ÁREA TECNOLOGÍA E INFORMÁTICA
GRADO ONCE.
TALLER TERCER PERIODO

Desempeño: Comprende el concepto de virus e identifica diversos tipos de virus y su implicación en el funcionamiento adecuado de un equipo de cómputo.

DBA: Identifica las características de diferentes tipos de virus informáticos.

VIRUS INFORMÁTICOS

Contenido

1. Introducción.
2. Como se producen las infecciones de los virus.
3. Especies de virus.
4. Tácticas antivíricas.
5. Estrategias virales.
6. Historia.

1. Introducción:

Virus (Informática), programa de computadora que se reproduce a si mismo e interfiere con el hardware de una computadora o con un sistema operativo (el software básico qué controla la computadora). Los virus están diseñados para reproducirse y evitar su detección. Como cualquier otro programa informático, un virus debe ser ejecutado para que funcione: es decir, la computadora debe cargar el virus desde la memoria de la computadora y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus. La carga activa puede transformar o modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo.

El objetivo de un virus es destruir su computadora.

1.1 Otros programas nocivos además de los virus

Existen otros programas informáticos nocivos similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección. Estos programas se dividen en tres categorías:

a. Caballos de Troya.

b. Bombas Lógicas.

c. Gusanos.

Caballos de Troya:

Un caballo de Troya aparenta ser algo interesante e inocuo, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos.

Bomba Lógica:

Una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de teclas. Una bomba de tiempo se activa al cumplirse una condición.

Una bomba de tiempo se activa al cumplirse una condición.

Gusano:

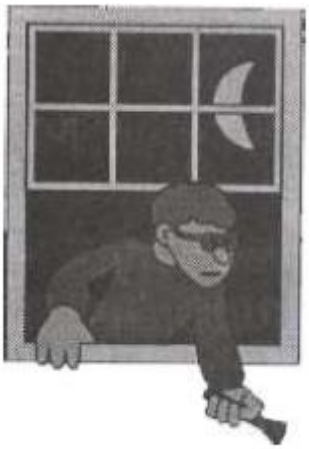
Un gusano se limita a reproducirse, pero puede ocupar memoria de la computadora y hacer que sus procesos vayan más lentos.

2. Como se reproducen las infecciones de los virus

Los virus informáticos se difunden cuando las instrucciones o código ejecutable que hacen funcionar los programas pasan de una computadora a otra. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos legítimos o a través de redes informáticas. Estas infecciones son mucho más frecuentes en PC que en sistemas profesionales de grandes computadoras, porque los programas de las PC se intercambian fundamentalmente a través de discos flexibles o de redes informáticas no reguladas.

Los virus funcionan, se reproducen y liberan sus cargas activas solo cuando se ejecutan. Por eso, si una computadora esta simplemente conectada a una red informática infectada o se limita a cargar un programa infectado, no se infectara necesariamente. Normalmente, un usuario no ejecuta conscientemente un código

informático potencialmente nocivo; sin embargo, los virus engañan frecuentemente al sistema operativo de la computadora o al usuario informático para que ejecute el programa viral.



Un virus es un intruso que desea hacer daño

Algunos virus tienen la capacidad de adherirse a programas legítimos. Esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo. Cuando se ejecuta dicho programa, lo mismo ocurre con el virus. Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca la computadora, por lo que dichos virus se ejecutan automáticamente.
En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

3. Especies de virus

Existen seis categorías de virus:

a. Parásitos
b. Del sector de arranque inicial
c. Multipartitos
d. Acompañantes
e. De vínculo
f. De fichero de datos

Virus Parásitos

Los virus parásitos infectan ficheros ejecutables o programas de la computadora. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser de acción directa o residentes. Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta. Un virus residente se oculta en la memoria del ordenador e infecta un programa determinado cuando se ejecuta dicho programa.

Virus del sector de arranque

Los virus del sector de arranque inicial residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan el ordenador. Estos virus suelen difundirse mediante el intercambio físico de discos flexibles.

Un virus es un devorador

Virus Multipartitos

Los virus Multipartitos combinan las capacidades de los virus parásitos y del sector de arranque inicial, y pueden infectar tanto ficheros como sectores de arranque inicial.

Virus Acompañantes

Los virus acompañantes no modifican los ficheros, si no que crean un nuevo programa con el mismo nombre que un programa legítimo y engañan al sistema operativo para que lo ejecute. Los virus de vínculo modifican la forma en que el sistema operativo encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa diseñado.

Virus de Vinculo

Un virus de vinculo puede infectar todo un directorio (sección) de una computadora, y cualquier programa ejecutable al que se acceda en dicho directorio desencadena el virus.

Virus de Ficheros

Otros virus infectan programas que contienen lenguajes de marcos potentes (lenguajes de programación que permiten al usuario crear nuevas características y herramientas) que pueden abrir, manipular y cerrar ficheros de datos. Estos virus, llamados virus de ficheros de daros, están escritos en lenguajes de macros y se ejecutan automáticamente cuando se abre el programa legítimo. Son independientes de la máquina y del sistema operativo.

4. Tácticas antivíricas

4.1 Preparación y Prevención

Los usuarios pueden prepararse frente a una infección viral tomando en cuenta las siguientes recomendaciones:

a. Creando regularmente copias de seguridad del software original legítimo y de los ficheros de datos, para poder recuperar el sistema informático en caso necesario.

b. Copiar en un disco flexible el software del sistema operativo y proteger el disco contra escritura, para que ningún virus pueda sobrescribir el disco.

c. Obteniendo los programas de fuentes legítimas, empleando una computadora en cuarentena para proteger los nuevos programas y protegiendo contra escritura los discos flexibles siempre que sea posible.

Un Anti-virus es como un policía cuyo objetivo es proteger la propiedad privada

4.2 Detección de virus

Para detectar la presencia de un virus pueden emplearse varios tipos de programas antivíricos, entre los cuales tenemos los siguientes:

Los programas de rastreo

Estos programas pueden reconocer las características del código informático de un virus y buscar estas características en los ficheros de las computadoras. Como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces.

Algunos programas de rastreo buscan características habituales de los programas virales; suelen ser menos fiables.

Detectores de comprobación de suma

Los únicos programas que detectan todos los virus son los de comprobación de suma, que emplean cálculos matemáticos para comparar el estado de los programas ejecutables antes y después de ejecutarse.

Si la suma de comprobación no cambia, el sistema no está infectado. Los programas de comprobación de suma, sin embargo, solo pueden detectar una infección después de que se produzca.

Programas de vigilancia

Estos programas detectan actividades potencialmente nocivas, como la sobre escritura de ficheros informáticos o el formateo del disco duro de la computadora.

Los programas caparazones de integridad establecen capas por las que debe pasar cualquier orden de ejecución de un programa. Dentro del caparazón de integridad se efectúa automáticamente una comprobación de suma, y se detectan programas infectados no se permite que se ejecuten.

4.3 Contención y recuperación

Una vez detectada una infección viral, esta puede contenerse de la siguiente forma:

a. Aislando inmediatamente las computadoras de la red

b. Deteniendo el intercambio de ficheros y empleando sólo discos protegidos contra escritura.

Utilice cualquier medio posible para aniquilar los virus de su computadora

Para que un sistema informático se recupere de una infección viral debe considerarse lo siguiente:

a. Hay que eliminar el virus. Algunos programas antivirus intentan eliminar los virus detectados, pero a veces los resultados no son satisfactorios.

b. Se obtienen resultados más fiables desconectando la computadora infectada, arrancándola de nuevo desde un disco flexible protegido contra escritura, borrando los ficheros infectados y sustituyéndolos por copias de seguridad de ficheros legítimos y borrando los virus que pueda haber en el sector de arranque inicial.

5. Estrategias Virales

Los autores de un virus cuentan con varias estrategias para escapar de los programas antivirus y propagar sus creaciones con más eficacia, por lo cual tenemos los siguientes tipos de virus:

a. Los llamados virus polimorfitos

Efectúan variaciones en las copias de sí mismos para evitar su detección por los programas de rastreo.

b. Los virus sigilosos

Se ocultan del sistema operativo cuando este comprueba el lugar en que reside el virus, simulando los resultados que proporcionaría un sistema no infectado.

c. Los virus llamados infectores rápidos

No solo infectan los programas que se ejecutan si no también los que simplemente se abren. Esto hace que la ejecución d programas de rastreo antivírico en una computadora infectada por este tipo de virus pueda llevar a la infección de todos los programas de la computadora.

d. Los virus llamados infectores lentos

Infectan los archivos solo cuando se modifican, por lo que los programas de comprobación de suma interpretan que el cambio de suma es legítimo.

e. Los llamados infectores escasos

Solo infectan en algunas ocasiones: por ejemplo, pueden infectar un programa de cada 10 que se ejecutan. Esta estrategia hace más difícil detectar el virus.

6. Historia

En 1949, el matemático estadounidense de origen húngaro John Von Neumann, en el instituto de estudios avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se produjera. Esta teoría se comprobó experimentalmente en la década de 1950 en los laboratorios Bell, donde se desarrolló un juego llamado Core Wars en el que los jugadores creaban minúsculos programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él. En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuño el término de "Virus" para describir un programa informático que se reproduce a sí mismo. En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. Pronto les siguió un sinnúmero de virus cada vez más complejos. El virus llamado Brain apareció en 1986, y en 1987 se había extendido por todo el mundo. En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzo estados unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimorfito en 1990. En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.

ACTIVIDAD:

RESPONDA EN EL CUADERNO LAS SIGUIENTES PREGUNTAS:

1. ¿Qué es un virus?
2. ¿En qué parte de la computadora se cargan los virus?
3. ¿Qué otros programas nocivos existen además de los virus?
4. ¿Qué es un Caballo de Troya?
5. ¿Qué es una Bomba Lógica?
6. ¿Qué es un gusano?
7. ¿Cómo se difunden los virus?
8. ¿Una vez activado el virus como se reproduce?
9. ¿Qué capacidad tienen algunos virus?
10. ¿Cuáles son las 6 categorías de virus?
11. ¿Qué son los virus parásitos?
12. ¿Qué son los virus de arranque?
13. ¿Qué son los virus Multipartitos?
14. ¿Qué son los virus acompañantes?
15. ¿Qué son virus de vinculo?
16. ¿Qué son virus de ficheros?
17. ¿Mencione 3 tácticas antivíricas?
18. ¿Mencione 3 formas de prepararse y prevenirse contra los virus?
19. ¿Mencione los tres tipos de antivirus que existen?
20. ¿Qué son los programas de rastreo de virus?
21. ¿Qué son los programas antivirus de comprobación de suma?
22. ¿Qué son los programas antivirus de vigilancia?
23. ¿Una vez detectado el virus como puede detenerse su propagación?
24. ¿Cómo se puede recuperar un sistema de una infección viral?
25. ¿Qué son los virus poliformicos?

26. ¿Qué son los virus sigilosos?
27. ¿Qué son los virus infectores rápidos?
28. ¿Qué son los virus infectores lentos?
29. ¿Qué son los virus infectores escasos?
30. ¿Mencione algunos virus y su fecha de aparición?

PROFESOR: LUIS GERMAN AGUDELO CAMACHO.