Informática I

¿Qué es Virus Informático?

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

¿Como Trabajan los Virus Informáticos?

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, se replican a sí mismos; como el gusano informático, son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Los Virus en Microsoft-Windows

Las mayores incidencias se dan en el sistema operativo Windows debido, entre otras causas, a:

Su gran popularidad, como sistema operativo, entre los computadores personales, PC. Se estima que, en 2007, un 90% de ellos usaba Windows. Esta popularidad basada en la facilidad de uso sin conocimiento previo alguno, motiva a los creadores de software malicioso a desarrollar nuevos virus; y así, al atacar sus puntos débiles, aumentar el impacto que generan.

Los Virus en Microsoft-Windows

Falta de seguridad en esta plataforma (situación a la que Microsoft está dando en los últimos años mayor prioridad e importancia que en el pasado). Al ser un sistema muy permisivo con la instalación de programas ajenos a éste, sin requerir ninguna autentificación por parte del usuario o pedirle algún permiso especial para ello en los sistemas más antiguos (en los Windows basados en NT se ha mejorado, en parte, este problema). A partir de la inclusión del Control de Cuentas de Usuario en Windows Vista o Windows 7, y siempre y cuando no se desactive, se ha solucionado este problema.

Los Virus en Microsoft-Windows

Software como Internet Explorer y Outlook Express, desarrollados por Microsoft e incluidos de forma predeterminada en las últimas versiones de Windows, son conocidos por ser vulnerables a los virus ya que éstos aprovechan la ventaja de que dichos programas están fuertemente integrados en el sistema operativo dando acceso completo, y prácticamente sin restricciones, a los archivos del sistema.

Los Virus en Microsoft-Windows

Un ejemplo famoso de este tipo es el virus ILOVEYOU, creado en el año 2000 y propagado a través de Outlook.

La escasa formación de un número importante de usuarios de este sistema, lo que provoca que no se tomen medidas preventivas por parte de estos, ya que este sistema está dirigido de manera mayoritaria a los usuarios no expertos en informática. Esta situación es aprovechada constantemente por los programadores de virus.

Los Virus en Unix y derivados

En otros sistemas operativos como las distribuciones GNU/Linux, BSD, Open Solaris, Solaris, Mac OS X y otros basados en Unix las incidencias y ataques son prácticamente inexistentes. Esto se debe principalmente a:

Los Virus en Unix y derivados

- Los programadores y usuarios de sistemas basados en Unix han considerado la seguridad como una prioridad por lo que hay mayores medidas frente a virus, tales como la necesidad de autenticación por parte del usuario como administrador o *root* para poder instalar cualquier programa adicional al sistema.
- Los directorios o carpetas que contienen los archivos vitales del sistema operativo cuentan con permisos especiales de acceso, por lo que no cualquier usuario o programa puede acceder fácilmente a ellos para modificarlos o borrarlos. Existe una jerarquía de permisos y accesos para los usuarios.

Los Virus en Unix y derivados

A diferencia de los usuarios de Windows, la mayoría de los usuarios de sistemas basados en Unix no pueden normalmente iniciar sesiones como usuarios "administradores' o por el súper usuario root, excepto para instalar o configurar software, dando como resultado que, incluso si un usuario no administrador ejecuta un virus o algún software malicioso, éste no dañaría completamente el sistema operativo ya que Unix limita el entorno de ejecución a un espacio o directorio reservado llamado comúnmente home. Aunque a partir de Windows Vista, se pueden configurar las cuentas de usuario de forma similar.

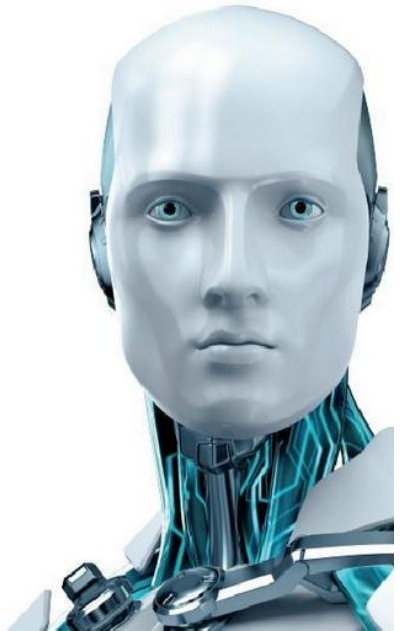
Los Virus en Unix y derivados

Estos sistemas, a diferencia de Windows, son usados para tareas más complejas como servidores que por lo general están fuertemente protegidos, razón que los hace menos atractivos para un desarrollo de virus o software malicioso.

En el caso particular de las distribuciones basadas en GNU/Linux y gracias al modelo colaborativo, las licencias libres y debido a que son más populares que otros sistemas Unix, la comunidad aporta constantemente y en un lapso de tiempo muy corto actualizaciones que resuelven bugs y/o agujeros de seguridad que pudieran ser aprovechados por algún malware.

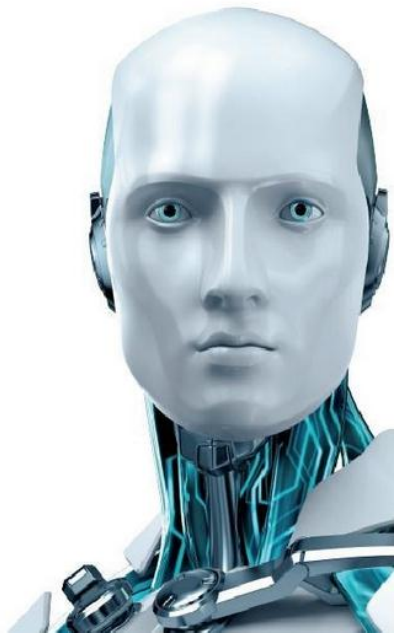
Activos

Antivirus: son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad. Por ejemplo, al verse que se crea un archivo llamado Win32.EXE.vbs en la carpeta C:\Windows\%System32%\ en segundo plano, ve que es comportamiento sospechoso, salta y avisa al usuario.



Activos

Filtros de ficheros: consiste en generar filtros de ficheros dañinos si el computador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.



Pasivos

- ✓ Evitar introducir a tu equipo medios de almacenamiento extraíbles que consideres que pudieran estar infectados con algún virus.
- ✓ No instalar software "pirata", pues puede tener dudosa procedencia.
- ✓ No abrir mensajes provenientes de una dirección electrónica desconocida.
- ✓ No aceptar e-mails de desconocidos.
- ✓ Informarse y utilizar sistemas operativos más seguros.
- ✓ No abrir documentos sin asegurarnos del tipo de archivo. Puede ser un ejecutable o incorporar macros en su interior.

Tipos de Virus

Existen diversos tipos de virus, varían según su función o la manera en que éste se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

- ✓ Troyano
- ✓ Gusano
- ✓ Bombas lógicas o de tiempo
- ✓ Hoax
- ✓ Joke

Troyano

En informática, se denomina troyano o caballo de Troya a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera (en inglés backdoor) que permite la administración remota a un usuario no autorizado.

Troyano

Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Los troyanos se concibieron como una herramienta para causar el mayor daño posible en el equipo infectado. En los últimos años y gracias al mayor uso de Internet, esta tendencia ha cambiado hacia el robo de datos bancarios o información personal.

Un troyano no es de por sí, un virus informático, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus, consiste en su finalidad. Para que un programa sea un "troyano" sólo tiene que acceder y controlar la máquina anfitriona sin ser advertido.

Gusano

Un gusano informático es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Y se propagan de ordenador a ordenador, y tienen la capacidad a propagarse sin la ayuda de una persona. Lo más peligroso de los gusanos informáticos es su capacidad para replicarse en tu sistema, por lo que tu ordenador podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador enorme

Gusano

Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda). Y es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos (es decir, a otras terminales en la red) y son capaces de llevar esto a cabo sin intervención del usuario propagándose, utilizando Internet, basándose en diversos métodos, como SMTP, IRC, P2P entre otros.

Bombas lógicas o de tiempo

Una **bomba lógica** es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa. Por ejemplo, un programador puede ocultar una pieza de código que comience a borrar archivos cuando sea despedido de la compañía (en un disparador de base de datos (trigger) que se dispare al cambiar la condición de trabajador activo del programador).

Bombas lógicas o de tiempo

El software que es inherentemente malicioso, como virus o gusanos informáticos, frecuentemente contiene bombas lógicas que ejecutan algún programa en un tiempo predefinido o cuando cierta condición se cumple. Esta técnica puede ser usada por un virus o un gusano para ganar ímpetu y para esparcirse antes de ser notado. Muchos virus atacan sus sistemas huéspedes en fechas específicas, tales como un viernes 13. Los troyanos que se activan en ciertas fechas son llamados frecuentemente bombas de tiempo.

Para ser considerado una bomba lógica, la acción ejecutada debe ser indeseada y desconocida al usuario del software. Por ejemplo los programas demos, que desactivan cierta funcionalidad después de un tiempo prefijado, no son considerados como bombas lógicas.

HOAX

Un bulo, (también conocidos como HOAX en inglés) o noticia falsa, es un intento de hacer creer a un grupo de personas que algo falso es real.

Es un mensaje de correo electrónico con contenido falso o engañoso y atrayente. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante que parece provenir de una fuente seria y fiable, o porque el mismo mensaje pide ser reenviado.

HOAX

Las personas que crean bulos suelen tener como objetivo captar indirectamente direcciones de correo electrónico (para mandar correo masivo, virus, mensajes con suplantación de identidad, o más bulos a gran escala), o también engañar al destinatario para que revele su contraseña o acepte un archivo de malware, o también de alguna manera confundir o manipular a la opinión pública de la sociedad.

Básicamente, los bulos pueden ser alertas sobre virus incurables; falacias sobre personas, instituciones o empresas, mensajes de temática religiosa; cadenas de solidaridad; cadenas de la suerte; métodos para hacerse millonario; regalos de grandes compañías; leyendas urbanas; y otras cadenas.

JOKE

Un joke es un tipo de virus informático, cuyo objetivo es crear algún efecto molesto o humorístico como una broma. Es el tipos de malware que menos daño produce sobre el ordenador.

Los joke producen efectos muy variados:

Hay una gran cantidad de jokes que hacen efectos sobre el cursor. Por ejemplo, tambalearlo o cambiar su icono cada pocos segundos

Otros juegan directamente con la imagen del monitor, haciéndola girar o dando un efecto de temblor.

JOKE

También hay algunos que abren y cierran constantemente la bandeja de CD o DVD, a la vez que muestran mensajes humorísticos en el monitor

En ocasiones un joke puede producir efectos que al principio pueden asustar, colocando en el monitor una imagen en la que, por ejemplo, parezca que el ordenador ha sido totalmente formateado, con lo que reinicia, apaga o suspende el sistema (normalmente es apagado).

ANTIVIRUS

En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, etc.

ANTIVIRUS

Es conveniente disponer de una licencia activa de antivirus. Dicha licencia se empleará para la generación de discos de recuperación y emergencia. Sin embargo no se recomienda en una red el uso continuo de antivirus.

El motivo radica en la cantidad de recursos que dichos programas obtienen del sistema, reduciendo el valor de las inversiones en hardware realizadas.

ANTIVIRUS

Aunque si los recursos son suficientes, este extra de seguridad puede ser muy útil.

Sin embargo los filtros de correos con detectores de virus son imprescindibles, ya que de esta forma se asegurará una reducción importante de elecciones de usuarios no entrenados que pueden poner en riesgo la red.

Los virus más comunes son los troyanos y gusanos, los cuales ocultan tu información, creando Accesos Directos.

ANTIVIRUS

Tipos de vacunas:

- ✓ **Sólo detección**: Son vacunas que sólo actualizan archivos infectados sin embargo no pueden eliminarlos o desinfectarlos.
- ✓ **Detección y desinfección**: son vacunas que detectan archivos infectados y que pueden desinfectarlos.
- ✓ **Detección y aborto de la acción**: son vacunas que detectan archivos infectados y detienen las acciones que causa el virus
- ✓ **Comparación por firmas**: son vacunas que comparan las firmas de archivos sospechosos para saber si están infectados.
- ✓ **Comparación de firmas de archivo**: son vacunas que comparan las firmas de los atributos guardados en tu equipo.
- ✓ **Por métodos heurísticos**: son vacunas que usan métodos heurísticos para comparar archivos.
- ✓ **Invocado por el usuario**: son vacunas que se activan instantáneamente con el usuario.
- ✓ **Invocado por la actividad del sistema**: son vacunas que se activan instantáneamente por la actividad del sistema operativo.

ANTIVIRUS

Clasificación de Antivirus:

- ✓ **ANTIVIRUS PREVENTORES**
- ✓ **ANTIVIRUS IDENTIFICADORES**
- ✓ **ANTIVIRUS DESCONTAMINADORES**
- ✓ **CORTAFUEGOS O FIREWALL**
- ✓ **ANTIESPÍAS O ANTISPYWARE**
- ✓ **ANTIPOP-UPS**
- ✓ **ANTISPAM**

ANTIVIRUS

Clasificación de Antivirus:

- **ANTIVIRUS PREVENTORES**

Como su nombre lo indica, este tipo de antivirus se caracteriza por anticiparse a la infección, previniéndola. De esta manera, permanecen en la memoria de la computadora, monitoreando ciertas acciones y funciones del sistema.

- **ANTIVIRUS IDENTIFICADORES**

Esta clase de antivirus tiene la función de identificar determinados programas infecciosos que afectan al sistema. Los virus identificadores también rastrean secuencias de bytes de códigos específicos vinculados con dichos virus.

- **ANTIVIRUS DESCONTAMINADORES**

Comparte una serie de características con los identificadores. Sin embargo, su principal diferencia radica en el hecho de que el propósito de esta clase de antivirus es descontaminar un sistema que fue infectado, a través de la eliminación de programas malignos. El objetivo es retornar dicho sistema al estado en que se encontraba antes de ser atacado. Es por ello que debe contar con una exactitud en la detección de los programas malignos.

ANTIVIRUS

Clasificación de Antivirus:

- **CORTAFUEGOS O FIREWALL**: estos programas tienen la función de bloquear el acceso a un determinado sistema, actuando como muro defensivo. Tienen bajo su control el tráfico de entrada y salida de una computadora, impidiendo la ejecución de toda actividad dudosa.
- **ANTIESPÍAS O ANTISPYWARE**: esta clase de antivirus tiene el objetivo de descubrir y descartar aquellos programas espías que se ubican en la computadora de manera oculta
- **ANTIPOP-UPS**: tiene como finalidad impedir que se ejecuten las ventanas pop-ups o emergentes, es decir a aquellas ventanas que surgen repentinamente sin que el usuario lo haya decidido, mientras navega por Internet.
- **ANTISPAM**: se denomina spam a los mensajes basura, no deseados o que son enviados desde una dirección desconocida por el usuario. Los antispam tienen el objetivo de detectar esta clase de mensajes y eliminarlos de forma automática.

ANTIVIRUS

Tipos de Antivirus:

- ✓ **Panda**
- ✓ **Mcfee**
- ✓ **Norton**
- ✓ **TrendMicro**
- ✓ **Secuware**
- ✓ **Norman**
- ✓ **Authentium**
- ✓ **Kaspersky**
- ✓ **Antivir**
- ✓ **Sophos**
- ✓ **PerAntivirus**
- ✓ **Nod-32**
- ✓ **Avg**
- ✓ **BitDefender**
- ✓ **Etrust**
- ✓ **Avast**
- ✓ **Rav**
- ✓ **Zone Alarm**
- ✓ **F-secure**
- ✓ **Clam**
- ✓ **Hacksoft**
- ✓ **Esafe**
- ✓ **Portland**
- ✓ **Avira**
- ✓ **G-data**
- ✓ **Avast**
- ✓ **Eset**

¿Preguntas?