direcciones de los buzones de los usuarios conectados a la red y se transmitía hacia cada uno de ellos. Muchos usuarios realizaron la misma operación en sus respectivas microcomputadoras y como resultado de esto ocurrió una sobrecarga de las líneas de la red, lo que provocó que se bloqueara.

- INTERNET:

El mismo actuó en una red de computadoras llamada Internet que trabaja sobre el Sistema Operativo UNIX. Se basó en puntos de entrada que existían hasta ese momento en el UNIX y consistió en un proceso que se enlazaba con una computadora remota, se transmitía hacia ella, averiguaba la palabra clave de usuarios conectados a la red y a través de las mismas lograba enlazarse con sus respectivas computadoras. Esta operación se desarrollaba nuevamente en éstas y así ocurrió el bloqueo de la red.

-Caballos de Troya:

Los Caballos de Troya son conocidos así porque su mecanismo de acción es similar al utilizado por los griegos para entrar en Troya. Sus autores los introducen en programas, generalmente muy utilizados por el dominio público, para que sean propagados a través de copias de los mismos que realicen los usuarios. Es decir, no son capaces de autopropagarse y han sido diseñados generalmente para destruir la información almacenada en los discos.

Los más conocidos son:

***AIDS INFORMATION DISKETTE**:*

Actuó en Diciembre de 1989. Consistió en un Software que fue enviado en disquetes de 5 1/4" a usuarios de la PC Bussines World. El mismo contenía información sobre el virus del SIDA y creaba durante el proceso de instalación subdirectorios y ficheros ocultos. Ocultaba un fichero AUTOEXEC.BAT creado por él, el cual llamaba a otro llamado AUTO.BAT que era el AUTOEXEC.BAT original, pero renombrado. Cada vez que el fichero AUTOEXEC.BAT era ejecutado (lo que generalmente ocurre durante el proceso de inicialización de la microcomputadora) se actualizaba un contador el cual una vez que tomaba el valor 90 provocaba la activación del programa Troyano contenido en el propio Software. Este encriptaba los nombres de los ficheros existentes en el disco y les agregaba el atributo de Oculto (Hidden). De esta forma, el usuario no podía trabajar con los mismos y cuando ejecutaba el comando DIR, parecía que los mismos no existían en el disco.

HAPPY99:

HAPPY99 es una aplicación Win32 que una vez instalado en un máquina es capaz de propagarse en forma de un anexo incluido en los mensajes de correo electrónico o en servicios de noticias que el usuario envía. Este proceso y el de la instalación del programa ocurren de manera oculta para el usuario, de ahí su clasificación como programa troyano. Es importante señalar que el proceso de instalación sólo ocurre si el usuario de la computadora ejecuta el programa HAPPY99.EXE, ya sea desde el mensaje recibido o una vez descargado en el disco duro o disquete.

Cuando el destinatario del mensaje ejecuta el anexo (un fichero que se nombra Happy99.exe con tamaño de 10,000 bytes) en una computadora con Sistema Operativo Windows9x, se observa en la pantalla una imagen animada correspondiente al lanzamiento de fuegos artificiales y de manera oculta, el troyano se instala en el sistema realizando las siguientes acciones:

En el subdirectorio sistema \Windows\System
Se copia con el nombre SKA.EXE.
Crea una DLL nombrada SKA.DLL.
Hace una copia de la DLL WSOCK32.DLL con el nombre WSOCK32.SKA.
Altera la DLL WSOCK32.DLL.
Y en el caso en que no pueda modificarla porque esté en uso:
Modifica los registros del sistema:
\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce SKA.EXE
con el fin de que este programa se ejecute cada vez que el sistema sea inicializado.

La modificación que realiza a WSOCK32.DLL consiste en agregar un código al final de la sección .text, sin alterar el tamaño del fichero, y hacer apuntar a las funciones "connect" y "send" que exporta la DLL hacia las respectivas rutinas en dicho código. Esto implica que cada vez que se ejecute una aplicación que importe éstas funciones de WSOCK32.DLL, se ejecute el código agregado por el troyano.

Cuando un usuario ejecuta un programa como el Outlook Express se activa WSOCK32.DLL y el troyano controla los eventos "connection" y "data sending" y monitorea los puertos SMTP (para correo) y NNTP (para noticias). Cuando el troyano detecta una conexión a uno de estos puertos carga la SKA.DLL que exporta las funciones "mail" y "news". En dependencia del puerto crea un

nuevo mensaje, al que anexa el programa troyano Happy99.exe, y lo envía a la dirección seleccionada por el usuario.

El troyano guarda estas direcciones en el fichero de texto LISTE.SKA en \WINDOWS\SYSTEM con el fin de no reenviar el anexo a las mismas.

-Bombas lógicas y de tiempo:

Las Bombas Lógicas y Bombas de Tiempo son casos particulares de Caballos de Troya. Bajo ciertas condiciones aparentan mal funcionamiento de la microcomputadora y provocan errores en el funcionamiento de los programas, que van haciéndose cada vez más frecuentes y dañinos hasta causar la destrucción total de la información.

Una Bomba de Tiempo se activa en una fecha u hora determinada, mientras que una Bomba Lógica se activa al darse una condición específica, como puede ser el número de accesos al disco, una determinada combinación de teclas que sea presionada, o cualquier otra condición que se le ocurra a su programador.

-Virus:

Los Virus Informáticos son aquellos programas capaces de reproducirse a sí mismos sin que el usuario esté consciente de ello. Estos se adicionan a programas de aplicación o documentos con macros, así como a componentes ejecutables del Sistema de forma tal que puedan tomar el control de este último durante la ejecución del programa infectado. El código del virus se ejecuta antes que el del programa original y una vez que haya realizado la acción para la que fue diseñado le da el control a este programa, con el objetivo de que el usuario no note su presencia. Un virus al igual que un programa puede realizar tantas cosas como su autor entienda. Por ejemplo:

- *-Borrar información.*
- *-Formatear un disco.*
- *-Alterar información.*
- *-Hacer más lenta la microcomputadora.*
- *- etc.*

Programas malignos:

Virus

Un virus en simplemente un programa. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco. De todas formas, dentro del término "virus informático" se suelen englobar varios tipos de programas, por lo que a continuación se da un pequeño repaso a cada uno de ellos poniendo de manifiesto sus diferencias. La clasificación es la siguiente:

Virus 'Puro'

Caballo de Troya

Bomba Lógica

Gusano o Worm

Todos estos programas tienen en común la creación de efectos perniciosos; sin embargo, no todos pueden ser considerados como virus propiamente dichos.

Virus Puro

Un verdadero virus tiene como características más importantes la capacidad de copiarse a sí mismo en soportes diferentes al que se encontraba originalmente, y por supuesto hacerlo con el mayor sigilo posible y de forma transparente al usuario; a este proceso de autorréplica se le conoce como "infección", de ahí que en todo este tema se utilice la terminología propia de la medicina: "vacuna", "tiempo de incubación", etc. Como soporte entendemos el lugar donde el virus se oculta, ya sea fichero, sector de arranque, partición, etc.

Un virus puro también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma trasparente al usuario.

Caballo de Troya

Al contrario que el virus puro, un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este ultimo. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

Bomba Lógica

Se trata simplemente de un programa maligno que permanece oculto en memoria y que solo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto (Viernes 13), cuando se ejecuta cierto programa o cierta combinación de teclas, etc.

Gusano o Worm

Por último, un gusano en un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.

La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas: por ejemplo, los virus como el Viernes 13 son capaces de infectar otros archivos, siendo así virus puro, pero también realizan su efecto destructivo cuando se da una condición concreta, la fecha Viernes 13, característica propia de una bomba lógica; por último, se oculta en programas ejecutables teniendo así una cualidad de Caballo de Troya. De ahí la gran confusión existente a este respecto.

Formas De Infección

Antes de nada, hay que recordar que un virus no puede ejecutarse por si solo, necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse a un programa portador necesita modificar la estructura de este, para que durante su ejecución pueda realizar una llamada al código del virus.

Las partes del sistema más susceptibles de ser infectadas son el sector de arranque de los disquetes, la tabla de partición y el sector de arranque del disco duro, y los ficheros ejecutables (.EXE y *.COM). Para cada una de estas partes tenemos un tipo de virus, aunque muchos son capaces de infectar por sí solos estos tres componentes del sistema.*

En los disquetes, el sector de arranque es una zona situada al principio del disco, que contiene datos relativos a la estructura del mismo y un pequeño programa, que se ejecuta cada vez que arrancamos desde disquete.

En este caso, al arrancar con un disco contaminado, el virus se queda residente en memoria RAM, y a partir de ahí, infectara el sector de arranque de todos los disquetes a los que se accedan, ya sea al formatear o al hacer un DIR en el disco, dependiendo de cómo esté programado el virus).

El proceso de infección consiste en sustituir el código de arranque original del disco por una versión propia del virus, guardando el original en otra parte del disco; a menudo el virus marca los sectores donde guarda el boot original como en mal estado, protegiéndolos así de posibles accesos, esto suele hacerse por dos motivos: primero, muchos virus no crean una rutina propia de arranque, por lo que una vez residentes en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y así aparentar que se ha iniciado el sistema como siempre, con normalidad. Segundo, este procedimiento puede ser usado como técnica de ocultamiento.

Normalmente un virus completo no cabe en los 512 bytes que ocupa el sector de arranque, por lo que en éste suele copiar una pequeña parte de si mismo, y el resto lo guarda en otros sectores del disco, normalmente los últimos, marcándolos como defectuosos. Sin embargo, puede ocurrir que alguno de los virus no marquen estas zonas, por lo que al llenar el disco estos sectores pueden ser sobrescritos y así dejar de funcionar el virus.

La tabla de partición esta situada en el primer sector del disco duro, y contiene una serie de bytes de información de cómo se divide el disco y un pequeño programa de arranque del sistema. Al igual que ocurre con el boot de los disquetes, un virus de partición suplanta el código de arranque original por el suyo propio; así, al

arrancar desde disco duro, el virus se instala en memoria para efectuar sus acciones. También en este caso el virus guarda la tabla de partición original en otra parte del disco, aunque algunos la marcan como defectuosa y otros no. Muchos virus guardan la tabla de partición y a ellos mismos en los últimos sectores de disco, y para proteger esta zona, modifican el contenido de la tabla para reducir el tamaño lógico del disco. De esta forma el DOS no tiene acceso a estos datos, puesto que ni siquiera sabe que esta zona existe.

Casi todos los virus que afectan la partición también son capaces de hacerlo en el boot de los disquetes y en los ficheros ejecutables; un virus que actuara sobre particiones de disco duro tendría un campo de trabajo limitado, por lo que suelen combinar sus habilidades.

Con todo, el tipo de virus que más abunda es el de fichero; en este caso usan como vehículo de expansión los archivos de programa o ejecutables, sobre todo .EXE y . COM, aunque también a veces .OVL, .BIN y .OVR. AL ejecutarse un programa infectado, el virus se instala residente en memoria, y a partir de ahí permanece al acecho; al ejecutar otros programas, comprueba si ya se encuentran infectados. Si no es así, se adhiere al archivo ejecutable, añadiendo su código al principio y al final de éste, y modificando su estructura de forma que al ejecutarse dicho programa primero llame al código del virus devolviendo después el control al programa portador y permitiendo su ejecución normal.

Este efecto de adherirse al fichero original se conoce vulgarmente como "engordar" el archivo, ya que éste aumenta de tamaño al tener que albergar en su interior al virus, siendo esta circunstancia muy útil para su detección. De ahí que la inmensa mayoría de los virus sean programados en lenguaje ensamblador, por ser el que genera el código más compacto, veloz y de menor consumo de memoria; un virus no seria efectivo si fuera fácilmente detectable por su excesiva ocupación en memoria, su lentitud de trabajo o por un aumento exagerado en el tamaño de los archivos infectados. No todos los virus de fichero quedan residentes en memoria, si no que al ejecutarse se portador, éstos infectan a otro archivo, elegido de forma aleatoria de ese directorio o de otros.

Efectos Destructivos De Los Virus

Los efectos perniciosos que causan los virus son variados; entre éstos se encuentran el formateo completo del disco duro, eliminación de la tabla de partición, eliminación de archivos, ralentización del sistema hasta limites exagerados, enlaces de archivos destruidos, archivos de datos y de programas corruptos, mensajes o efectos extraños en la pantalla, emisión de música o sonidos.

Formas De Ocultamiento

Un virus puede considerarse efectivo si, además de extenderse lo más ampliamente posible, es capaz de permanecer oculto al usuario el mayor tiempo posible; para ello se han desarrollado varias técnicas de ocultamiento o sigilo. Para que estas técnicas sean efectivas, el virus debe estar residente en memoria, puesto que debe monitorizar el funcionamiento del sistema operativo. La base principal del funcionamiento de los virus y de las técnicas de ocultamiento, además de la condición de programas residentes, la intercepción de interrupciones. El DOS y los programas de aplicación se comunican entre sí mediante el servicio de interrupciones, que son como subrutinas del sistema operativo que proporcionan una gran variedad de funciones a los programas. Las interrupciones se utilizan, por ejemplo, para leer o escribir sectores en el disco, abrir ficheros, fijar la hora del sistema, etc. Y es aquí donde el virus entra en acción, ya que puede sustituir

alguna interrupción del DOS por una suya propia y así, cuando un programa solicite un servicio de esa interrupción, recibirá el resultado que el virus determine.

Entre las técnicas más usuales cabe destacar el ocultamiento o stealth, que esconde los posibles signos de infección del sistema. Los síntomas más claros del ataque de un virus los encontramos en el cambio de tamaño de los ficheros, de la fecha en que se crearon y de sus atributos, y en la disminución de la memoria disponible.

Estos problemas son indicadores de la posible presencia de un virus, pero mediante la técnica stealth es muy fácil (siempre que se encuentre residente el virus) devolver al sistema la información solicitada como si realmente los ficheros no estuvieran infectados. Por este motivo es fundamental que cuando vayamos a realizar un chequeo del disco duro arranquemos el ordenador con un disco de sistema totalmente limpio.

La autoencriptación o self-encryption es una de las técnicas víricas más extendidas. En la actualidad casi todos los nuevos ingenios destructivos son capaces de encriptarse cada vez que infectan un fichero, ocultando de esta forma cualquier posible indicio que pueda facilitar su búsqueda. No obstante, todo virus encriptado posee una rutina de desencriptación, rutina que es aprovechada por los antivirus para remotoizar el origen de la infección.

El mayor avance en técnicas de encriptación viene dado por el polimorfismo. Gracias a él un virus no sólo es capaz de encriptarse sino que además varía la rutina empleada cada vez que infecta un fichero. De esta forma resulta imposible encontrar coincidencias entre distintos ejemplares del mismo virus, y ante esta técnica el tradicional método de búsqueda de cadenas características se muestra inútil.

Otra técnica básica de ocultamiento es la intercepción de mensajes de error del sistema. Supongamos que un virus va a infectar un archivo de un disco protegido contra escritura; al intentar escribir en el obtendríamos el mensaje: "Error de protección contra escritura leyendo unidad A Anular, Reintentar, Fallo?", por lo que descubriríamos el anormal funcionamiento de nuestro equipo. Por eso, al virus le basta con redireccionar la interrupción a una rutina propia que evita la salida de estos mensajes, consiguiendo así pasar desapercibido.

Prevención, Detección Y Eliminación

Una buena política de prevención y detección nos puede ahorrar sustos y desgracias. Las medidas de prevención pasan por el control, en todo momento, del software ya introducido o que se va a introducir en nuestro ordenador, comprobando la fiabilidad de su fuente. Esto implica la actitud de no aceptar software no original, ya que el pirateo es una de las principales fuentes de contagio de un virus, siendo también una practica ilegal y que hace mucho daño a la industria del software.

Por supuesto, el sistema operativo, que a fin de cuentas es el elemento software más importante del ordenador, debe ser totalmente fiable; si éste se encuentra infectado, cualquier programa que ejecutemos resultara también contaminado. Por eso, es imprescindible contar con una copia en disquetes del sistema operativo, protegidos éstos contra escritura; esto ultimo es muy importante, no solo con el S.O. sino con el resto de disquetes que poseamos. Es muy aconsejable mantenerlos siempre protegidos, ya que un virus no puede escribir en un disco protegido de esta forma. Por último es también imprescindible poseer un buen software antivirus, que detecte y elimine cualquier tipo de intrusión en el sistema.

Windows 95

La existencia de un nuevo sistema operativo con bastantes diferencias técnicas respecto a desarrollos anteriores merece un estudio especial para comprobar cómo reacciona ante virus conocidos y el tipo de protección que ofrece.

Ante la infección del sector de arranque (boot sector) Windows 95 reacciona sorprendentemente bien, o al menos mucho mejor que sus antecesores. De hecho, frente a cualquier modificación del sector de arranque el sistema presenta un mensaje durante la inicialización. Nos anuncia que algo se ha cambiado y que la causa de tal hecho puede ser un virus de boot, aunque no necesariamente.

También debemos precisar que si hay un error remotoizado en la tabla de particiones el sistema nos da el mismo aviso que en el caso anterior, lo que sin duda puede ser motivo de confusión. En general siempre que Windows 95 se dé cuenta de un fallo en el sistema de ficheros que le impida trabajar con la VFAT a pleno rendimiento, se inicia con el «Sistema de archivos en modo compatibilidad MS-DOS», sugiriendo como posible causa el ataque de un virus.

Que Microsoft achaque estos fallos a la acción de un virus es una solución un tanto drástica, ya que una falsa alarma puede ser tan peligrosa como la presencia real de un ingenio vírico.

Problemas Con Windows 95

El nuevo sistema operativo de Microsoft ha creado más de un problema a las empresas de seguridad, y no sólo por el trabajo adicional de reprogramar sus desarrollos para adecuarse a las características el nuevo entorno, sino también por algunos fallos de diseño propios de W95.

En MS-DOS (también en Windows 3.1) se podían solicitar informes al sistema de todas las actividades realizadas, y todo ello en tiempo real. Es decir, a través de un residente era factible conseguir información sobre acciones como abrir, leer y escribir en ficheros, cambio de atributos, etc. Cuando hablamos de tiempo real nos referimos al hecho de recibir la información solicitada en el mismo momento en que se realiza la acción.

Desgraciadamente en W95 la cosa varía, ya que a pesar de tratarse de un sistema operativo multitarea no se envían informes en tiempo real, sino cada determinados intervalos de tiempo o cuando el procesador está menos ocupado. Por este motivo la programación de un controlador capaz de monitorizar el sistema con seguridad es muy difícil, ya que el antivirus recibe la información de que se va a producir una infección cuando el fichero ya está infectado.

A pesar de ello, gran parte de los antivirus para Windows 95 incluyen drivers virtuales o controladores VxD capaces de mantener bajo su atenta mirada el sistema en todo momento. De todas formas, la realización de un driver de este tipo para W95 no es una tarea sencilla y acarrea bastantes problemas. Además, es importante que la protección se ofrezca en todo momento, es decir, que se controle la interfaz gráfica, la versión previa del sistema operativo, las sesiones DOS y el modo MS-DOS 7.0 (arrancando sin la interfaz o al apagar el sistema). Desde luego todas estas acciones no son controlables por un driver VxD exclusivamente.

Virus De Macros

Esta entre las novedades surgidas últimamente en el mundo de los virus, aunque no son totalmente nuevos, parece que han esperado hasta 1995 para convertirse en una peligrosa realidad. Por desgracia, ya existe un número importante de virus de este tipo catalogados, que han sido escritos en WordBasic, el potente lenguaje incluido en Microsoft Word.

Estos virus sólo afectan a los usuarios de Word para Windows y consisten en un conjunto de macros de este procesador de textos. Aunque el peligro del virus se restringe a los usuarios de Word, tiene una importante propagación ya que puede infectar cualquier texto, independientemente de la plataforma bajo la que éste se ejecute: Mac, Windows 3.x, Windows NT, W95 y OS/2. Este es el motivo de su peligrosidad, ya que el intercambio de documentos en disquete o por red es mucho más común que el de ejecutables.

El primer virus de este tipo que salió a la luz se llamaba «WordMacro/DMV» y era inofensivo, ya que sólo anunciaba su presencia y guardaba un informe de sus acciones. Escrito por Joel McNamara para el estudio de los virus de macros, fue desarrollado en 1994 pero su autor guardó el resultado hasta que observó la aparición del virus conocido por «WordMacro/Concept». Tras ello, McNamara decidió hacer público su desarrollo esperando que la experiencia adquirida sirviera de enseñanza para todos los usuarios. Y aunque probablemente tenga un efecto negativo, McNamara ha publicado también las pautas para crear virus que afecten a los ficheros de Exel.

«WinMacro/Concept», también conocido como «WW6Infector», «WBMV-Word Basic Macro Virus» o «WWW6 Macro», no es demasiado molesto, ya que al activarse infecta el fichero «normal.dot» y sólo muestra en pantalla un cuadro de diálogo con el texto «1». Microsoft ya tiene disponible un antivirus llamado «prank.exe» que distribuye gratuitamente entre sus usuarios registrados, pero que también puede encontrarse en numerosas BBS, Internet o Compuserve.

Sin embargo, la evolución de este tipo de virus sigue su camino y ya se han detectado dos nuevas creaciones llamadas «WordMacro/Nuclear» y «WordMacro/Colors». El primero de ellos puede llegar a introducir un virus tradicional en el sistema o modificar la salida impresa o por fax en determinados momentos. El «WordMacro/Colors», también conocido por Rainbow o arco iris, cambia (cada 300 ejecuciones de la macro) la configuración de colores de Windows.

De momento la macros conocidas para Word no son capaces de infectar las versiones nacionales del programa, los usuarios españoles pueden estar tranquilos ya que los comandos del lenguaje de macros han sido traducidos al castellano y las macros creadas con versiones en inglés no funcionan. No obstante, siempre es posible que alguien traduzca el virus o cree uno nuevo. Por último, aclarar que aunque otros procesadores de texto como WordPerfect o AmiPro son capaces de leer documentos escritos con Word, en estos casos el virus no entra en acción por lo que no se corre ningún peligro.

Virus De Nueva Hornada

Aunque la principal novedad vírica ha venido de la mano de los virus de macros, se han remotoizado en España nuevas creaciones que merece la pena conocer para luchar contra ellas de manera efectiva.

Se ha descubierto un virus que incrementa los ficheros en 1.376 bytes simplemente por abrirlos. Una vez que el virus está en memoria basta con una

orden COPY o TYPE para que infecte el fichero. Su acción pasa por borrar los ficheros de validación de antivirus como CPAV o Microsoft.

Muchos usuarios españoles se han visto afectados por el virus 1.099, que si bien no es nuevo, es la primera vez que aparece en nuestro país. Este virus se queda residente en RAM e infecta los ficheros ".EXE" aumentando su tamaño en 1.099 bytes. Ha llegado a España a través de los discos de drivers que acompañaban a una pequeña partida de tarjeta Cirrus Logic, y se puede identificar ya que en los ficheros VER se señala como «BIN3, Ver1.2» con fecha 27-5-94.

Por su parte, el virus MiliKK infecta en primer lugar la tabla de partición para desde ahí comenzar con su siniestro cometido. Emplea técnicas stealth por lo que no podremos ver cómo se queda residente en la RAM, aumenta los ficheros ".COM" en 1.020 bytes e incrementa la fecha de los ficheros infectados en 100 años. Además, cada vez que se enciende el PC se visualiza el mensaje "M I L I K K".

Por último, en Sevilla se ha detectado el virus DelCMOS, que como su nombre indica borra el contenido de la CMOS cuando se arranca desde un disco duro con la partición afectada. Aunque borra la información sobre la configuración de disqueteras, sólo es dañino con los datos de los discos duros correspondientes al tipo 47.

Virus En Internet

En ocasiones se propagan rumores que dan por cierto noticias de dudosa procedencia. Más o menos esto es lo que ha sucedido de un tiempo a esta parte con el virus por correo electrónico de Internet conocido por Good Times. Lógicamente las primeras noticias de esta maligna creación aparecieron en la «red de redes», en un mensaje alarmante que decía que si algún usuario recibía un mensaje con el tema «Good Times» no debía abrirlo o grabarlo si no quería perder todos los datos de su disco duro. Posteriormente el mensaje recomendaba que se informara a todo el mundo y se copiara el aviso en otros lugares. En esta ocasión el rumor es totalmente falso, aunque todavía sigue existiendo gente que se lo cree y no es raro encontrar en algún medio de comunicación electrónica nuevo reenvíos del mensaje original. De hecho, es totalmente inviable la posibilidad de una infección vía correo electrónico.

El riesgo de contraer un virus en la Internet es menor que de cualquier otra manera, tanto los mensajes de correo, como las página WEB transfieren datos. Sólo si se trae un software por la red y lo instala en su máquina puede contraer un virus

Software Antivirus

Para combatir la avalancha de virus informáticos se creó el software antivirus. Estos programas suelen incorporar mecanismos para prevenir, detectar y eliminar virus. Para la prevención se suelen usar programas residentes que alertan al usuario en todo momento de cualquier acceso no autorizado o sospechoso a memoria o a disco, por lo que resultan sumamente útiles al impedir la entrada del virus y hacerlo en el momento en que este intenta la infección, facilitándonos enormemente la localización del programa maligno. Sin embargo presentan ciertas desventajas, ya que al ser residentes consumen memoria RAM, y pueden también resultar incompatibles con algunas aplicaciones. Por otro lado, pueden llegar a resultar bastante molestos, puesto que por lo general suelen interrumpir nuestro trabajo habitual con el ordenador avisándonos de intentos de acceso a memoria o a disco que en muchos casos provienen de programas legítimos. A pesar de todo,

son una medida de protección excelente y a ningún usuario debería faltarle un programa de este tipo.

A la hora de localizar virus, los programas usados sin los detectores o scanners. Normalmente estos programas chequean primero la memoria RAM, después las zonas criticas del disco como el boot o partición, y por ultimo los ficheros almacenados en él.

Los productos antivirus han mejorado considerablemente sus algoritmos de búsqueda, aunque en la actualidad la exploración de cadenas sigue siendo la técnica más empleada. Pero el aumento imparable del número de virus y las técnicas de camuflaje y automodificación que suelen emplear hacen que la búsqueda a través de una cadena genérica sea una tarea cada vez más difícil. Por ello, es cada día es más frecuente el lanzamiento de antivirus con técnicas heurísticas.

La detección heurística es una de las fórmulas más avanzadas de remotoización de virus. La búsqueda de virus mediante esta técnica se basa en el desensamblado del código del programa que se intenta analizar con el objetivo de encontrar instrucciones (o un conjunto de ellas) sospechosas. Sin duda, lo mejor es disponer de un antivirus que combine la búsqueda de cadenas características y además cuente con técnicas heurísticas.

Gracias a la heurística se buscan programas que puedan quedarse residentes o que sean capaces de capturar aplicaciones que se estén ejecutando, código preparado para mover o sobreescribir un programa en memoria, código capaz de automodificar ejecutables, rutinas de encriptación y desencriptación, y otras actividades propias de los virus.

Aunque las técnicas heurísticas han representado un gran avance en la detección de virus desconocidos, presentan un gran inconveniente: es muy alta la posibilidad de obtener «falsos positivos y negativos». Se produce un «falso positivo» cuando el antivirus anuncia la presencia de un virus que no es tal, mientras que se llama «falso negativo» cuando piensa que el PC esta limpio y en realidad se encuentra infectado.

¿Que Debemos Buscar En Un Antivirus?

A la hora de decidirnos por un antivirus, no debemos dejarnos seducir por la propaganda con mensajes como "detecta y elimina 56.432 virus". Realmente existen miles de virus, pero en muchísmos casos son mutaciones y familias de otros virus; esto está bien, pero hay que tener en cuenta que una inmensa mayoría de virus no han llegado ni llegaran a nuestro país.

Por lo que de poco nos sirve un antivirus que detecte y elimine virus muy extendidos en América y que desconozca los más difundidos en España. Por tanto, estaremos mejor protegidos por un software que, de alguna forma, esté más "especializado" en virus que puedan detectarse en nuestro país. Por ejemplo "Flip", "Anti Tel", "Barrotes", "Coruña", etc. Por otro lado, hemos de buscar un software que se actualice el mayor numero posible de veces al año; puesto que aparecen nuevos virus y mutaciones de otros ya conocidos con mucha frecuencia, el estar al día es absolutamente vital.

Cómo Reaccionar Ante Una Infección

La prevención y la compra de un buen antivirus son las mejores armas con las que cuenta el usuario ante el ataque de los virus. Sin embargo, siempre cabe la

posibilidad de que en un descuido se introduzca un inquilino no deseado en el PC. Ante esta situación lo primero que debemos hacer es arrancar el ordenador con un disco de sistema totalmente libre de virus. Posteriormente deberemos pasar un antivirus lo más actualizado posible, ya que si es antiguo corremos el riesgo de que no remotoice mutaciones recientes o nuevos virus.

En el disco de sistema limpio (que crearemos con la orden «format a: /s») incluiremos utilidades como «mem.exe», «chkdsk.exe», «sys.com», «fdisk.exe» y todos los controladores para que el teclado funcione correctamente. Si disponemos de dos o más antivirus es muy recomendable pasarlos todos para tener mayor seguridad a la hora de inmunizar el PC.

Si la infección se ha producido en el sector de arranque podemos limpiar el virus con la orden «sys c:», siempre y cuando hayamos arrancado con el disquete antes mencionado. Para recuperar la tabla de particiones podemos ejecutar «fdisk /mbr».

Software AntiVirus Comercial

Análisis heurístico

Hay que señalar una marcada mejoría en las técnicas de detección heurísticas, que aunque en determinadas condiciones siguen provocando «falsos positivos», muestran una gran efectividad a la hora de remotoizar virus desconocidos. En este apartado debemos destacar al ThunderByte, ya que la técnica heurística de este antivirus le ha permitido detectar 42 de los virus no remotoizados mediante el método adicional. De hecho, la mayoría de estos virus son desarrollos nacionales de reciente aparición, por lo que o ha habido tiempo de incluirlos en la última versión. Además, este producto destaca por una relación de «falsos positivos» realmente baja.

Otros productos que permiten la detección heurística son Artemis Profesional, Dr. Solomon´s y F-Prot 2.20. En todos los casos esta técnica ha servido para aumentar el porcentaje de virus detectados, aunque de esta forma no se identifica el virus, sino que sólo se sospecha de su presencia. Por otra parte, el Dr. Solomon´s combina perfectamente una gran base de datos de virus conocidos con su análisis heurístico.

Búsqueda específica

Aunque algunos antivirus engordan su porcentaje de efectividad gracias a técnicas de remotoización genérica (heurísticamente), muchos usuarios pueden preferir la seguridad aportada por un sistema específico que identifique, e incluso elimine, sin problemas ni dudas el mayor número de virus posible.

Los usuarios más inexpertos probablemente no sepan enfrentarse a las alarmas producidas por el análisis heurístico, por lo que en todos los antivirus es posible realizar la exploración de las unidades de disco sin dicha posibilidad. En tal caso será necesario conocer cuál es la efectividad del producto prescindiendo de tal análisis.

Por este motivo, si nos basamos en técnicas tradicionales como la búsqueda de cadenas y dejamos a un lado métodos heurísticos tenemos que reconocer que el producto dominante es el antivirus Artemis Profesional 4.0,. tras él, el conocido Scan de McAfee demuestra el porqué de su prestigio, seguido muy de cerca por el F-Prot.

Virus nacionales

En todos los casos han sido los virus de procedencia de nacional y aquellos de aparición más reciente los que han planteado mayores problemas de identificación. Por este motivo, los productos Artemis y Anyware (desarrollados por empresas españolas) no han fallado en la detección de ingenios patrios como los virus Raquel, Maripuri, Mendoza, Diálogos, RNE, Currante y nuevas mutaciones de Barrotes.

Los productos internacionales muestran buenos índices globales de detección, aunque todos fallan al encontrarse con virus españoles. Esta carencia, sin embargo, se ve solventada en los antivirus con análisis heurístico, que si bien no son capaces de identificar el virus sí logran detectar su presencia.

Inseguridad Informática

*El 5 de noviembre de 1988 quedó señalado para siempre en la historia de la "inseguridad" informática. El personal que estaba trabajando en los ordenadores de la Universidad de Cornell vieron sorprendidos y asustados como sus computadoras, uno a uno e irremediablemente, quedaban bloqueados. Estos eran los primeros síntomas de una terrible epidemia "bloqueante" que atacó seguida y rápidamente a las Universidades de Stanford, California, Princeton, al propio MIT, a la Rand Corporation, a la NASA, hasta un total aproximado de 6.000 ordenadores, ¡6.0000!, que permanecieron inactivos durante dos o tres días, con un coste estimado de 96 millones de dólares (más de 10.000 millones de pesetas). Causa: un simple y único gusano "**worm**", activado sólo una vez, resultado de un sencillo trabajo de autoprácticas de Robert T. Morris, "bienintencionado einofensivo" estudiante de la Universidad de Cornell. Eficiencia demostrada. Un solo Worm, 6.000 ordenadores inactivos, 96.000.000 de dólares de pérdidas.*

La epidemia vírica ha alcanzado en pocos años una magnitud escalofriante. Según el experto virólogo Vesselin V. Bontchev, nacen cada día 2 o 3 virus.

Las amenazas a la informática no terminan con los virus. Los "hackers" constituyen una potente fuerza de ataque a la seguridad informática. Personas dotadas de probados conocimientos, utilizando tecnologías de alto nivel, agrupados en clubes, celebrando Congresos Internacionales, con seminarios y clases: su nivel de peligrosidad alcanza altísimos valores.

Fraudes, sabotajes, espionaje comercial e industrial, vandalismo, terrorismo, desastres naturales como el fuego y el agua, amenazan constantemente a nuestros sistemas de proceso de datos, convirtiendo a la Seguridad Informática en un importantísimo objetivo a alcanzar en la empresa, toda vez que está en peligro su más preciado tesoro: la información.

Por otra parte, las empresas han cambiado su estilo de trabajo, apoyándose en y dependiendo fuertemente del sistema informático y de las telecomunicaciones. La ofimática, las Bases de Datos corporativas o distribuidas, el EDI, el SWIFT, el homebaking, la necesidad de sistemas y comunicaciones "trusted", los sistemas distribuidos, etc., colocan a la Seguridad Informática en la cúspide de los objetivos a alcanzar en la empresa.

Si no existe seguridad no hay calidad en la Información, si ésta no es segura, exacta, precisa y rabiosamente actual, es decir, si no es de calidad, las operaciones y decisiones serán equivocadas y si éstas son erróneas la empresa muere.

2DA PARTE

Seguridad informática

Virus informáticos

Cómo protegerse Marzo - 2000

Índice general

Introducción

Los virus informáticos son una de los principales riesgos de seguridad para los sistemas, ya sea que estemos hablando de un usuario hogareño que utiliza su máquina para trabajar y conectarse a Internet o una empresa con un sistema informático importante que debe mantener bajo constante vigilancia para evitar pérdidas causadas por los virus.

Un virus se valdrá de cualquier técnica conocida –o poco conocida- para lograr su cometido. Así, encontraremos virus muy simples que sólo se dedican a presentar mensajes en pantalla y algunos otros mucho más complejos que intentan ocultar su presencia y atacar en el momento justo.

A lo largo de este trabajo haremos referencia a qué es exactamente un virus, cómo trabaja, algunos tipos de virus y también cómo combatirlos. Nos proponemos a dar una visión general de los tipos de virus existentes para poder enfocarnos más en cómo proteger un sistema informático de estos atacantes y cómo erradicarlos una vez que lograron penetrar.

Conceptos básicos sobre virus informáticos

¿Qué es un virus informático?

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras

computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.

Un virus tiene tres características primarias:

-
- *Es dañino. Un virus informático siempre causa daños en el sistema que infecta, pero vale aclarar que el hacer daño no significa que valla a romper algo. El daño puede ser implícito cuando lo que se busca es destruir o alterar información o pueden ser situaciones con efectos negativos para la computadora, como consumo de memoria principal, tiempo de procesador, disminución de la performance.*
-
- *Es autorreproductor. A nuestro parecer la característica más importante de este tipo de programas es la de crear copias de sí mismo, cosa que ningún otro programa convencional hace. Imagínense que si todos tuvieran esta capacidad podríamos instalar un procesador de textos y un par de días más tarde tendríamos tres de ellos o más. Consideramos ésta como una característica propia de virus porque los programas convencionales pueden causar daño, aunque sea accidental, sobrescribiendo algunas librerías y pueden estar ocultos a la vista del usuario, por ejemplo: un programita que se encargue de legitimar las copias de software que se instalan.*
-
- *Es subrepticio. Esto significa que utilizará varias técnicas para evitar que el usuario se de cuenta de su presencia. La primera medida es tener un tamaño reducido para poder disimularse a primera vista. Puede llegar a manipular el resultado de una petición al sistema operativo de mostrar el tamaño del archivo e incluso todos sus atributos.*

  La verdadera peligrosidad de un virus no está dada por su arsenal de instrucciones maléficas, sino por lo crítico del sistema que está infectando. Tomemos como ejemplo un virus del tipo conejo. Si este infectara una computadora hogareña la máquina se colgaría, pudiendo luego reiniciarla con un disquete de arranque limpio y con un antivirus para eliminar el virus. Si afectara a un servidor de una PyME, posiblemente el sistema informático de la empresa dejaría de funcionar por algún tiempo significando una pérdida de horas máquina y de dinero. Pero si este virus infectara una máquina industrial como una grúa robótica o algún aparato utilizado en medicina como una máquina de rayos láser para operar, los costos serían muy altos y posiblemente se perderían vidas humanas. ¿Qué pasaría si se alteraran los registros médicos de una persona de forma que se mostrara un tipo de sangre o factor RH diferente? El paciente podría morir. ¿Qué pasaría si el dígito 4 millonésimo en los cálculos para el aterrizaje de una misión espacial se alterara en un factor del 0.001 por 100? Los astronautas morirían.

Los virus informáticos no pueden causar un daño directo sobre el hardware. No existen instrucciones que derritan la unidad de disco rígido o que hagan estallar el cañon de un monitor. En su defecto, un virus puede hacer ejecutar operaciones que reduzcan la vida útil de los dispositivos. Por ejemplo: hacer que la placa de sonido envíe señales de frecuencias variadas con un volumen muy alto para averiar los parlantes, hacer que la impresora desplace el cabezal de un lado a otro o que lo golpee contra uno de los lados, hacer que las unidades de almacenamiento muevan a gran velocidad las cabezas de L / E para que se desgasten. Todo este tipo de cosas son posibles aunque muy poco probables y por lo general los virus prefieren atacar los archivos y no meterse con la parte física.

¿Quién los hace?

En primer lugar debemos decir que los virus informáticos están hechos por personas con conocimientos de programación pero que no son necesariamente genios de las computadoras. Tienen conocimientos de lenguaje ensamblador y de cómo funciona internamente la computadora. De hecho resulta bastante más difícil hacer un programa "en regla" como sería un sistema de facturación en donde hay que tener muchísimas más cosas en cuenta que en un simple virus que aunque esté mal programado sería suficiente para molestar al usuario.

En un principio estos programas eran diseñados casi exclusivamente por los hackers y crackers que tenían su auge en los Estados Unidos y que hacían temblar a las compañías con solo pensar en sus actividades. Tal vez esas personas lo hacían con la necesidad de demostrar su creatividad y su dominio de las computadoras, por diversión o como una forma de manifestar su repudio a la sociedad que los oprimía. Hoy en día, resultan un buen medio para el sabotaje corporativo, espionaje industrial y daños a material de una empresa en particular.

Un poco de historia

Los virus tienen la misma edad que las computadoras. Ya en 1949 John Von Neumann, describió programas que se reproducen a sí mismos en su libro "Teoría y Organización de Autómatas Complicados". Es hasta mucho después que se les comienza a llamar como virus. La característica de auto-reproducción y mutación de estos programas, que las hace parecidas a las de los virus biológicos, parece ser el origen del nombre con que hoy los conocemos.

Antes de la explosión de la micro computación se decía muy poco de ellos. Por un lado, la computación era secreto de unos pocos. Por otro lado, las entidades gubernamentales, científicas o militares, que vieron sus equipos atacados por virus, se quedaron muy calladas, para no demostrar la debilidad de sus sistemas de seguridad, que costaron millones, al bolsillo de los contribuyentes. Las empresa privadas como Bancos, o grandes corporaciones, tampoco podían decir nada, para no perder la confianza de sus clientes o accionistas. Lo que se sabe de los virus desde 1949 hasta 1989, es muy poco.

Se reconoce como antecedente de los virus actuales, un juego creado por programadores de la empresa AT&T, que desarrollaron la primera versión del sistema operativo Unix en los años 60. Para entretenerse, y como parte de sus investigaciones, desarrollaron un juego llamado "Core Wars", que tenía la capacidad de reproducirse cada vez que se ejecutaba. Este programa tenía instrucciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento. Al mismo tiempo, desarrollaron un programa llamado "Reeper", que destruía las copias hechas por Core Wars. Un antivirus o antibiótico, como hoy se los conoce. Conscientes de lo peligroso del juego, decidieron mantenerlo en secreto, y no hablar más del tema. No se sabe si esta decisión fue por iniciativa propia, o por órdenes superiores.

En el año 1983, el Dr. Ken Thomson, uno de los programadores de AT&T, que trabajó en la creación de "Core Wars", rompe el silencio acordado, y da a conocer la existencia del programa, con detalles de su estructura.

La Revista Scientific American a comienzos de 1984, publica la información completa sobre esos programas, con guías para la creación de virus. Es el punto de partida de la vida pública de estos programas, y naturalmente de su difusión sin control, en las computadoras personales.

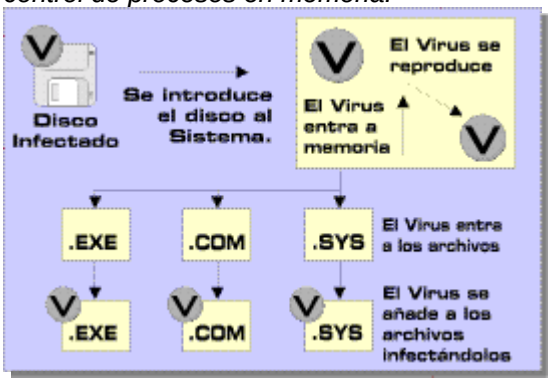
Por esa misma fecha, 1984, el Dr. Fred Cohen hace una demostración en la Universidad de California, presentando un virus informático residente en una PC. Al Dr. Cohen se le conoce hoy día, como "el padre de los virus". Paralelamente aparece en muchas PCs un virus, con un nombre similar a Core Wars, escrito en Small-C por un tal Kevin Bjorke, que luego lo cede a dominio público. ¡La cosa comienza a ponerse caliente!

El primer virus destructor y dañino plenamente identificado que infecta muchas PC's aparece en 1986. Fue creado en la ciudad de Lahore, Paquistán, y se le conoce con el nombre de BRAIN. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Supercalc o Wordstar, por suma bajísimas. Los turistas que visitaban Paquistán, compraban esas copias y las llevaban de vuelta a los EE.UU. Las copias pirateadas llevaban un virus. Fue así, como infectaron mas de 20,000 computadoras. Los códigos del virus Brain fueron alterados en los EE.UU., por otros programadores, dando origen a muchas versiones de ese virus, cada una de ellas peor que la precedente. Hasta la fecha nadie estaba tomando en serio el fenómeno, que comenzaba a ser bastante molesto y peligroso.

En 1987, los sistemas de Correo Electrónico de la IBM, fueron invadidos por un virus que enviaba mensajes navideños, y que se multiplicaba rápidamente. Ello ocasionó que los discos duros se llenaran de archivos de origen viral, y el sistema se fue haciendo lento, hasta llegar a paralizarse por mas de tres días. La cosa había llegado demasiado lejos y el Big Blue puso de inmediato a trabajar en los virus su Centro de Investigación Thomas J. Watson, de Yorktown Heights, NI.
Las investigaciones del Centro T. J. Watson sobre virus, son puestas en el dominio público por medio de Reportes de Investigación, editados periódicamente, para beneficio de investigadores y usuarios.
El virus Jerusalem, según se dice creado por la Organización de Liberación Palestina, es detectado en la Universidad Hebrea de Jerusalem a comienzos de 1988. El virus estaba destinado a aparece el 13 de Mayo de 1988, fecha del 40 aniversario de la existencia de Palestina como nación. Una interesante faceta del terrorismo, que ahora se vuelca hacia la destrucción de los sistemas de cómputo, por medio de programas que destruyen a otros programas.
El 2 de Noviembre del '88, dos importantes redes de EE.UU. se ven afectadas seriamente por virus introducidos en ellas. Mas 6,000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados se ven atacados.
Por 1989 la cantidad de virus detectados en diferentes lugares sobrepasan los 100, y la epidemia comienza a crear situaciones graves. Entre las medidas que se toma, para tratar de detener el avance de los virus, es llevar a los tribunales a Robert Morís Jr. acusado de ser el creador de un virus que infectó a computadoras del gobierno y empresas privadas. Al parecer, este muchacho conoció el programa Core Wars, creado en la AT&T, y lo difundió entre sus amigos. Ellos se encargaron de diseminarlo por diferentes medios a redes y equipos. Al juicio se le dio gran publicidad, pero no detuvo a los creadores de virus.
La cantidad de virus que circula en la actualidad no puede llegar a ser precisada pero para tener una idea los últimos antivirus pueden identificar alrededor de cincuenta mil virus (claro que en este valor están incluidos los clones de un mismo virus).

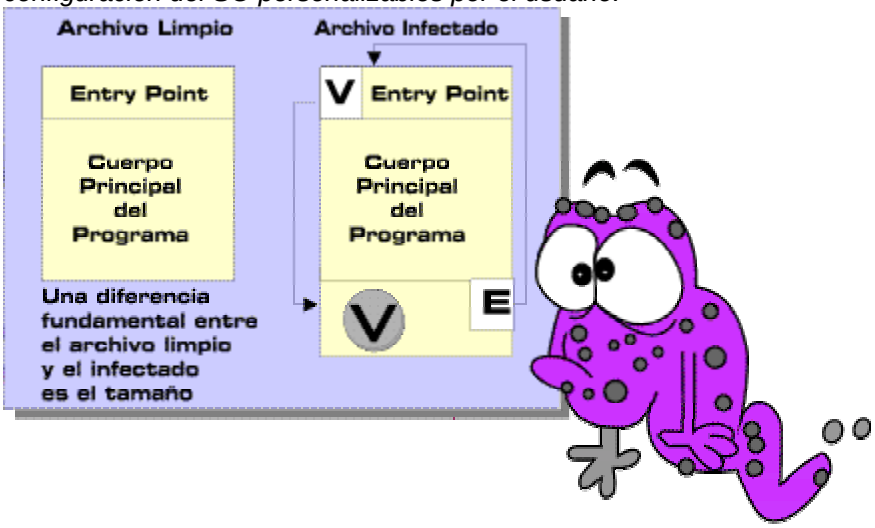
Funcionamiento de los virus

Los virus informáticos están hechos en Assembler, un lenguaje de programación de bajo nivel. Las instrucciones compiladas por Assembler trabajan directamente sobre el hardware, esto significa que no es necesario ningún software intermedio –según el esquema de capas entre usuario y hardware- para correr un programa en Assembler (opuesto a la necesidad de Visual Basic de que Windows 9x lo secunde). No solo vamos a poder realizar las cosas típicas de un lenguaje de alto nivel, sino que también vamos a tener control de cómo se hacen. Para dar una idea de lo poderoso que puede ser este lenguaje, el sistema operativo Unix está programado en C y las rutinas que necesitan tener mayor profundidad para el control del hardware están hechas en Assembler. Por ejemplo: los drivers que se encargan de manejar los dispositivos y algunas rutinas referidas al control de procesos en memoria.



Sabiendo esto, el virus puede tener control total de la máquina -al igual que lo hace el SO- si logra cargarse antes que nadie. La necesidad de tener que "asociarse" a una entidad ejecutable viene de que, como cualquier otro programa de computadora, necesita ser ejecutado y teniendo en cuenta que ningún usuario en su sano juicio lo hará, se vale de otros métodos furtivos. Ahora que marcamos la importancia para un virus el ser ejecutado, podemos decir que un virus puede encontrarse en una computadora sin haber infectado realmente algo. Es el caso de personas que pueden coleccionar virus en archivos comprimidos o encriptados.

Normalmente este tipo de programas se pega a alguna entidad ejecutable que le facilitará la subida a memoria principal y la posterior ejecución (métodos de infección). Como entidades ejecutables podemos reconocer a los sectores de arranque de los discos de almacenamiento magnéticos, ópticos o magneto-ópticos (MBR, BR), los archivos ejecutables de DOSs (.exe, .com, entre otros), las librerías o módulos de programas (.dll, .lib, .ovl, .bin, .ovr). Los sectores de arranque son fundamentales para garantizar que el virus será cargado cada vez que se encienda la computadora.
Según la secuencia de booteo de las PCs, el microprocesador tiene seteada de fábrica la dirección de donde puede obtener la primer instrucción a ejecutar. Esta dirección apunta a una celda de la memoria ROM donde se encuentra la subrutina POST (Power On Self Test), encargada de varias verificaciones y de comparar el registro de la memoria CMOS con el hardware instalado (función checksum). En este punto sería imposible que el virus logre cargarse ya que la memoria ROM viene grabada de fábrica y no puede modificarse (hoy en día las memorias Flash-ROM podrían contradecir esto último).
Luego, el POST pasa el control a otra subrutina de la ROM BIOS llamada "bootstrap ROM" que copia el MBR (Master Boot Record) en memoria RAM. El MBR contiene la información de la tabla de particiones, para conocer las delimitaciones de cada partición, su tamaño y cuál es la partición activa desde donde se cargará el SO. Vemos que en este punto el procesador empieza a ejecutar de la memoria RAM, dando la posibilidad a que un virus tome partida. Hasta acá el SO todavía no fue cargado y en consecuencia tampoco el antivirus. El accionar típico del virus sería copiar el MBR en un sector alternativo y tomar su posición. Así, cada vez que se inicie el sistema el virus logrará cargarse antes que el SO y luego, respetando su deseo por permanecer oculto hará ejecutar las instrucciones del MBR.
Con la información del MBR sabremos qué partición es la activa y en que sector se encuentra su sector de booteo (boot record o BR). El BR contiene una subrutina que se ocupará de cargar los archivos de arranque del SO. Los demás pasos de la carga del SO son irrelevantes, pero es importante recordar que el SO es el último en cargarse en la secuencia de booteo antes de que el usuario pueda introducir comandos en la shell. El antivirus es cargado por los archivos de configuración del SO personalizables por el usuario.



Cuando un virus infecta un archivo ejecutable .EXE, por ejemplo, intenta rastrear en el código los puntos de entrada y salida del programa. El primer punto señalado es en donde, dentro del archivo, se iniciará la ejecución de instrucciones. El segundo punto resulta ser lo opuesto. Cuando un virus localiza ambos puntos escribe su propio código antes de cada uno. Según el tipo de virus, este código cargará el virus en memoria –si es que no lo estaba- y apuntará a esa zona infectada con el virus. A partir de ahí el programa virósico determinará cuáles son las acciones a seguir: puede continuar infectando archivos que sean cargados en memoria, ocultarse si es que detecta la presencia de un antivirus o ejecutar el contenido de su módulo de ataque. El virus puede infectar también las copias de los archivos cargados en memoria que están en la unidad de

almacenamiento. Así se asegura que ante un eventual apagado de la computadora su código igualmente se encuentra en los archivos de la unidad.
Es importante comprender que la computadora no estará infectada hasta que ejecutemos algo parasitado previamente con el virus. Veamos un ejemplo sencillo: nosotros bajamos de Internet un archivo comprimido (con la extensión .ZIP según el uso popular) sabiendo que es un programa de prueba que nos gustaría instalar. Lo que no sabemos es que uno de los archivos dentro del .ZIP es un virus informático, y lo peor de todo es que viene adosado al archivo Install.exe. Al momento de descomprimir el contenido, el virus todavía no fue ejecutado (ya que la información dentro del .ZIP no puede ser reconocida como instrucciones por el procesador). Luego identificamos el archivo Install.exe como el necesario para instalar el programa y lo ejecutamos. Recién en este momento el virus se cargará en memoria y pasará a hacer las cosas para lo que fue programado.
El ejemplo anterior es un modo muy básico de infección. Pero existen otros tantos tipos de virus que son mucho más sofisticados y no podrá ser reconocida su presencia con mucha facilidad. Según sus características un virus puede contener tres módulos principales: el módulo de ataque, el módulo de reproducción, y el módulo de defensa.

-
- *Módulo de reproducción. Es el encargado de manejar las rutinas para infectar entidades ejecutables que asegurarán la subsistencia del virus. Cuando toma el control del sistema puede infectar otras entidades ejecutables. Cuando estas entidades sean trasladadas a otras computadoras se asegura la dispersión del virus.*

-
- *Módulo de ataque. Es el módulo que contiene las rutinas de daño adicional o implícito. El módulo puede ser disparado por distintos eventos del sistema: una fecha, hora, el encontrar un archivo específico (COMMAND.COM), el encontrar un sector específico (MBR), una determinada cantidad de booteos desde que ingreso al sistema, o cualquier otra cosa a la que el programador quisiera atacar.*

-
- *Módulo de defensa. Su principal objetivo es proteger el cuerpo del virus. Incluirá rutinas que disminuyan los síntomas que delaten su presencia e intentarán que el virus permanezca invisible a los ojos del usuario y del antivirus. Las técnicas incluidas en este módulo hoy en día resultan ser muy sofisticadas logrando dar información falsa al SO -y en consecuencia al usuario- y localizándose en lugares poco comunes para el registro de los antivirus, como la memoria Flash-Rom.*

Algunos métodos de infección

Añadidura o empalme. Por este método el código del virus se agrega al final del archivo ejecutable a infectar, modificando las estructuras de arranque del archivo anfitrión de manera que el control del programa pase primero al virus cuando se quiera ejecutar el archivo. Este cambio de secuencia permite al virus realizar sus tareas específicas y luego pasar el control al programa para que este se ejecute normalmente. La principal desventaja de este método es que el tamaño del archivo infectado es mayor al original, lo que permite una fácil detección.
Inserción. Los virus que utilizan el método de inserción buscan alojarse en zonas de código no utilizadas o en segmentos de datos dentro de los archivos que contagian, de esta manera la longitud total del archivo infectado no varía. Este método, parecido al de empalme, exige mayores técnicas de programación de los virus para poder detectar las zonas posibles de contagio dentro de un ejecutable, por lo que generalmente no es muy utilizada por los programadores de virus informáticos.
Reorientación. Este método es una variante interesante del anterior. Bajo este esquema se introducen centrales virósicas (los códigos principales del virus) en zonas físicas del disco rígido marcadas como defectuosas o en archivos ocultos del sistema. Estos códigos virales, al ejecutarse, implantan pequeños trozos de código en los archivos ejecutables que infectan, que

luego actúan como llamadores de las centrales virósicas. La principal ventaja de este método es que el cuerpo del virus, al no estar inserto en el archivo infectado sino en otro sitio oculto, puede tener un tamaño bastante grande, aumentando así su funcionalidad. La desventaja más fuerte es que la eliminación de este tipo de infecciones es bastante sencilla. Basta con borrar archivos ocultos sospechosos o reescribir las zonas del disco marcadas como defectuosas.
Polimorfismo. Este es el método más avanzado de contagio logrado por los programadores de virus. La técnica básica usada es la de inserción del código viral en un archivo ejecutable, pero para evitar el aumento de tamaño del archivo infectado, el virus compacta parte de su código y del código del archivo anfitrión de manera que la suma de ambos sea igual al tamaño original del archivo. Al ejecutar el programa infectado actúa primero el código del virus descompactando en memoria las porciones previamente compactadas. Una variante mejorada de esta técnica permite a los virus usar métodos de encriptación dinámicos para disfrazar el código del virus y evitar ser detectados por los antivirus.
Sustitución. El método de sustitución, usado con variantes por los Caballos de Troya, es quizás el método más primitivo. Consiste en sustituir el código completo del archivo original por el código del virus. Al ejecutar el programa infectado el único que actúa es el virus, que cumple con sus tareas de contagiar otros archivos y luego termina la ejecución del programa reportando algún tipo de error. Esta técnica tiene sus ventajas, ya que en cada infección se eliminan archivos de programas válidos, los cuales son reemplazados por nuevas copias del virus.
Tunneling. Es una técnica usada por programadores de virus y antivirus para evitar todas las rutinas al servicio de una interrupción y tener así un control directo sobre esta. Requiere una programación compleja, hay que colocar el procesador en modo kernel. En este modo de funcionamiento, tras ejecutarse cada instrucción se produce la INT 1. Se coloca una ISR (Interrupt Service Routine) para dicha interrupción y se ejecutan instrucciones comprobando cada vez si se ha llegado a donde se quería hasta recorrer toda la cadena de ISRs que halla colocando el parche al final de la cadena.
Los virus utilizan el tunneling para protegerse de los módulos residentes de los antivirus que monitorean todo lo que sucede en la máquina para interceptar todas las actividades "típicas" de los virus.
Para entender como funciona esta técnica basta saber como trabaja este tipo de antivirus. El módulo residente queda colgado de todas las interrupciones usualmente usadas por los virus (INT 21, INT 13, a veces INT 25 Y 26) y entonces cuando el virus intenta llamar a INT 21, por ejemplo, para abrir un ejecutable para lectura / escritura (y luego infectarlo), el antivirus emite una alerta, pues los ejecutables no son normalmente abiertos, ni menos para escritura. Y así con todas las llamadas típicas de los virus.
En cambio, cuando se hace una llamada común y corriente, el antivirus no le da mayor importancia y la deja pasar, llamando a la INT 21 original. Un virus con tunneling, entonces, antes de llamar a ninguna función ni hacer nada, intenta obtener el address absoluto de esta INT 21 original, que está en alguna parte de la memoria del antivirus residente. Una vez que obtiene este address, accede al MS-DOS por medio de el, sin llamar al antivirus. Y así, efectivamente, le "pasa por debajo", lo "tunelea". ¿Cómo se hace esto?
Existen dos formas fundamentales de obtener este address:

-
- *La primera, y la mas usada, es utilizando la interrupción de trace (INT 1) y la trap flag. (Que son usadas por los DEBUGGERS) para atravesar el código línea por línea hasta hallar lo que se busca. Es usada por todos los virus que usan esta técnica, como por ejemplo, el Predator II o el (ya viejo) Yankee Doodle.*
-
- *La segunda, hacer un simple y llano scanning del código, byte a byte, hasta hallar el address. Se usa en pocos virus, pero es la que usa Kohntark en su célebre Kohntark Recursive Tunneling Toolkit.*

Problemas Generales del Tunneling.

Pero el problema principal del tunneling es que aún teniendo éxito en obtener la INT 21 posta, se pueden tener problemas si hay algún residente importante y uno lo esta pasando por debajo. Es famoso ya el caso del Predator II y el DoubleSpace. El predator II tuneleaba por debajo del DoubleSpace y trataba de acceder al disco directamente por MS-DOS. Esto produjo que destruyera el contenido de varios discos rígidos. En definitiva, esto es contrario a las intenciones del tunneling.

Clasificación de los virus

La clasificación correcta de los virus siempre resulta variada según a quien se le pregunte. Podemos agruparlos por la entidad que parasitan (sectores de arranque o archivos ejecutables), por su grado de dispersión a nivel mundial, por su comportamiento, por su agresividad, por sus técnicas de ataque o por como se oculta, etc. Nuestra clasificación muestra como actúa cada uno de los diferentes tipos según su comportamiento. En algunos casos un virus puede incluirse en más de un tipo (un multipartito resulta ser sigiloso).

Caballos de Troya

Los caballos de troya no llegan a ser realmente virus porque no tienen la capacidad de autoreproducirse. Se esconden dentro del código de archivos ejecutables y no ejecutables pasando inadvertidos por los controles de muchos antivirus. Posee subrutinas que permitirán que se ejecute en el momento oportuno. Existen diferentes caballos de troya que se centrarán en distintos puntos de ataque. Su objetivo será el de robar las contraseñas que el usuario tenga en sus archivos o las contraseñas para el acceso a redes, incluyendo a Internet. Después de que el virus obtenga la contraseña que deseaba, la enviará por correo electrónico a la dirección que tenga registrada como la de la persona que lo envió a realizar esa tarea. Hoy en día se usan estos métodos para el robo de contraseñas para el acceso a Internet de usuarios hogareños. Un caballo de troya que infecta la red de una empresa representa un gran riesgo para la seguridad, ya que está facilitando enormemente el acceso de los intrusos. Muchos caballos de troya utilizados para espionaje industrial están programados para autodestruirse una vez que cumplan el objetivo para el que fueron programados, destruyendo toda la evidencia.

Camaleones

Son una variedad de similar a los Caballos de Troya, pero actúan como otros programas comerciales, en los que el usuario confía, mientras que en realidad están haciendo algún tipo de daño. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales). Un software camaleón podría, por ejemplo, emular un programa de acceso a sistemas remotos (rlogin, telnet) realizando todas las acciones que ellos realizan, pero como tarea adicional (y oculta a los usuarios) va almacenando en algún archivo los diferentes logins y passwords para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

Virus polimorfos o mutantes

Los virus polimorfos poseen la capacidad de encriptar el cuerpo del virus para que no pueda ser detectado fácilmente por un antivirus. Solo deja disponibles unas cuantas rutinas que se encargaran de desencriptar el virus para poder propagarse. Una vez desencriptado el virus intentará alojarse en algún archivo de la computadora.

En este punto tenemos un virus que presenta otra forma distinta a la primera, su modo desencriptado, en el que puede infectar y hacer de las suyas libremente. Pero para que el virus presente su característica de cambio de formas debe poseer algunas rutinas especiales. Si mantuviera siempre su estructura, esté encriptado o no, cualquier antivirus podría reconocer ese patrón.

Para eso incluye un generador de códigos al que se conoce como engine o motor de mutación. Este engine utiliza un generador numérico aleatorio que, combinado con un algoritmo matemático, modifica la firma del virus. Gracias a este engine de mutación el virus podrá crear una rutina de desencripción que será diferente cada vez que se ejecute.

Los métodos básicos de detección no pueden dar con este tipo de virus. Muchas veces para virus polimorfos particulares existen programas que se dedican especialmente a localizarlos y eliminarlos. Algunos softwares que se pueden baja gratuitamente de Internet se dedican solamente a erradicar los últimos virus que han aparecido y que también son los más peligrosos. No los

fabrican empresas comerciales sino grupos de hackers que quieren protegerse de otros grupos opuestos. En este ambiente el presentar este tipo de soluciones es muchas veces una forma de demostrar quien es superior o quien domina mejor las técnicas de programación.
Las últimas versiones de los programas antivirus ya cuentan con detectores de este tipo de virus.

Virus sigiloso o stealth

El virus sigiloso posee un módulo de defensa bastante sofisticado. Este intentará permanecer oculto tapando todas las modificaciones que haga y observando cómo el sistema operativo trabaja con los archivos y con el sector de booteo. Subvirtiendo algunas líneas de código el virus logra apuntar el flujo de ejecución hacia donde se encuentra la zona que infectada.
Es difícil que un antivirus se de cuenta de estas modificaciones por lo que será imperativo que el virus se encuentre ejecutándose en memoria en el momento justo en que el antivirus corre. Los antivirus de hoy en día cuentan con la técnica de verificación de integridad para detectar los cambios realizados en las entidades ejecutables.
El virus Brain de MS-DOS es un ejemplo de este tipo de virus. Se aloja en el sector de arranque de los disquetes e intercepta cualquier operación de entrada / salida que se intente hacer a esa zona. Una vez hecho esto redirigía la operación a otra zona del disquete donde había copiado previamente el verdadero sector de booteo.
Este tipo de virus también tiene la capacidad de engañar al sistema operativo. Un virus se adiciona a un archivo y en consecuencia, el tamaño de este aumenta. Está es una clara señal de que un virus lo infectó. La técnica stealth de ocultamiento de tamaño captura las interrupciones del sistema operativo que solicitan ver los atributos del archivo y, el virus le devuelve la información que poseía el archivo antes de ser infectado y no las reales. Algo similar pasa con la técnica stealth de lectura. Cuando el SO solicita leer una posición del archivo, el virus devuelve los valores que debería tener ahí y no los que tiene actualmente.
Este tipo de virus es muy fácil de vencer. La mayoría de los programas antivirus estándar los detectan y eliminan.

Virus lentos

Los virus de tipo lento hacen honor a su nombre infectando solamente los archivos que el usuario hace ejecutar por el SO, simplemente siguen la corriente y aprovechan cada una de las cosas que se ejecutan.
Por ejemplo, un virus lento únicamente podrá infectar el sector de arranque de un disquete cuando se use el comando FORMAT o SYS para escribir algo en dicho sector. De los archivos que pretende infectar realiza una copia que infecta, dejando al original intacto.
Su eliminación resulta bastante complicada. Cuando el verificador de integridad encuentra nuevos archivos avisa al usuario, que por lo general no presta demasiada atención y decide agregarlo al registro del verificador. Así, esa técnica resultaría inútil.
La mayoría de las herramientas creadas para luchar contra este tipo de virus son programas residentes en memoria que vigilan constantemente la creación de cualquier archivo y validan cada uno de los pasos que se dan en dicho proceso. Otro método es el que se conoce como Decoy launching. Se crean varios archivos .EXE y .COM cuyo contenido conoce el antivirus. Los ejecuta y revisa para ver si se han modificado sin su conocimiento.

Retro-virus o Virus antivirus

Un retro-virus intenta como método de defensa atacar directamente al programa antivirus incluido en la computadora.
Para los programadores de virus esta no es una información difícil de obtener ya que pueden conseguir cualquier copia de antivirus que hay en el mercado. Con un poco de tiempo pueden descubrir cuáles son los puntos débiles del programa y buscar una buena forma de aprovecharse de ello.
Generalmente los retro-virus buscan el archivo de definición de virus y lo eliminan, imposibilitando al antivirus la identificación de sus enemigos. Suelen hacer lo mismo con el registro del comprobador de integridad.
Otros retro-virus detectan al programa antivirus en memoria y tratan de ocultarse o inician una rutina destructiva antes de que el antivirus logre encontrarlos. Algunos incluso modifican el entorno de tal manera que termina por afectar el funcionamiento del antivirus.

Virus multipartitos

Los virus multipartitos atacan a los sectores de arranque y a los ficheros ejecutables. Su nombre está dado porque infectan las computadoras de varias formas. No se limitan a infectar un tipo de archivo ni una zona de la unidad de disco rígido. Cuando se ejecuta una aplicación infectada con uno de estos virus, éste infecta el sector de arranque. La próxima vez que arranque la computadora, el virus atacará a cualquier programa que se ejecute.

Virus voraces

Estos virus alteran el contenido de los archivos de forma indiscriminada. Generalmente uno de estos virus sustituirá el programa ejecutable por su propio código. Son muy peligrosos porque se dedican a destruir completamente los datos que puedan encontrar.

Bombas de tiempo

Son virus convencionales y pueden tener una o más de las características de los demás tipos de virus pero la diferencia está dada por el trigger de su módulo de ataque que se disparará en una fecha determinada. No siempre pretenden crear un daño específico. Por lo general muestran mensajes en la pantalla en alguna fecha que representa un evento importante para el programador. El virus Michel Angelo sí causa un daño grande eliminando toda la información de la tabla de particiones el día 6 de marzo.

Conejo

> *Cuando los ordenadores de tipo medio estaban extendidos especialmente en ambientes universitarios, funcionaban como multiusuario, múltiples usuarios se conectaban simultáneamente a ellos mediante terminales con un nivel de prioridad. El ordenador ejecutaba los programas de cada usuario dependiendo de su prioridad y tiempo de espera. Si se estaba ejecutando un programa y llegaba otro de prioridad superior, atendía al recién llegado y al acabar continuaba con lo que hacia con anterioridad. Como por regla general, los estudiantes tenían prioridad mínima, a alguno de ellos se le ocurrió la idea de crear este virus. El programa se colocaba en la cola de espera y cuando llegaba su turno se ejecutaba haciendo una copia de sí mismo, agregándola también en la cola de espera. Los procesos a ser ejecutados iban multiplicándose hasta consumir toda la memoria de la computadora central interrumpiendo todos los procesamientos.*

Macro-virus

Los macro-virus representan una de las amenazas más importantes para una red. Actualmente son los virus que más se están extendiendo a través de Internet. Representan una amenaza tanto para las redes informáticas como para los ordenadores independientes. Su máximo peligro está en que son completamente independientes del sistema operativo o de la plataforma. Es más, ni siquiera son programas ejecutables.

Los macro-virus son pequeños programas escritos en el lenguaje propio (conocido como lenguaje script o macro-lenguaje) propio de un programa. Así nos podemos encontrar con macro-virus para editores de texto, hojas de cálculo y utilidades especializadas en la manipulación de imágenes. En Octubre de 1996 había menos de 100 tipos de macro-virus. En Mayo de 1997 el número había aumentado a 700.

Sus autores los escriben para que se extiendan dentro de los documentos que crea el programa infectado. De esta forma se pueden propagar a otros ordenadores siempre que los usuarios intercambien documentos. Este tipo de virus alteran de tal forma la información de los documentos infectados que su recuperación resulta imposible. Tan solo se ejecutan en aquellas plataformas que tengan la aplicación para la que fueron creados y que comprenda el lenguaje con el que fueron programados. Este método hace que este tipo de virus no dependa de ningún sistema operativo. El lenguaje de programación interno de ciertas aplicaciones se ha convertido en una poderosa herramienta de trabajo. Pueden borrar archivos, modificar sus nombres y (como no) modificar el contenido de los ficheros ya existentes. Los macro-virus escritos en dichos lenguajes pueden efectuar las mismas acciones.

Al día de hoy, la mayoría de virus conocidos se han escrito en WordBasic de Microsoft, o incluso en la última versión de Visual Basic para Aplicaciones (VBA), también de Microsoft. WordBasic es el lenguaje de programación interno de Word para Windows (utilizado a partir de la versión 6.0) y

Word 6.0 para Macintosh. Como VBA se ejecuta cada vez que un usuario utiliza cualquier programa de Microsoft Office, los macro-virus escritos en dicho lenguaje de programación representan un riesgo muy serio. En otras palabras, un macro-virus escrito en VBA puede infectar un documento de Excel, de Access o de PowerPoint. Como estas aplicaciones adquieren más y más importancia cada día, la presencia de los macro-virus parece que está asegurada.
Microsoft Word es una de las aplicaciones preferidas para los macro-virus. Y lo es por varias razones:

- *Microsoft Word está muy difundido, por lo que un macro-virus para esta aplicación tendrá un gran impacto. Además, Microsoft Word es un producto pensado para plataformas cruzadas, disponible para DOS, Windows 3. 1, Windows 95, Windows NT y Mac OS, con lo que se amplía enormemente la posibilidad de infección.*
- *La plantilla Normal de Word (en las versiones de Windows se llama normal. dot) contiene todas las macros que se pueden utilizar con Word. Para un macro-virus esta plantilla es suelo fértil en el cual puede incubar sus virus y copiarlos luego a otros documentos de Word o incluso al resto de aplicaciones de Microsoft.*
- *Microsoft Word puede ejecutar automáticamente macros sin necesidad del consentimiento humano. Esta habilidad hace que el escritor de macro-virus asocie sus programas con algún tipo de macro legítima. Word usa macros para (entre otras cosas) abrir y cerrar documentos. E incluso para cerrar el propio programa.*
- *Comparado con lo complicado que resulta escribir macros en ensamblador, escribir en el leguaje de programación de Word es un juego de niños. Las principales ventajas de WordBasic y VBA son que son lenguajes muy intuitivos.*
- *Los usuarios suelen pegar sus documentos de Word a sus mensajes de correo electrónico, publicarlos en sitios FTP o bien mandarlos a una lista de mail. Como se puede figurar la cantidad de gente que se infectará con este tipo de documentos es enorme. Desgraciadamente, debido a la novedad de estos sistemas de transmisión, el creador de un macro-virus puede estar seguro de que su virus llegará a mucha gente.*

Un macro-virus para Word también es capaz de sobreescribir las opciones Guardar, Guardar cómo y Nuevo del menú Archivo para asegurar su permanencia. La verdad es que sobreescribir estas opciones no representa ningún tipo de problema. Basta con copiar la macro al documento y copiarla a otra macro con las modificaciones deseadas. La naturaleza polimorfa de este tipo de virus es una de las razones por la que los profesionales los consideran tan peligrosos.
Word 7.0 para Windows 95 y NT y Microsoft Word 97 avisan automáticamente a sus usuarios cuando abren un documento y éste contiene macros. Además, Microsoft proporciona una herramienta de protección contra los virus llamada MVP válida para sus usuarios de Windows y Macintosh. Dicha herramienta instala una serie de macros que detectan cualquier macro sospechosa y avisa al usuario del peligro que conlleva abrir un documento determinado. Conviene que escanee todos los documentos de Word que reciba a través del correo electrónico antes de abrirlos por si están infectados. En las últimas versiones de Microsoft Word (a partir de la 7.0) hay un detalle que las hace menos susceptibles ante la infección de los macro-virus de Word. Y es que, al igual que las últimas versiones de programas como Excel, Access y PowerPoint, se ha cambiado el lenguaje de programación interno. Microsoft usa un lenguaje nuevo al que ha bautizado como

Visual Basic para Aplicaciones 5.0 (VBA). Además, las nuevas versiones de Chamaleon (de NetManage), Photoshop (de Adobe) y AutoCAD (de AutoDesk) utilizan VBA.
Es una buena noticia saber que el cambio de lenguaje anulará la mayoría de los macro-virus de Word (siempre que no se esté trabajando en un modo compatible con las antiguas versiones de WordBasic). Sin embargo, la aparición de VBA 5.0 y su aceptación entre las aplicaciones indica que nos encontramos ante una nueva era de macrovirus. Y como VBA es un lenguaje que utilizan muchas aplicaciones será posible que un mismo macro-virus infecte a aplicaciones muy distintas entre sí.
Los pasos que se deben seguir para eliminar macro-virus son los siguientes:

1.
2. *Activar la protección antivirus si está desactivada.*

-
- *Abrir el Word directamente, sin ningún documento.*
-
- *Ir al menú Herramientas, y elegir Opciones....*
-
- *En la pestaña General, activar la casilla donde dice Protección antivirus en macro.*

1.
2. *Abrir el documento infectado teniendo en cuenta que, cuando se presente la ventana de Advertencia, se debe elegir la opción Abrir sin Macros para no infectarse.*
3.
4. *Una vez abierto el documento, elegir, dentro del menú Herramientas, la opción Macro y dentro de ella, la que dice Editor de Visual Basic, o directamente, presionar la combinación de teclas ALT+F11. Donde, en la parte izquierda de la pantalla, se podrá observar un cuadro que dice "Proyecto - ..." y el nombre del archivo abierto, en este caso Normal.*
5.
6. *Se debe desplegar cada uno de los ítems de ese cuadro para ver el código de las macros. Al hacer doble click sobre algunos de estos elementos, se abrirá una nueva ventana con código.*
7.
8. *Se debe marcar el texto que aparece en la nueva ventana, y eliminarlo como se haría con cualquier texto. Al hacer esto, se estarán eliminando las macros que contiene el documento, lo que eliminará completamente el Macrovirus.*

Estos pasos deben repetirse por todos los elementos que se encuentren en el cuadro Proyectos.

Gusanos

Un gusano se puede decir que es un set de programas, que tiene la capacidad de desparramar un segmento de el o su propio cuerpo a otras computadoras conectadas a una red.
Hay dos tipos de Gusanos:

-

- *Host Computer Worm: son contenidos totalmente en una computadora, se ejecutan y se copian a si mismo vía conexión de una red. Los Host Computer Worm, originalmente terminan cuando hicieron una copia de ellos mismos en otro host. Entonces, solo hay una copia del gusano corriendo en algún lugar de una red. También existen los Host Computer Worm, que hacen una copia de ellos mismos e infectan otras redes, es decir, que cada maquina guarda una copia de este Gusano.*

- *Network Worms: consisten en un conjunto de partes (llamadas "segmentos"), cada una corre en una maquina distinta (y seguramente cada una realiza una tarea distinta) y usando la red para distintos propósitos de comunicación.*

  Propagar un segmento de una maquina a otra es uno de los propósitos. Los Network Worm tienen un segmento principal que coordina el trabajo de los otros segmentos, llamados también "octopuses".

El Famoso Internet Worm creado por Morrison en 1988 y que tantas máquinas infectó era del tipo Host Computer. Para conocer un Gusano, veamos detalladamente como funcionaba el que hizo Morrison.
El objetivo de ese virus era obtener una "shell" en la otra maquina. Para esto el gusano usaba tres técnicas distintas Sendmail, fingerd y rsh/rexec.

- *The Sendmail Attack. En el ataque por Sendmail, el gusano abría una conexión TCP con el sendmail de otra maquina (puerto SMTP). Mediante un error del Sendmail, el Gusano creaba un programa C que se compilaba en la máquina ya infectada y reemplazaba la shell común sh por una Worm.*

- *The Fingerd Attack. En este ataque, intentaba infiltrarse por un bug en el daemon del finger (fingerd). Aparentemente era con este bug que el gusano se pudo desparramar con tanta libertad. Al parecer, los argumentos del daemon de finger eran leídos sin tener controles preestablecidos de los límites. El gusano, aprovechándose de eso, ejecutaba un comando y reemplazaba la shell común sh con el gusano. Así, cada vez que un usuario se logueara empezaba a funcionar el Gusano.*

- *The Rsh/Rexec Attack. La tercera forma de entrar a un sistema por una Red, era utilizando la confianza de host. Para esto, necesitaba tener un nombre de usuario y contraseña. Por eso abría el /etc/passwd y probaba contraseñas conocidas. Combinaba nombre de usuario, con la descripción, etc. Cuando conseguía la password de algún usuario, buscaba el archivo .rhosts y usando los comandos de confianza rsh/rexec para obtener una cuenta en otra maquina de confianza y empezar el proceso de nuevo. Cuando el gusano se conectaba a un host satisfactoriamente, creaba un proceso (hijo) que continuaba con la infección, mientras que el primer proceso (padre) sigue buscando host para seguir infectando. Para conseguir host para infectar, el gusano usa distintas técnicas, como por ejemplo el netstat, o edita el /etc/hosts en busca de algún host, cada vez que encuentra uno, intenta infectarlo.*

Los Nuevos Worm
Happy99. Fue descubierto en Junio de 1999. La primera vez que es ejecutado se ven fuegos artificiales y un cartel que dice "Happy 99". Este cartel es un fachada, ya que mientras se encarga de reemplazar algunos archivos. Cada mensaje que se manda por e-mail, crea un mensaje alternativo que tiene adjunto el Happy99.
Este gusano tiene una lista de cada e-mail al cual fue enviado una copia del Happy99.
Melissa Virus. El virus Melissa es un virus de Macro en Word, que infecta el sistema y manda 50 copias de sí mismo, utilizando el Microsoft Outlook. Muestra un mensaje que dice "Important Message from <nombre>" y manda un e-mail adjuntando el archivo .doc. Aún, si la máquina no tuviera el Microsoft Outlook, este Troyano / Virus infecta la máquina.
Bubbleboy Worm. Este gusano nunca salió a la luz, sino que fue creado por una persona que quiso demostrar las falencias que tiene el sistema VBS Script. Lo importante de este virus es que es

enviado por e-mail, pero puede infectar a la máquina sin la necesidad de abrir ningún archivo adjunto, ya que el gusano vienen incluido en el e-mail, por eso hace de este gusano muy peligroso. Simplemente al hacerle un click en el mensaje el virus se activa. Es por esto, que este virus solo infecta maquinas Windows 98 / 2000, con IE 5 y Outlook / Outlook Express.
La propagación del Bubbleboy depende de dos controles ActiveX particulares que fueron marcados como "seguros".