GUIA PEDAGÓGICA N° 10 – **NIVEL SECUNDARIO.**

Escuela de Educación Técnica Obrero Argentino ETOA

Profesores: José A. Barboza Guerrero David

CURSO: 2° año todas las Div.

TURNO: MAÑANA Y TARDE

ESPACIO CURRICULAR INFORMÁTICA

TEMA:

Normas de Seguridad Informático-Reconocimiento de Virus-Malware

BIBLIOGRAFÍA:

Cuadernillo de informática

ACTIVIDADES DE APLICACIÓN

1. VIRUS INFORMÁTICOS

2. ***Definición**: son programas malicioso (Malware) que infectan a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo "victima"(normalmente en ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección. Su nombre lo adoptan de la similitud que tiene con los virus biológicos que afectan a los humanos, donde los antibióticos en este caso serían los programas antivirus.*

3. ***Antivirus**: software que permite contrarrestar los daños generados por programas maliciosos, generalmente requieren algunas interacciones por parte del usuario (por ejemplo, abrir un archivo adjunto que recibimos por correo electrónico). Hoy también existen virus que afectan los teléfonos*

celulares, como Cabir (que se desplaza a través del bluetooth y que permiten sustraer mensajes, contactos y escuchar nuestras conversaciones.)

4. MALWARE

5. El malware (abreviatura de "software malicioso") se considera un tipo molesto o dañino de software destinado a acceder a un dispositivo de forma inadvertida, sin el conocimiento del usuario. Los tipos

6. de malware incluyen spyware (software espía), adware (software publicitario), phishing, virus, troyanos, gusanos, rootkits, y secuestradores del navegador.

7. De dónde proviene el malware

El malware accede a su dispositivo a través de Internet y del correo electrónico, aunque también puede conseguir acceder a través de sitios web hackeados, demos de juegos, archivos de música, barras de herramientas, software, suscripciones gratuitas o cualquier otra cosa que descargue de Internet.

Clasificación de los Virus Informáticos

1. **Virus Residentes**: se llaman "virus residente" por la razón de que ellos están presentes permanentemente en nuestra computadora, y son ejecutados cuando una función predeterminada específica se efectúa.
2. **Virus de Acción directa**: Caso contrario de los virus residentes. Los virus de acción directa infectan nuestra computadora cuando es ejecutado enseguida, realizando todas las funciones predeterminadas por el programador a la hora de su creación.
3. **Virus de Sobre escritura**: Éstos son probablemente los virus más peligrosos. Si bien, la sobre escritura significa: "reemplazar un archivo con otro nuevo", esto quiere decir que, destruyen los archivos infectados enseguida que son ejecutados y a su vez, son reemplazados por otros archivos.
4. **Virus Boot o de Arranque**: El término boot hace referencia al sector de arranque de nuestra computadora. Los virus boot infectan nuestra computadora al introducir un disquete infectado. A partir de ese momento, todos los dispositivos extraíbles que insertemos, serán infectados posteriormente.
5. **Virus de Macro**: Los virus macros infectan aquellos documentos de la ofimática, ya sean documentos hechos en Word, Excel, Powerpoint, Access o Publisher.
6. **Virus de Archivo**: Estos virus infectan programas o ficheros ejecutables (aplicaciones EXE y COM). Al ejecutarse el programa infectado, el virus se activa y se esparce en toda la computadora, realizando la función predeterminada por el programador.

8. Cómo reconocer el malware

- ***Mi computadora me habla**: aparecen todo tipo de pop-ups y mensajes en el escritorio. Aquí podría tratarse de un software espía o un falso antivirus.*
- ***El PC va tremendamente lento**. Aunque existen varios posibles motivos, se puede dar el caso de que un Troyano esté realizando tareas que consumen recursos.*
- ***No arrancan las aplicaciones**. Es un indicio de infección, aunque puede tratarse de otro fallo.*

- ***No puedo conectarme a Internet o me conecto, pero navego muy lento****. El Malware podría estar haciendo llamadas, robando así ancho de banda.*
- ***Cuando se conecta a Internet****, se abren muchas ventanas o el navegador muestra páginas no solicitadas. Este es un signo inequívoco de infección, ya que algunas amenazas están destinadas a redirigir tráfico a ciertos sitios.*
- *¿Dónde han ido mis archivos? Existen tipos de Malware diseñados para borrar información, cifrarla o cambiarla de sitio.*

- ***Mi antivirus ha desaparecido, mi Firewall está desactivado****. Algunas amenazas se diseñan para deshabilitar el sistema de seguridad instalado.*
- ***Mi computadora me habla en un idioma raro****. Puede que la PC esté infectado si se cambian los idiomas de las aplicaciones o la pantalla se vuelve del revés.*
- ***Mi PC se ha vuelto loco****. Si el equipo realiza acciones por sí solo, como conectarse a Internet o enviar emails, tal vez la causa sea una amenaza.*

El Spyware

Es un programa espía es un software que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario de la computadora. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Un spyware típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha en la computadora (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados. Sin embargo, a diferencia de los virus, no se intenta replicar en otras computadoras, por lo que funciona como un parásito.

Las consecuencias de una infección de spyware moderada o severa (aparte de las cuestiones de privacidad) generalmente incluyen una pérdida considerable del rendimiento del sistema (hasta un 50 % en casos extremos), y problemas de estabilidad graves (la computadora se queda "colgado"). También causan dificultad a la hora de conectar a Internet. Algunos ejemplos de programas espía conocidos son Gator o Bonzi Buddy.

Virus más populares que atacan a las computadoras

Caballos de Troya

Los troyanos son programas que imitan programas útiles o ejecutan algún tipo de acción aparentemente inofensiva, pero que de forma oculta al usuario ejecutan el código dañino. Los troyanos no cumplen con la función de auto-reproducción, sino que generalmente son diseñados de forma que por su contenido sea el mismo usuario el encargado de realizar la tarea de difusión del virus. (Generalmente son enviados por e-mail)

Gusanos (Worms)

Los gusanos utilizan las redes de comunicaciones para expandirse de sistema en sistema. Es decir, una vez que un gusano entra a un sistema examina las tablas de ruta, correo u otra información sobre otros sistemas, a fin de copiarse en todos aquellos sistemas sobre los cuales encontró información. Este método de propagación presenta un crecimiento exponencial con lo que puede infectar en muy corto tiempo a una red completa.

9. ***Rootkit***

10. *Un RootKit es un programa o conjunto de programas que un intruso usa para esconder su presencia en un sistema y le permite acceder en el futuro para manipular este sistema.*
11. *Para completar su objetivo, un Rootkit altera el flujo de ejecución del sistema operativo o manipula un*
12. *conjuntos de datos del sistema para evitar la auditoria.*
13. *Es importante remarcar que un Rootkit no es un Malware en sí mismo pero, debido a que es utilizado ampliamente para ocultar los mismos, muchas veces se lo considera incorrectamente como programa dañino.*

Tipos de Virus Informáticos según sus acciones y modo de activación

Bombas
Se denominan así a los virus que ejecutan su acción dañina como si fuesen una bomba. Esto significa que se activan segundos después de verse el sistema infectado o después de un cierto tiempo (bombas de tiempo) o al comprobarse cierto tipo de condición lógica del equipo (bombas lógicas). Ejemplos de bombas de tiempo son los virus que se activan en una determinada fecha u hora determinada. Ejemplos de bombas lógicas son los virus que se activan cuando al disco rígido solo le queda el 10% sin uso, una secuencia de teclas o comandos, etc. Ejemplos de este tipo de programas son virus como Viernes 13 o el virus Miguel Ángel

Camaleones
Son una variedad de virus similares a los caballos de Troya que actúan como otros programas parecidos, 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 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 password para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

Reproductores
Los reproductores (también conocidos como conejos-rabbits) se reproducen en forma constante una vez que son ejecutados hasta agotar totalmente (con su descendencia) el espacio de disco o memoria del sistema.
La única función de este tipo de virus es crear clones y lanzarlos a ejecutar para que ellos hagan lo mismo. El propósito es agotar los recursos del sistema, especialmente en un entorno multiusuario interconectado, hasta el punto que el sistema principal no puede continuar con el procesamiento normal.

Backdoors

Son también conocidos como herramientas de administración remotas ocultas. Son programas que permiten controlar remotamente el PC infectado. Generalmente son distribuidos como troyanos.

Cuando un virus de estos es ejecutado, se instala dentro del sistema operativo, al cual monitorea sin ningún tipo de mensaje o consulta al usuario. Incluso no se le ve en la lista de programas activos. Los Backdoors permiten al autor tomar total control del PC infectado y de esta forma enviar, recibir archivos, borrar o modificarlos, mostrarle mensajes al usuario, etc....

1.
2. **SINTOMAS MÁS COMUNES DE VIRUS**
3.

- **Reducción del espacio libre en la memoria o disco duro.**

Un virus, cuando entra en un ordenador, debe situarse obligatoriamente en la memoria RAM, y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce en la misma cuantía que tiene el código del virus.

- Aparición de mensajes de error no comunes.
- Fallos en la ejecución de programas.
- Frecuentes caídas del sistema
- Tiempos de carga mayores.
- Las operaciones rutinarias se realizan con más lentitud.
- Aparición de programas residentes en memoria desconocidos.

- **Actividad y comportamientos inusuales de la pantalla**

Muchos de los virus eligen el sistema de vídeo para notificar al usuario su presencia en el ordenador. Cualquier desajuste de la pantalla, o de los caracteres de esta nos puede notificar la presencia de un virus.

- **El disco duro aparece con sectores en mal estado**

Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.

- Cambios en las características de los ficheros ejecutables
- Casi todos los virus de fichero, aumentan el tamaño de un fichero ejecutable cuando lo infectan. También puede pasar, si el virus no ha sido programado por un experto, que cambien la fecha del fichero a la fecha de infección.

PROPAGACION

Entre las principales vías de infección actualmente podemos destacar:

- Al insertar en el equipo un dispositivo USB infectado.
- Al visitar algún sitio web legítimo que haya sido infectado.
- Al descargar falsas medicinas de programas piratas o programas "con regalo"
- Al descargar un supuesto codec o actualizado de Adobe Flash para ver un vídeo
- Al abrir un archivo adjunto o seguir un enlace de un correo no solicitado (Spam)
- Al seguir un enlace infectado de un contacto en Messenger, Twitter, Facebook, etc.
- Al visitar paginas maliciosas a las cuales fuimos dirigidos por búsquedas en Google (BlackHatSEO)

Actividades:

1) ¿Defina que es un Virus Informático?
2) ¿Qué es un Malware?¿Qué incluye un Malware?¿De donde proviene un Malware? ¿Cómo reconoce un Malware?
3) ¿Clasifique los virus Informáticos? ¿Qué es un Spyware? Detalle virus Troyano y Gusano
4) ¿Cuáles son los síntomas para darnos cuenta que tenemos un virus?

DIRECTOR A CARGO: JORGE GROSSO