C.E.N.S. JUAN DE GARAY

Guía Práctica de FTP 3° Año ciclo lectivo 2020

Escuela: C.E.N.E. JUAN DE GARAY

Docente: Rojas A. Elias Kevin, Saban Marcelo

Curso: 3° año

División: 1° y 2°

Turno: Noche

Área Curricular: Formación Teórico Practico

Título de la propuesta: VIRUS INFORMATICOS

Objetivo: Entender el funcionamiento de los virus informáticos de la misma manera que un virus biológico

Virus informáticos

Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador. Aunque no todos son tan dañinos. Existen unos un poco más inofensivos que se caracterizan únicamente por ser molestos.

Métodos de Infección de los Virus Informatices

Hay muchas formas con las que un computador puede exponerse o infectarse con virus. Veamos algunas de ellas:

- Mensajes dejados en redes sociales como Twitter o Facebook.
- Archivos adjuntos en los mensajes de correo electrónico.
- Sitios web sospechosos.
- Insertar USBs, DVDs o CDs con virus.
- Descarga de aplicaciones o programas de internet.
- Anuncios publicitarios falsos.

Tipos de Virus

1. Tipos de virus informáticos residentes en memoria

Estos virus se alojan en la memoria del ordenador y se activan cuando el sistema operativo se ejecuta, infectando a todos los archivos que se abren. Permanecen allí incluso después de que se ejecute el código malicioso. Tienen control sobre la memoria del sistema y asignan bloques de memoria a través de los cuales ejecuta su propio código. Su objetivo es corromper archivos y programas cuando son abiertos, cerrados, copiados, renombrados, etc.

2. Virus de acción directa

El objetivo principal de estos tipos de virus informáticos es replicarse y actuar cuando son ejecutados. Cuándo se cumple una condición específica, el virus se pondrán en acción para infectar a los ficheros en el directorio o carpeta que se especifica en el archivo autoexec.bat Este archivo de procesamiento por lotes está siempre en el directorio raíz del disco duro y carga ciertas operaciones cuando el ordenador arranca. El virus infecta uno tras otro todos los archivos que encuentra y que previamente ha seleccionado como sus víctimas. También es capaz de infectar dispositivos externos. Cada vez que se ejecuta el código, estos tipos de virus informáticos cambian su ubicación para infectar nuevos archivos, pero generalmente se encuentra en el directorio raíz del disco duro.

3. Virus de sobreescritura

Estos tipos de virus informáticos se caracterizan por el hecho de que borran la información contenida en los ficheros que infectan, haciéndolos parcial o totalmente inútiles. Una vez infectados, el virus reemplaza el contenido del fichero sin cambiar su tamaño. La única manera de limpiar un archivo infectado por un virus de sobreescritura es borrar el archivo completamente, perdiendo así el contenido original. Sin embargo, es muy fácil de detectar este tipo de virus ya que el programa original se vuelve inútil.

4. Virus de sector de arranque

Este tipo de virus afecta al sector de arranque del disco duro. Se trata de una parte crucial del disco en la que se encuentra la información que hace posible arrancar el ordenador desde disco.

5. Virus polimórfico

Estos tipos de virus informáticos se encriptan o codifican de una manera diferente, utilizando diferentes algoritmos y claves de cifrado cada vez que infectan un sistema. Esto hace imposible

que el software antivirus los encuentre utilizando búsquedas de cadena o firma porque son diferentes cada vez.

6. Virus de secuencias de comandos web

Muchas páginas web incluyen código complejo para crear contenido interesante e interactivo. Este código es a menudo explotado por estos tipos de virus informáticos para producir ciertas acciones indeseables.

Clasificación de los Virus Informatices

Los virus informáticos son una de las grandes amenazas de la sociedad actual. Es así porque vivimos en un mundo digital e hiperconectado. Cada segundo se crean tres virus en el planeta por lo que existen infinidad de softwares maliciosos.

Como usuario de cualquier equipo informático o smartphone te interesa conocer los virus más comunes a los que estamos expuestos:

Malware

Altera el funcionamiento normal de un dispositivo destruyendo archivos o corrompiéndolos. Para seguir contagiando equipos emplean un código vía mail, por ejemplo.

Gusanos

Se caracterizan por poder multiplicarse en cada sistema a través de envío masivo de copias de sí mismo por mail u otras vías de contacto como redes domésticas y de wifi. Es muy importante tener cuidado con los datos que insertamos al estar conectados a redes inalámbricas de acceso público.

Troyano

Entra en el quipo porque nosotros mismos lo instalamos. Puede ser aparentemente un juego, un power point o cualquier otro archivo que buscamos. Al ejecutar este software el virus accede por completo al sistema.

Phishing

Consiste en el envío de correos electrónicos para obtener datos confidenciales del usuario haciéndose pasar por fuentes fiables como entidades bancarias. Suelen incluir un enlace que

lleva a páginas web falsificadas en donde si se pone la información solicitada llegará a manos del estafador.

Antivirus

Parece bastante simple y fácil de decir lo *que es un antivirus*. Quién todavía no escuchó hablar de este tipo de software, de su importancia, y de porque debe estar siempre actualizado, etc, etc?. Aquí vas a encontrar mucha información relacionada a los antivirus, para ayudarlos a entender mejor este tipo de software y cómo funcionan.

El antivirus es un programa que ayuda a proteger su computadora contra la mayoría de los virus, worms, troyanos y otros invasores indeseados que puedan infectar su ordenador.

Entre los principales daños que pueden causar estos programas están: la pérdida de rendimiento del microprocesador, borrado de archivos, alteración de datos, informacion confidencial expuestas a personas no autorizadas y la desinstalación del sistema operativo.

Con el paso de los años, los virus, malwares y demás amenazas que nos acechan cada vez que accedemos a Internet o conectamos un pendrive desconocido en nuestro equipo, han ido avanzando hasta alcanzar un nivel en que prácticamente son indetectables. Asimismo las formas en que se introducen en nuestros equipos es cada vez más sofisticada y traicionera.

Difícilmente un usuario que utiliza el sistema operativo Windows, cualquiera de sus versiones, no haya utilizado algún software antivirus en su equipo, por lo menos una vez en la vida. No queremos decir que sólo Windows es propicio al malware, pero por ser el sistema operativo más utilizado en el mundo, es el blanco preferido por los creadores de plagas digitales. Esto porque los crackers siempre intentan alcanzar al mayor número posible de usuarios.

Normalmente, los antivirus monitorizan actividades de virus en tiempo real y hacen verificaciones periódicas, o de acuerdo con la solicitud del usuario, buscando detectar y, entonces, anular o remover los virus de la computadora.

Los antivirus actuales cuentan con vacunas específicas para decenas de miles de plagas virtuales conocidas, y gracias al modo con que monitorizan el sistema consiguen detectar y eliminar los virus, worms y trojans antes que ellos infecten el sistema.

Esos programas identifican los virus a partir de «firmas», patrones identificables en archivos y comportamientos del ordenador o alteraciones no autorizadas en determinados archivos y áreas del sistema o disco rígido.
El antivirus debe ser actualizado frecuentemente, pues con tantos códigos maliciosos siendo descubiertos todos los días, los productos pueden hacerse obsoletos rápidamente. Algunos antivirus pueden ser configurados para que se actualicen automáticamente. En este caso, es aconsejable que esta opción esté habilitada.

Tipos de antivirus

Los antivirus son uno de los puntos de apoyo básicos de un sistema de seguridad personal, al lado de firewalls y de detectores de spyware. Como en las otras categorías de software, también es posible encontrar buenos antivirus gratuitos y comerciales. Normalmente, los productos monitorizan actividades de virus en tiempo real y hacen verificaciones periódicas, o de acuerdo con la solicitud del usuario.
Además de tener uno de esos programas, usted puede querer utilizar un antivirus online, que no necesita ser instalado en el ordenador. Es útil en el caso de ya haber sufrido una infección, porque algunos virus y programas maliciosos impiden el funcionamiento correcto de los antivirus, y continúan actuando después de una verificación completa del sistema.
Los antivirus online también pueden ser útiles cuando se necesita usar sistemas desconocidos o sospechosos, como ordenadores colectivos en cibercafés. Otra ventaja de los verificadores online es que están siempre actualizados, pues estan hospedados en los servidores de las propias empresas que los mantienen.

Técnicas de detección de virus

El antivirus tiene como objetivo primordial, detectar y remover los programas malwares de tu computadora. Como el primer paso es detectar, existen algunas técnicas para eso.
Entre las técnicas de detección están:
– *Verificación de Firmas*
– *Verificación Heurística*
– *Bloqueo de Comportamiento*

Técnica de verificación de firmas

La Verificación de Firmas determina las características que lleva un archivo a ser o no considerado un malware. Es verifican características como: tamaño del archivo, secuencia de instrucciones binarias, entre otras. Cuando un archivo es reconocido como un malware, recibe

una identidad propia, con su respectiva firma. Estas firmas son las que determinan cada malware que forma parte de la lista de definición del antivirus.

Este tipo de detección puede no ser muy eficiente, pues no posibilita que un nuevo malware, que aún no fue incluido en la base de datos del antivirus sea detectado. O sea, nuevos malwares no serán detectados antes de que el software antivirus tenga su lista de definición actualizada.

Técnica de Bloqueo de Comportamiento

El Bloqueo de Comportamiento es la técnica que analiza las acciones ejecutadas por los programas (acciones sospechosas), a fin de identificar posibles tentativas de invasiones o infecciones. Conforme a las acciones realizadas por algún software, él podrá ser considerado un malware y no permitírsele su ejecución.

La mayoría de los softwares antivirus hacen una combinación de estas técnicas para detectar y remover los malwares.

Actividad

1) ¿Qué son los virus Informáticos?

2) ¿Cómo se clasifican los virus informáticos?

3) ¿Cómo se infecta una computadora con virus?

4) ¿Qué tipo de virus existen?

6) ¿Qué son los antivirus?

7) ¿Cómo funcionan?