Concepto de **Virus** Informático

- Es un programa que tiene la capacidad de causar daño a las computadoras, empresas y personas, su característica más relevante es que puede replicarse a sí mismo y propagarse e Infectar "entidades ejecutables”.

Características de los **Virus** 1

- Es dañino. 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 eficiencia.

Características de los **Virus** 2

- Es autorreproductor. crean copias de sí mismo, cosa que ningún otro programa convencional hace.
- Es versátil: 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

Efectos 1

- La verdadera peligrosidad de un **virus** no está dada por su arsenal de instrucciones maléficas, sino por lo crítico del sistema que está infectando.
- 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**.

Efectos 2

- 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.

Efectos 3

- 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.

Efectos 4

- ¿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

Daños en el Hardware

- Los **virus** informáticos no pueden causar un daño directo sobre el hardware. No existen instrucciones que derritan la unidad de disco rígido o que estallen un monitor.
- 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

Daños en el Hardware

- 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

- 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.

Clasificación de los **Virus**

- 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.

Caballo de Troya 2

- Después de que el programa obtenga la contraseña que

deseaba, la enviará por correo electrónico a la dirección electrónica que tenga registrada la persona que implanto el caballo.

- 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 1

- 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).

Camaleones 2

- 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.

Polimorfos o Mutantes

- **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.

Polimorfos o Mutantes

- 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.

Virus Polimorfos o Mutantes

- Para eso incluye un generador de códigos al que **se** conoce como motor de mutación. Este motor 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.

Virus Polimorfos o Mutantes

- 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.

Retro **virus**

- 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.
- 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.

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.

Macrovirus

- Actualmente son los **virus** que más **se** están extendiendo a través de Internet. Representan una amenaza tanto para las redes informáticas como para los computadores independientes. Su máximo peligro está en que son completamente independientes del sistema operativo o de la plataforma. Es más,

ni siquiera son programas ejecutables.

Macrovirus

- Los macro-**virus** son pequeños programas escritos en el lenguaje propio (conocido como lenguaje script o macro-lenguaje) de un programa. Así encontramos macro-**virus** para editores de texto, hojas de cálculo y utilidades

especializadas en la manipulación de imágenes.

Macro **Virus**

- 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.

Gusanos

- **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. 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.

Gusanos

- 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".

Síntomas más Comunes de **Virus**

- Incluso el mejor software antivirus puede fallar a la hora de detectar un **virus**. La educación del personal sobre cuáles son posibles síntomas de **virus** informáticos puede ser la diferencia entre un simple dolor de cabeza y un gran problema. Veamos algunos síntomas:
- Los programas comienzan a ocupar más espacio de lo habitual.
- Aparecen o desaparecen archivos.
- Cambia el tamaño de un programa o un objeto.
- Aparecen mensajes u objetos extraños en la pantalla.
- El disco trabaja más de lo necesario.
- Los objetos que **se** encuentran en la pantalla aparecen ligeramente distorsionados.

- La cantidad de espacio libre del disco disminuye sin ningún tipo de explicación,
- **Se** modifican sin razón aparente el nombre de los archivos.
- No **se** puede acceder al disco duro.

Software antivirus

- El software antivirus es un programa más de computadora y como tal debe ser adecuado para nuestro sistema y debe estar correctamente configurado según los dispositivos de hardware que tengamos. Si trabajamos en un **lugar** que posee conexión a redes es necesario tener un programa antivirus que tenga la capacidad de detectar **virus** de redes. Los antivirus reducen sensiblemente los riesgos de infección pero cabe reconocer que no serán eficaces el cien por ciento de las veces y su utilización debería estar

acompañada con otras formas de prevención (Más información).

Recomendaciones

- Jamás ejecute ningún software sin revisarlo antes (incluidos disquetes, CDs, adjuntos a e-mails, bajados por Internet, Messenger, etc.).
- Recuerde que hasta el software original distribuido legítimamente por sus fabricantes, puede contener **virus**.
- Un caso bastante común y difícil de solventar, es cuando el PC es usado por niños o adolescentes que viven probando e intercambiando cuánto software caiga en sus manos. En esos casos, si no impone cierta disciplina, aténgase a las consecuencias. **Se** trata de un poco de sentido común.

Recomendaciones

- Archivos ejecutables o que puedan causar una modificación con solo abrirlos (Ej.: EXE, COM, BAT, REG, DLL, VBS, etc.) o que contengan macros (DOC, RTF (*), XLS, etc.), no deberían ser aceptados vía e-mail (Nota (*): Los archivos RTF por naturaleza, no pueden contener macros, sin embargo, si **se** renombra un .DOC como .RTF, Word lo abrirá sin quejarse, dando **lugar** a la ejecución de los posibles macros incluidos).
- Formatos aparentemente inocentes como .PIF, .PDF y otros, hoy día pueden llegar a contener **virus**.
- Solo archivos adjuntos en formato ASCII (.TXT) de solo texto, pueden ser abiertos sin peligro si van adjuntos a un mensaje.

Recomendaciones

- Aún en el caso de que alguien renombre un .DOC como .TXT, este no sería abierto por Word, ya que la definición a esa extensión no corresponde a ese programa (por lo general es el Bloc de notas el que los abrirá por defecto).
- Sin embargo, la extensión puede no ser la verdadera. Windows oculta por defecto las extensiones de los programas más usados. De ese modo, un archivo LEAME.TXT.EXE o LEAME.TXT.VBS sería visto como LEAME.TXT, haciéndonos creer es un archivo inocente, cuando en realidad es un ejecutable