MODULO Nº 7

CLASE Nº 38

VIRUS INFORMÁTICOS

QUÉ ES UN VIRUS INFORMÁTICO ?:

Un virus es un pequeño PROGRAMA (generalmente menos de 1Kb), que se instala de forma de forma subrepticia (inadvertida) dentro de otro programa con el objeto de tomar el control del Sistema Operativo para causar algún tipo de daño.

Todo virus tiene las siguientes características:

* **Siempre produce algún tipo de DAÑO** : Está programado para causar daño en cualquiera de sus formas. En el mejor de los casos el daño es "TRIVIAL" (puede bajar la performance del sistema al consumir Memoria, tiempo de trabajo del Micro, espacio en disco, etc). En el peor de los casos el daño es "SEVERO" y consiste en la pérdida TOTAL o PARCIAL de la Información.

* **Tiene capacidad de AUTO-REPRODUCCIÓN:** Posee la habilidad de realizar copias de sí mismo, de manera que se asegura la supervivencia de su especie. Al copiarse en archivos de una unidad de Diskette se asegura su proliferación y transporte, supuestamente, hacia otra máquina.

* **Es OCULTO y trabaja en forma OCULTA :** El virus se instala dentro de un programa ejecutable modificándolo internamente, aunque no en su apariencia, de modo que su pesencia no sea notoria. De esta manera será transportado hacia la Memoria del equipo cada vez que el *programa anfitrión* se ejecute, quedando residente para llevar a cabo de esa manera su accionar, sin que se note su presencia.

Para lograr sus objetivos, un virus cuenta con las siguientes partes constitutivas:

* **Un Módulo de Reproducción:** Es la parte del código del virus encargada de realizar copias de sí mismo en otros archivos ejecutables con el objeto de que se asegure la supervivenvia de su especie.

* **Un Módulo de Defensa:** Es la parte del virus encargada de ocultar, por divesos medios, la presencia del virus ante la búsqueda de los programas *Antivirus*.

* **Un Módulo de Ataque:** Es la parte del virus encargada de ejecutar la acción destructiva, un vez dada un cierta condición.

FASES EN LA VIDA DE UN VIRUS:

Las fases de actuación de un virus son las siguientes:

a) INFECCIÓN: El virus llega al ordenador dentro de un programa existente en un DKT o vía Modem, o también sólo en el sector booteable de un DKT . El usuario, ignorando su presencia , ejecuta el programa infectado transladando también el VIRUS a la memoria RAM (donde generalmente queda residente). A partir de su presencia en la memoria ram principal el virus intentará tomar el control de SO infectando los archivos de sistema en primer lugar, luego el DBR y finalmente el MBR.

b) REPRODUCCIÓN: Una vez infectado el SO comienza esta etapa, en la cual el virus tiene el control de las operaciones de Sistema. Es aquí cuando comienza a infectar

a todo programa que se ponga a su alcance (al ser ejecutado y cargado en RAM). Todo programa que se utiliza en ésta etapa será modificado por el virus para incluir en él una copia del mismo. De éste modo, si uno de esos programas infectados es copiado en un dkt y llevado a otra máquina, la infección se propagará a está.

c) DETONACIÓN: Una vez que se da una determinada circunstancia, como por ejemplo la llegada de cierta fecha o la realización de cierta cantidad de copias de sí mismo, el virus "detona" su acción destructiva. El tipo de acción destructora es muy variada, desde borrar archivos ejecutables, a hacer aparecer en la pantalla diversos objetos, borrar la *Tabla de Partición* o formatear el *HDD*.

TIPOS DE VIRUS:

Según el lugar donde se alojan *(ZONA DE ATAQUE)* se pueden clasificar en:

*** CONTAMINADORES DEL MBR, DBR Y DEL SO**: Éste tipo de virus se aloja en las áreas más importantes del Sistema para lograr de ésa manera cargarse en la memoria RAM ppal. antes del booteo, cada vez que la máquina sea encendida. Existen virus que atacan una sola de ellas, o más de forma combinada. Recordemos que las áreas más importante del disco son:

1.- El MBR (Master Boot Record): El mismo es el primer sector físico de un HDD (*cyl 0, head 0, sector 1*) y contiene no sólo la **Tabla de Partición**, sino también, el **Master Boot** (de allí su nombre). Éste es un pequeño programa que permite que indica que el hdd es booteable y dirige el proceso de arranque hacia el DBR (*DOS Boot Record* , grabado *en cyl 0, head 0, sector 1*) el cual, a su vez, llama a los archivos de Sistema (*MSDOS.SYS , IO.SYS y COMMAND.COM*) . Los virus que atacan éste sector sustituyen el Master Boot por su propio código.

2.- El DBR (DOS Boot Record): Es el primer sector físico de la cara **1** de un hdd (*cyl 0, head 1, sector 1*), y contiene toda la información necesaria para acceder al disco una vez formateado por el SO (*cantidad y tamaños de FAT, tamaño de sector y de cluster, cantidad total de clusters, cantidad total de sectores, cantidad máxima de archivos en directorio raíz, tamaño de Área de Directorio, etiquet a de volumen, número de serie, etc*). Además, el DBR orienta la búsqeda de los archivos de sistema.
Los virus que atacan éste sector lo alteran de manera que se cargue el código del virus antes que los Archivos de Sistema, modificando también la FAT.

3.- Los Archivos de Sistema: Los archivos de sistema conforman el **SHELL** o interfase con el usuario (Command.com) y el **KERNELL** (IO.SYS y MSDOS.SYS, que son ocultos) y son los reponsables de la administración de todas las actividades del sistema. Los virus que atacan éstos archivos, copian su código en ellos, de forma que pasan a ser parte del SO para actuar sin restricciones y en forma totalmente desapercibida.

*** CONTAMINADORES DE ARCHIVOS EJECUTABLES:** Este tipo de virus atacan a los archivos ejecutables cuyas extensiones suelen ser **: *.COM, .EXE, .OVL, .DRV, y .SYS* .** Como ya sabemos, este tipo de virus copia su código dentro el ejecutable de manera que al cargar el programa en la memoria, también se cargue su propio código. Algunos virus *SOBREESCRIBEN* el programa, dañándolo irreparablemente, otros , en cambio, se suman al archivo , cambiando su tamaño oculta o visiblemente.

Según la forma de actuar en la memoria RAM, se pueden clasificar en:

* **RESIDENTES o TSR:** Se instalan residentes en la memoria RAM ppal cuando es ejecutado el programa "anfitrión" (es el caso de la mayoría).

* **DE ATAQUE ÚNICO:**También se instalan en memoria al ser ejecutado el programa "anfitrión", pero no quedan residentes , sino que actúan para realizar su acción destructiva, abandonando luego la memoria del sistema.

Según su Peligrosidad se pueden clasificar en:

* **Virus de Primera generación:** Responden a las tres fases de vida, antes descriptas, desatando rápidamente su acción destructora. Al activarse destruyen sistemáticamente toda la información existente.

* **Virus de Segunda Generación:** La aparición de programas Anti-Virus hace que los virus intenten ser menos notorios, con el objeto de permanecer activos más tiempo antes de ser detectados y provocar el mayor daño posible. Asi, atacan ahora a los archivos de Datos, nó destruyéndolos, sino alterando sutilmente su información constantemente y de forma acumulativa.

- **Virus de Tercera Generación:** Son los más peligrosos. Cumplen con las sig. principales características:

  + Superponen la fase de reproducción y ataque.

  + Utilizan mecanismos de Engaño para no ser detectados por los programas de Escaneo Antivirus como son : las técnicas STEALTH y el POLIMORFISMO y TUNNELING.

Virus Stealth (Cautelosos):

Si un virus Stealth está en memoria, cualquiera programa que intente leer el archivo (o sector de un archivo) que contiene el virus, es engañado por él, no advirtiendo su presencia en los datos leídos, y determinando por lo tanto que el virus *"no está allí"*.
Esto es posible ya que el virus activo en memoria filtra sus propios bytes, y solamente muestra los bytes originales del programa.

Virus Polimórficos:

Son virus capaces de auto-encriptarse gracias a un parte de sí mismo (o módulo) llamada módulo de defensa que se encarga de encriptar y desencriptar al virus, la cual es muy variable. El Encriptado es un medio muy eficaz para evitar la detección por parte de los programas antivrus que consiste básicamente en un desorden del código original del virus, merced a un patrón o algorítmo de encriptación.
Gracias a sofisticadas técnicas de encriptado, dos copias de un virus polimórfico no tienen ninguna secuencia de bytes en común, (debido a que el algoritmo de encriptación varia con cada copia) de manera que se dificulta su detección por parte de los programas de Escaneo Antivirus.

Virus de efecto Tunneling:

Son capaces de eludir la protección ofrecida por los programas antivirus TSR (residentes), sin que se detecte su presencia por esa vía de escaneo.

VIRUS Vs BOMBAS LÓGICAS, GUSANOS Y TROYANOS (o Programas de Daño Intencional)

Recordemos que un programa para ser un virus debe cumplir con tres condiciones:

a) Ser DAÑINO.
b) AUTOREPRODUCIRSE.
c) Ser OCULTO.

Estas características nos permiten diferenciarlos de otros programas similares, los cuales son sus ANTECESORES. Ellos son : las Bombas Lógicas, los Gusanos y los Troyanos.

Bombas Lógicas:

Es un programa que, bajo la forma de un archivo identificable y *localizable a simple vista,* que con un nombre sugestivo (ej: leame.com) tiene por objeto destruir Datos (utilizando diversos medios), o bien paralizar alguna parte o todo el equipo, de manera que no se pueda controlarlo (trabar el teclado o el video) si tener que resetear.

Una bomba no cumple con las tres características de los virus , ya que:

a) Causa Daño.
pero.... b) No se Autoreproduce (la copia y transporta intencionalmente un usuario).
y..... c) No es oculta (es visible).

Gusanos:

Es un programa *visible* que cada vez que se ejecuta, genera múltiples copias de sí mismo y en distintos lugares del disco. Su nombre se debe a su facilidad de reproducción indiscriminada. Muchas veces sus copias van cambiando ligeramente su nombre. El daño que producen consiste en el consumo inútil dealgunos recursos del sistema (memoria y espacio en disco).

Una Gusano no cumple con las tres características de los virus , ya que:

a) Causa Daño.
b) Se Autoreproduce (lo copia y transporta intencionalmente un usuario).
pero..... c) No es Oculto (es visible).

Troyanos:

Un Troyano es un pequeño programa que se instala dentro de otro, el cual deliberadamente tiene efectos destructivos diversos. Son los antecesores directos de los virus.

No son capaces de reproducirse por sí mismos (tampoco poseen un módulo de defensa) y realizan su proliferación a expensas de la copia realizada por los usuarios.

Una Troyano no cumple con las tres características de los virus , ya que:

a) Causa Daño (generalmente SEVERO).
pero..... b) No se Autoreproduce (lo debe copiar intencionalmente un usuario).
c) Es oculto.

Algunos antivirus son capaces de detectar la presencia de diversos Troyanos.

FUENTES TÍPICAS DE CONTAGIO:

Hay dos formas en que un virus puede llegar a alojarse en la memoria de un máquina:

1.- Por lectura de DISKETTE con Boot Sector infectado: Al poner un diskete en una unidad y tipear **A:** , el virus pasa a estar activo en la memoria RAM (no es necesario pedir un DIR!).

2.- Por ejecución de programa infectado: Como ya se aclaró más arriba, lo peligroso no es tener un archivo infectado en el hdd, sino EJECUTARLO!, ya que de ese modo estamos transportando el virus a la memoria.

Las vías más comunes de contagios son:

* **DISKETES (archivos infectados y boot sector infectado)**
* **TRANSFERENCIAS DE ARCHIVOS INFECTADOS POR MODEM.**
* **TRANSFERENCIAS DE ARCHIVOS INFECTADOS POR LINKEO.**
* **TRANSFERENCIAS DE ARCHIVOS INFECTADOS EN RED.**

CLASE Nº 39

PROGRAMAS ANTI - VIRUS:

Son programas capaces de combatir a los virus de manera efectiva. Generalmente son paquetes de soft que incluyen más de un programa .

Un programa Antivirus puede...

*** Detectar la presencia de un virus en memoria.**
*** Detectar la presencia de un virus en un archivo y eliminarlo.**
*** Detectar la presencia de un virus en las Áreas de Sistema del HDD (MBR y DBR) y eliminarlo.**
*** Impedir que un virus se cargue en memoria.**

La acción de detectar un virus es denominada ***ESCANEO*** (scan = rastreo o búsqueda).

Existen cuatro técnicas básicas de detectar la presencia de un virus:

*** SCANEO DE STRING O SIGNATURE.**
*** SCANEO HEURÍSTICO.**
*** CONTROL Y ADMINISTRACIÓN DE RECURSOS MEDIANTE UN TSR.**
*** CHEQUEO DE INTEGRIDAD.**

Scaneo de String o Signature:

El scaneo por String constituye el método de defensa más conocido en la lucha contra los virus. Su acción consiste en buscar en los archivos una porción de código característica de un virus conocido, llamada generalmente signature o string. Si esta cadena es encontrada, el programa infiere que el archivo en cuestión está infectado con un determinado virus.

Su única desventaja es que detecta sólo virus conocidos, y esto puede llegar a ser determinante ya que los expertos en virus analizan generalmente entre 150 y 200 nuevos virus cada mes. Es por eso que se debe conseguir casi cada mes una *ACTUALIZACION* del antivirus, la cual incluye las cadenas (o strings) de los virus de reciente aparición..

Con la creciente popularidad de las PC's y el aumento drástico del uso de Internet, nuevos virus están esparciendose más y más rápido que nunca. Hasta con actualizaciones mensuales, los usuarios pueden estar desprotegidos ante aproximadamente 200 nuevos virus cada mes.

Scaneo Heurístico:

El Análisis (o scaneo) Heurístico es la técnica de rastrear en un archivo la presencia de códigos y algorítmos sospechosos de contener un "Código Potencialmente Dañino". Esta técnica consiste en ejecutar un desensamblado automático, interno y transitorio del programa a analizar, para luego proceder al rastreo de sentencias o grupos de instrucciones que se consideren peligrosas. El método Heurístico detecta tanto virus ***Conocidos*** como ***Desconocidos***.

Si bien éste sistema es efectivo , es muy difícil determinar qué código es sospechoso.

Un código que podría ser inofensivo en un programa común (por ejemplo, el que ejecuta el formateo del hdd en el archivo *FORMAT.COM*) podría ser muy sospechoso en un archivo ejecutable infectado por un virus.

Por esta razón, y para calcular cuán sospechoso parece un archivo, el análisis heurístico generalmente instrumenta un sistema de *PUNTAJE*, y cualquiera archivo que tiene elementos suficientemente sospechosos (o sea una puntuación suficiente alta) es marcado como portador de un posible virus.

Los elementos sospechosos pueden incluir: Funciones no-documentadas de DOS , técnicas anti-debug para evitar el desensamblado, existencia de una máscara de búsqueda de archivos ejecutables (**.COM , *.EXE*) etc.

Hay dos grandes problemas con las técnicas tradicionales de Análisis Heurístico:

Primeramente, a menos que se tenga mucho cuidado, los programas de escaneo heuristico pueden dar alarmas falsas.

Una alarma falsa puede ser significativamente más problemática y ocupar más tiempo de trabajo que una infección genuina.

Lo normal es que un programa de escaneo que utiliza técnicas de Análisis Heurístico tradicional exhiba tasas de detección del **60%** y tasas de Falsa Alarma de **1 por 1000**.

En segundo lugar, los programas de escaneo Heurístico son incapaces de detectar todos los virus existentes.

Los autores de virus son conscientes de cuales son los códigos que los desarrolladores de Anti-virus consideran *"sospechosos"*.

Algunos investigadores de anti-virus han liberado documentación detallada de como trabaja su sistema de Puntaje para el escaneo de códigos sospechosos.

Con tal información es más fácil para el autor de virus escribir sus virus, de manera que se evite su detección.

Programas Anti-Virus Residentes en memoria (TSR):

Estos programas pueden ser instalados en memoria cuando arranca la computadora (desde el *autoexec.bat*), para proveer protección anti-virus por todo el tiempo que la computadora esté prendida. Una vez instalados en memoria controlan y monitorean el sistema para impredir que el código de un virus se cargue en *RAM*.

Sin embargo, estos programas ocupan un espacio de memoria y pueden bajar la performance del sistema .

Hay tres tipos de programas anti-virus residentes:

1.- *El primer tipo* puede impedir que se ejecute en memoria un ejecutable infectado con un virus conocido. Esto lo logra realizando un scaneo (por string) previo a su carga en memoria.

2.- *El segundo tipo* es un Bloqueador Heurístico de comportamiento, que señala y evita la ejecución de cualquier actividad sospechosa (comportamiento tipo virus) para la integridad de los datos del sistema.

3.- *El tercero* realiza un Chequo de Integridad del archivo ejecutable a cargarse en la memoria, realizando un checksum previo a su carga.

Chequeo de Integridad:

La técnica de *"Chequeo de Integridad"*, es utilizada para detectar cambios en la longitud de los archivos. Su principal ventaja es que detectan no solo virus conocidos, sino también virus desconocidos.

Para ello genera un archivo de *"checksum"* (suma de control) o fingerprint (huella dactilar) por cada archivo en el directorio que lo contiene . En un análisis posterior se compara cada archivo con su archivo de checksum previamente calculado, detectando de este modo cualquier diferencia.

Un virus se copia siempre dentro de un archivo ejecutable para asegurarse el transporte a memoria y así poder copiarse a sí mismo. De esa manera no puede evitar modificar el archivo original generando un cambio "detectable".

La ventaja que otorga el método de chequeo de integridad es la de no tener necesidad de actualizar constantemente el antivirus para detectar la presencia de nuevos virus.