Clase encuentro 7 6 de Mayo 2017

**Sumario**: Antecedentes, conceptualización, clasificación, y comportamiento de los virus y antivirus informáticos.

.

**Objetivo:**

Caracterizar los principales elementos que identifican los virus y Antivirus como parte fundamental en la seguridad informática.

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.

Tipos de Virus

Existen diversas clasificaciones de los virus. Cada una de ellas clasifica según una característica, ya sea dependiendo de la técnica usada, su origen, lugar donde se esconde, ficheros a los que ataca, daños que produce, etc. No se puede considerar que ninguna de estas clasificaciones sea errónea, ya que muchas de ellas tienen muchos puntos en común. A pesar de que todos se pueden considerar virus, los hemos separado en distintas “categorías”:

Virus residentes

Este tipo de virus se oculta en la memoria principal del sistema (RAM) de tal manera que pueden controlar todas las operaciones realizadas en el Sistema Operativo, pudiendo infectar todos los archivos que deseen. Normalmente sus creadores le indican una serie de condiciones (fecha, hora,...) bajo las cuales llevará cabo la acción para la cual fue programado.

Ejemplos de este tipo de virus son: Randex, CMJ, Meve.

Virus de acción directa

Estos virus no se ocultan en la memoria. Su función amiento consiste en que una vez cumplida una determinada condición, actuarán buscando los ficheros a infectar dentro de su mismo directorio o en aquellos directorios que se encuentren especificados en la línea PATH del fichero AUTOEXEC.BAT. Este tipo de virus se puede desinfectar totalmente y recuperar los archivos infectados.

Virus de sobre escritura

Se escriben dentro del contenido del fichero infectado, haciendo que pueda quedar inservible. Se ocultan por encima del fichero de tal forma que la única manera de desinfectarlo es borrar dicho archivo, perdiendo su contenido. Algún ejemplo: Trj.Reboot, Trivial.88.D.

Virus de boot o arranque

Son aquellos virus que no infectan a ficheros directamente, sino que actúan sobre los discos que los contienen, más concretamente al sector de arranque de dichos discos, de tal manera que si un ordenador se arranca con un disquete infectado, el sector de arranque del disco duro se infectará. A partir de este momento, se infectarán todas las unidades de disco del sistema.Algún ejemplo de virus de boot: Polyboot.B.

Virus de FAT

Tipo de virus muy dañino ya que atacan a la FAT (Tabla de Asignación de Ficheros), que es la encargada de enlazar la información del disco. Al atacar dicha tabla, impiden el acceso a ciertos ficheros o directorios críticos del sistema, provocando pérdidas de la información contenida en dichos ficheros o directorios. Reproductores o conejos Virus cuya característica principal es reproducirse constantemente hasta terminar ya sea con la capacidad total del disco duro o con la capacidad de la memoria principal. Esto lo consiguen simplemente creando clones de sí mismos que harán lo mismo que ellos, reproducirse.

Métodos de infección

A la hora de realizar la infección se pueden utilizar diferentes técnicas. Algunas podrían ser las siguientes:

**Añadidura o empalme**: Consiste en agregar al final del archivo ejecutable el código del virus, para que así una vez se ejecute el archivo, el control pase primeramente al virus y tras ejecutar la acción que desee, volverá al programa haciendo que funcione de manera normal. El inconveniente de esta técnica es que el tamaño del archivo será mayor que el original haciendo que sea más fácil su detección.

**Inserción**: No es una técnica muy usada por los programadores de virus ya que requiere técnicas de programación avanzadas. El motivo es que este método consiste en insertar el código del virus en zonas de código no usadas dentro del programa infectado. Así lo que se consigue es que el tamaño del archivo no varíe, pero el detectar las zonas de código en donde puede ser insertado el virus es complejo.

**Reorientación**: Es una variante del método de inserción. Consiste en introducir el código del virus en zonas del disco que estén marcadas como defectuosas o en archivos ocultos del sistema. Al ejecutarse introducen el código en los archivos ejecutables infectados. La ventaja principal es que al no estar insertado en el archivo, su tamaño puede ser mayor con lo que podría tener una mayor funcionalidad. Como inconveniente se encuentra su fácil eliminación ya que bastaría con eliminar archivos ocultos sospechosos o con sobrescribir las zonas del disco marcadas como defectuosas.

CÓMO ELIMINAR UN VIRUS INFORMÁTICOS

La prevención consiste en un punto vital a la hora de proteger nuestros equipos ante la posible infección de algún tipo de virus y para esto hay tres puntos vitales que son:

* **Un programa Antivirus.**
* **Un programa Cortafuegos.**
* **Un “poco” de sentido común.**

Normas básicas que le ayudarán a protegerse de los virus informáticos:

* Instale en su computador un software Antivirus confiable.
* Actualice con frecuencia su software Antivirus (mínimo dos veces al mes).
* Analice con un software Antivirus actualizado, cualquier correo electrónico antes de abrirlo, así conozca usted al remitente.
* Analice siempre con un software Antivirus los archivos en disquete o Cd-Rom antes de abrirlos o copiarlos a su computador.
* No descargue, ni mucho menos ejecute, archivos adjuntos (attachement) a un mensaje de correo electrónico sin antes verificar con la persona que supuestamente envió el mensaje, si efectivamente lo hizo.
* No ejecute nunca un programa de procedencia desconocida, aun cuando el software Antivirus indique que no está infectado. Dicho programa puede contener un troyano o un sniffer que reenvíe a otra persona su clave de acceso u otra información.
* Instale los parches de actualización de software que publican las compañías fabricantes para solucionar vulnerabilidades de sus programas. De esta manera se puede hacer frente a los efectos que puede provocar la ejecución de archivos con códigos maliciosos.
* Nunca abra archivos adjuntos a un mensaje de correo electrónico cuya extensión sea “.exe”, “.vbs”, “.pif”, “.bat” o “.bak”.
* Cerciórese que el archivo adjunto no tenga doble extensión. Por ejemplo: “NombreArchivo.php.exe”.

Virus informáticos más destructivos de los últimos años

**Carta de amor/ I LOVE YOU (2000)**

En el año 2000, millones de personas cometieron el error de abrir lo que parecía ser un correo electrónico de un admirador secreto. Llevaba por título simplemente “I Love You”, pero en vez de ser una confesión amorosa, realmente era un “gusano”, que después de sobrescribir las imágenes de los usuarios se mandaba por correo electrónico a 50 contactos de la agenda Windows del usuario. En tan sólo una s horas se convirtió en una infección global.

**Code Red (2001)**

Comparado al malware moderno Code Red parece no ser tan peligroso, sin embargo en el 2001 sorprendió a expertos de seguridad en línea al utilizar una falla en el Servidor de Información de Microsoft, logrando bajar y cambiar algunos sitios web. El más memorable quizá fue el sitio de la Casa Blanca: whitehouse.gov y obligó también a otros sitios gubernamentales a bajar sus páginas momentáneamente.

**Slammer (2003)**

En enero del 2003, Slammer probó que tan dañino podía ser un gusano para los servicios públicos y privados. El gusano liberaba una avalancha de paquetes de red, y la cantidad de datos que transmitía a través del internet causó que varios servidores suspendieran actividades casi inmediatamente. Entre las víctimas del gusano se encontraron Bank of America, el servicio de emergencias estadounidense 911 y una planta nuclear en Ohio.

**Fizzer (2003)**

Los gusanos que se habían visto hasta el año 2004 eran principalmente para crear un poco de caos, Fizzer, iba tras el dinero. Muchos desestimaron al gusano ya que no se movía con la rapidez de Code Red, pero lo que lo hacía más peligroso es que era un gusano creado para obtener ganancias –una vez en tu correo electrónico enviaba correos no solo para propagarse, si no para enviar spam de porno y pastillas.

**My Doom (2004)**

En el 2004 logró infectar alrededor de un millón de máquinas lanzando una negación masiva del servicio de ataque, al hacer esto abruma a su objetivo al enviarle información de diversos sistemas. El gusano se propagaba por correo electrónico y lo hizo con una rapidez jamás antes vista.

**PoisonIvy (2005)**

Es la pesadilla de todo sistema de seguridad ya que permite que el virus controle la computadora que ha infectado. PoisonIvy pertenece al grupo de malware conocido como “un troyano remoto”, ya que le permite al creador del virus tener acceso completo a las máquinas que infectado usando una especie de puerta trasera, al grado que permite grabar y manipular información del equipo. Inicialmente se le consideró una herramienta de hackers principiantes, el virus ha llegado a afectar a muchas compañías de occidente.

**Zeus (2007)**

Actualmente es el malware más usado para obtener, de manera ilegal, información personal. Se puede comprar por un precio de 50 centavos de dólar en el mercado del crimen virtual y permite robar contraseñas y archivos. La información personal robada puede ser utilizada para hacer compras en línea o crear cuentas bancarias a nombre de una identidad comprometida.

**agent.btz (2008)**

Este malware fue el responsable de la creación de un nuevo departamento militar en Estados Unidos, el Cyber Command. El virus se propaga a través de memorias infectadas que instalan un malware que roba información. Cuando se encontró agent.btz en computadoras del Pentágono, sospecharon que era el trabajo de espías extranjeros.

**Virus Conficker (2009)**

En el 2009 este nuevo virus afectó a millones de máquinas con Windows en todo el mundo. Logró crear una especia de ejército global que robaba todo tipo de información. Debido a que era realmente difícil de parar se creó un grupo de expertos dedicados específicamente a detenerlo, el virus se llegó a conocer como el “súper bicho”, o “super gusano”. Lo que ha dejado a los expertos realmente perplejos es que nadie sabe para qué es exactamente, la información robada jamás se utilizó.

**Stuxnet (2009-2010)**

Este virus fue el primero en ser creado para causar daño en el mundo real y no sólo en el mundo virtual. El malware tenía como objetivo principal dañar sistemas industriales –se cree que el virus fue responsable de causar daños al equipo que procesaba uranio en una planta de Natanz en Irán-. Basándose en información de la Agencia Internacional de Energía Atómica, los expertos creen que el virus fue responsable de causar que muchas centrifugues que procesaban uranio en Irán giraran hasta perder el control y se auto-destruyeran. El virus no se descubrió hasta el 2010 pero sospechan que infectó computadoras desde el 2009.

Concepto de Antivirus

Un antivirus es una aplicación o programa que identifica y elimina a los programas malignos en las computadoras; ayudan a eliminar algunas amenazas a la seguridad computacional que no necesariamente clasifican como programas malignos. Pueden realizar varias funciones en dependencia de su configuración, como por ejemplo anti–hacker, anti–spam, defensa proactiva y muchas más.

Antecedentes:

Los antivirus son programas surgidos durante la década de 1990 cuyo objetivo es detectar o eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e internet los antivirus han evolucionado hacia programas más avanzados que además de buscar detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos. Actualmente son capaces de reconocer otros tipos de malware como spyware, gusanos, troyanos, rootkits, etc.

Características que debe poseer un sistema antivirus

La expresión "cuál es el mejor antivirus", puede variar de un usuario a otro. Es evidente que para un usuario inexperto el término define casi con seguridad al software que es más fácil de instalar y utilizar, algo

totalmente intranscendente para usuarios expertos, administradores

de redes, etc.4

No se puede afirmar que exista un solo sistema antivirus que presente

todas las características necesarias para la protección total de las computadoras; algunos fallan en unos aspectos, otros tienen determinados problemas o carecen de ciertas facilidades. De acuerdo con los diferentes autores consultados, las características esenciales son las siguientes:

1. Gran capacidad de detección y de reacción ante un nuevo virus.

2. Actualización sistemática.

3. Detección mínima de falsos positivos o falsos virus.

4. Respeto por el rendimiento o desempeño normal de los equipos.

5. Integración perfecta con el programa de correo electrónico.

6. Alerta sobre una posible infección por las distintas vías de entrada (Internet, correo electrónico, red o discos flexibles).

7. Gran capacidad de desinfección.

8. Presencia de distintos métodos de detección y análisis.

9. Chequeo del arranque y posibles cambios en el registro de las aplicaciones.

10. Creación de discos de emergencia o de rescate.

11. Disposición de un equipo de soporte técnico capaz de responder en un tiempo mínimo (ejemplo 48 horas) para orientar al usuario en caso de infección.

Clasificación de los antivirus

**Preventores**: Los programas que previenen la infección, quedan residentes en la memoria de la computadora todo el tiempo y monitorean algunas funciones del sistema.

**Identificadores**: Estos productos antivirus identifican programas malignos específicos que infectan al sistema. Los mismos trabajan con las características de un programas malignoss o sus variantes, o exploran el sistema buscando cadenas (secuencias de bytes) de códigos particulares o patrones característicos de los mismos para identificarlos.

**Descontaminadores**: Sus características son similares a los productos identificadores, con la diferencia que su principal función es descontaminar a un sistema que ha sido infectado, eliminando el programas malignos y retomando el sistema a su estado original por lo que tiene que ser muy preciso en la identificación de los programas malignos contra los que descontaminan.

Principales programas Antivirus

**Panda Antivirus Pro 2017**

Panda se ha establecido, en los últimos años, como el gran modelo a seguir dentro de los programas antivirus para Windows y Mac. No es perfecto –¿qué lo es?–, pero casi. Desarrollado por una compañía española con el mismo nombre. Ofrece una extraordinaria eficacia contra todo tipo de software malicioso (hay programas a la par, pero ninguno que lo supere), su escudo anti phishing no presenta grieta alguna y, al mismo tiempo, Panda es la suite de seguridad más veloz, más discreta y que, junto con Norton, menos impacto tiene en el rendimiento del ordenador.

**Norton Security 2017**

Norton Antivirus (o Norton Security como se llama ahora), el producto estrella de la compañía californiana Symantec, es ya un viejo conocido entre los usuarios de PC y una de las marcas más importantes de la industria. Tras tantos años en el mercado, los responsables de Norton saben desde luego cómo entregar un buen antivirus. Este programa de protección para Windows obtiene unos magníficos resultados en las pruebas antimalware de AV-Test, presenta (tal y como acostumbra) una interfaz limpia e intuitiva, sólidas herramientas de seguridad y, ello, sin tener apenas impacto en el rendimiento del sistema.

**McAfee Antivirus Plus & Internet Security 2017**

El McAfee Antivirus Plus 2017 ha logrado obtener excelentes puntuaciones en los principales laboratorios independientes, tanto a nivel de protección como de rendimiento. Perteneciente a la compañía californiana McAfee, Incluye una enorme cantidad de herramientas adicionales y, como ocurre con Norton, al comprar el producto puedes proteger todos tus dispositivos Windows, Mac, iOS y Android. Si posees varios dispositivos y andas a la caza del mejor software antivirus de 2017.

**Kaspersky Anti-Virus 2017**

Kaspersky es una reconocida marca, con tradición y prestigio en el mundo de la seguridad informática, y su último programa de protección para Windows se halla por completo a la altura de semejante nombre. Las pruebas de los laboratorios tecnológicos independientes más autorizados lo avalan: a día de hoy no existe otro antivirus más eficaz contra los códigos maliciosos. Pero es que su escudo anti phishing (término éste que engloba los fraudes informáticos por abuso de identidad) tampoco le va en absoluto en la zaga. Ofreciendo además, la suite Kaspersky Anti-Virus 2016, muy útiles funciones adicionales de protección y limpieza para tu PC.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **Puntuación de protección**  Indica lo completa que es la protección tanto en línea como sin conexión. | 100% | 98% | 96% | 93% |
| **Compatible Windows 10**  Compatibilidad garantizada con Windows 10 |  |  |  |  |
| **Protección Antivirus**  Detección y protección frente a malware, virus y más. |  |  |  |  |
| **Protección Anti-Phising**  Mantiene seguros todos tus datos económicos y privados |  |  |  |  |
| **Protección de Contraseñas**  Recuerda y asegura tus contraseñas |  |  |  |  |
| **Cortafuegos**  Mantiene tu ordenador a salvo de hackers y otras amenazas |  |  |  |  |
| **Sistemas compatibles**  Dispositivos que puedes proteger usando este software |  |  |  |  |
| **Cantidad de Dispositivos**  La cantidad de dispositivos que puedes proteger con una sola suscripción. | 1-10 | 1-10 | 1-ilimitado | 1-10 |

Estudio Independiente

1. Identificar el Antivirus usado en sus empresas.
2. Ventajas y Desventajas del Uso de Ese Antivirus.
3. De Los Tipos de Virus investigar sobre:

**Retrovirus, Virus de enlace o directorio**

1. De los Métodos de infección investigar sobre:

**Polimorfismo, Sustitución**, **Tunneling**