

Seguridad informática

Virus informáticos

Cómo protegerse Marzo - 2000

Índice general

Introducción * [Ir...](#)

Conceptos básicos sobre virus informáticos * [Ir...](#)

¿Qué es un virus informático? * [Ir...](#)

¿Quién los hace? * [Ir...](#)

Un poco de historia * [Ir...](#)

Funcionamiento de los virus * [Ir...](#)

Algunos métodos de infección * [Ir...](#)

Clasificación de los virus * [Ir...](#)

Caballos de Troya * [Ir...](#)

Camaleones * [Ir...](#)

Virus polimorfos o mutantes * [Ir...](#)

Virus sigiloso * [Ir...](#)

Virus lentos * [Ir...](#)

Retro-virus o Virus antivirus * [Ir...](#)

Virus multipartitos * [Ir...](#)

Virus voraces * [Ir...](#)

Bombas de tiempo * [Ir...](#)

Conejo * [Ir...](#)

Macro-virus * [Ir...](#)

Gusanos * [Ir...](#)

Virus propios de Internet * [Ir...](#)

[Determinar si existe infección * Ir...](#)

[Cómo proceder ante una infección * Ir...](#)

[Programas antivirus * Ir...](#)

[Identificación * Ir...](#)

[Técnicas de detección * Ir...](#)

[Análisis heurístico * Ir...](#)

[Eliminación * Ir...](#)

[Comprobación de integridad * Ir...](#)

[Proteger áreas sensibles * Ir...](#)

[Demonios de protección * Ir...](#)

[Aplicar cuarentena * Ir...](#)

[Definiciones antivirus * Ir...](#)

[Estrategia de seguridad contra los virus * Ir...](#)

[Conclusión del trabajo * Ir...](#)

[Bibliografía](#)

[* Ir...](#)

[Introducción !\[\]\(235bfe13ebf007ce2eea9e689707fac7_img.jpg\)](#)

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 !\[\]\(291e070cef6c4d5e78fefe4696ef53be_img.jpg\)](#)

□ ¿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 vaya 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 vaya 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 Automatas 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 empresas 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.

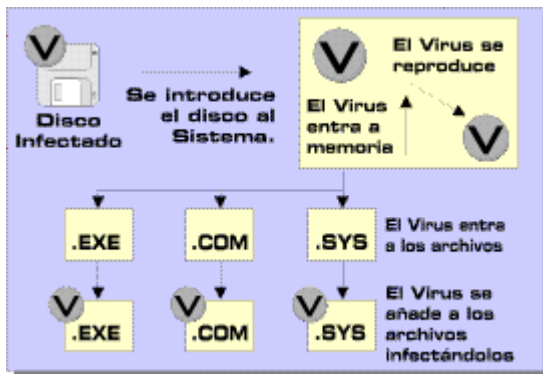
El 2 de Noviembre del '88, dos importantes redes de EE.UU. se ven afectadas seriamente por virus introducidos en ellas. Mas 6,000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados se ven atacados.

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.



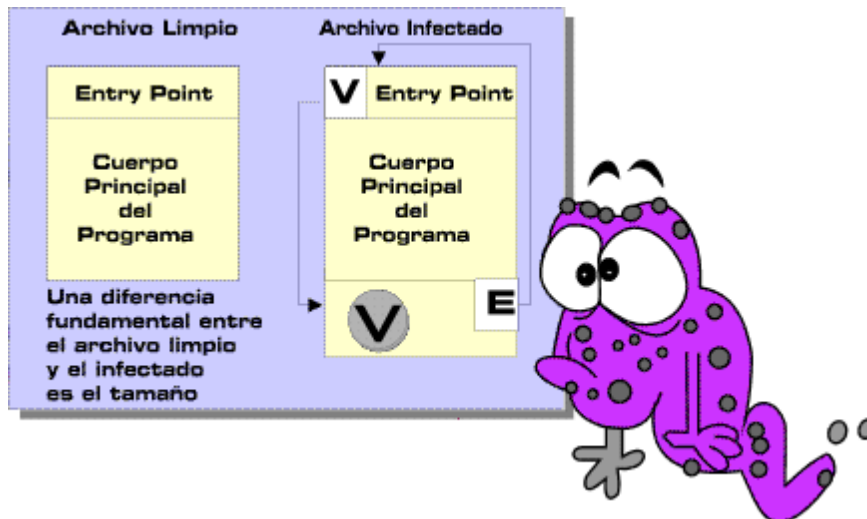
Sabiendo esto, el virus puede tener control total de la máquina -al igual que lo hace el SO- si logra cargarse antes que nadie. La necesidad de tener que "asociarse" a una entidad ejecutable viene de que, como cualquier otro programa de computadora, necesita ser ejecutado y teniendo en cuenta que ningún 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 primera 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 desencriptación 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 bajar 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 hacía 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 lenguaje 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 sobrescribir las opciones Guardar, Guardar cómo y Nuevo del menú Archivo para asegurar su permanencia. La verdad es que sobrescribir 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 sí 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 máquina guarda una copia de este Gusano.
-
- Network Worms: consisten en un conjunto de partes (llamadas "segmentos"), cada una corre en una máquina distinta (y seguramente cada una realiza una tarea distinta) y usando la red para distintos propósitos de comunicación.
 - Propagar un segmento de una máquina 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 máquina. 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 máquina (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 máquina 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 viene 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 máquinas 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".