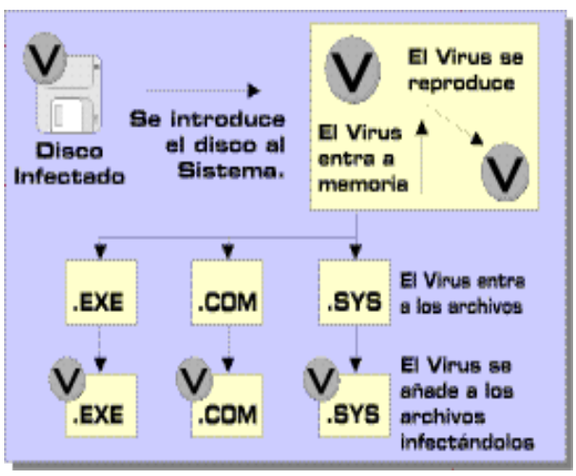
FUNCIONAMIENTO, CARACTERÍSTICAS Y CLASIFICACIÓN DE LOS VIRUS INFORMÁTICOS

FUNCIONAMIENTO DE LOS VIRUS. Un virus puede tener control total de la máquina -al igual que lo hace el Sistema Operativo- 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.

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.

CARACTERÍSTICAS DE LOS VIRUS

Según sus características un virus puede contener tres módulos principales:

1. **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.

2. **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 (arranques), desde que ingreso al sistema, o cualquier otra cosa a la que el programador quisiera atacar.
3. **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 Sistema Operativo -y en consecuencia al usuario- y localizándose en lugares poco comunes para el registro de los antivirus, como la memoria Flash-Rom.

CLASIFICACIÓN DE LOS VIRUS INFORMÁTICOS

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 (usuarios) y passwords (contraseñas), 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.

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 quién 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 (arranque). Subvirtiendo algunas líneas de código el virus logra apuntar el flujo de ejecución hacia donde se encuentra la zona infectada.

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.

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.

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.

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.
- 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.
- 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.

Gusanos: Un gusano se puede decir que es un set de programas, que tiene la capacidad de desparramar un segmento de él 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 máquina 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 "octopuses".

TALLER

1. Usando sus propias palabras diga cómo funcionan los virus.
2. ¿Cuál es la necesidad que tiene un virus para poder cargarse y generar su función maligna?
3. Escriba en su cuaderno los tres módulos principales de los cuales se compone un virus.
4. Liste en su cuaderno cada tipo de virus de éste documento y haga un resumen de lo que hace.
5. Según la descripción del virus “Caballo de Troya”, ¿en razón a que llevan ese nombre?
6. Explique con sus propias palabras el retro-virus.
7. Según su criterio, ¿cuál sería el virus más peligroso o destructivo de los mencionados en la teoría?
8. ¿En que se parecen los virus gusanos con los gusanos reales?
9. Escriba en su cuaderno los tipos de gusanos informáticos (virus) que existen.
10. Comente que hace usted constantemente para contrarrestar el peligro o la amenaza a la que se expone diariamente su información en su computador.
11. Comente ¿por qué es importante que esté informado sobre los tipos de virus que existen en la actualidad?