Los virus informáticos: Clasificación, funcionamiento y sus principales creadores

INTRODUCCION

Actualmente los virus informáticos se han incrementado notablemente; desde la primera aparición su crecimiento ha sido sorprendente. En la actualidad se crean cinco virus diarios aproximadamente, los virus no solamente copian sus códigos en forma parcial a otros programas sino que además lo hacen en áreas importantes de un sistema (sector de arranque, tabla de partición, entre otros).

Con Internet se hace más fácil tener el total control de los virus informáticos, lo que resulta perjudicial a todos los usuarios. El crecimiento veloz de los virus, hace necesario un rápido tratamiento usando las técnicas de prevención, detección y eliminación de virus informáticos, teniéndose que llevar a cabo de forma rápida y eficiente.

Como causa de éste crecimiento innumerable de los virus informáticos, aparece, paradójicamente la solución, mediante las actualizaciones de los antivirus.

Este trabajo tiene como objetivo brindar información relevante al lector sobre todo lo primordial que debe saber para prevenir la contaminación de un antivirus, y además ser engañado por algunos de los delincuentes informáticos junto a sus técnicas. Se estará describiendo la función y el concepto de antivirus y algunas diferencias entre los que se encuentran en el mercado.

Esperando que la lectura sea enriquecedora para el lector.

1. **VIRUS INFORMÁTICOS**

Historia

Su origen se remonta a 1959, en los laboratorios de la BELL Computer, subsidiaria de la AT&T, en New Jersey, donde 3 jóvenes programadores, inspirados en la "teoría de autómatas complejos" del científico John Von Neuman expuesta en 1949, desarrollaron un programa al que llamaron CoreWar, el cual consistía en que cada contendor ejecutaba una órden cada vez y el primero que consumía la memoria del computador se convertía en el ganador.

Las rutinas del juego CoreWar, desarrolladas en assemblerpnemónico son consideradas como los programas precursores de los virus contemporáneos. Por motivos de investigación se puede descargar (download) una copia del juego COREWAR, adaptado a PC, haciendo click en: CoreWar.

Muchos años han pasado y la historia nos hace saber de la existencia de esporádicos virus en las antiguas y enormes computadoras y que no es nuestro propósito relatar. Sucedió con la

aparición de las IBM PC en 1981 que el auge de la computación conllevó también a la fiebre de la programación en diversos lenguajes.

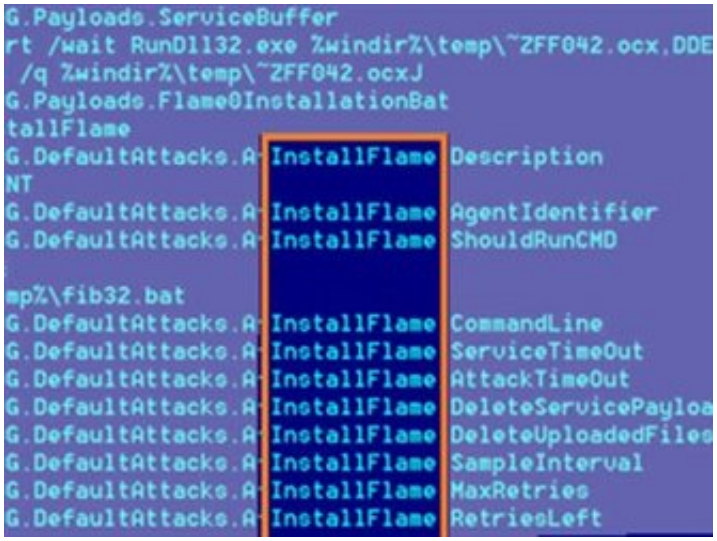
El término virus no se adoptaría hasta 1984, pero éstos ya existían desde antes. Sus inicios fueron en los laboratorios de *Bell Computers*. Cuatro programadores (H. Douglas Mellory, Robert Morris, VictorVysottsky y Ken Thompson) desarrollaron un juego llamado CoreWar, el cual consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.

Después de 1984, los virus han tenido una gran expansión, desde los que atacan los sectores de arranque de disquetes hasta los que se adjuntan en un correo electrónico.

Los primeros virus de PC fueron desarrollados en lenguaje Assembler. Sin embargo hubieron algunas especies virales desarrolladas en lenguajes de alto nivel tales Turbo Pascal, Lenguaje C, etc. A partir de 1995 se crearon los virus de 32 bits en Assembler, Visual C++, Borland Delphi, etc., predominando los desarrollados en Assembler, con el objeto de tener menor extensión y así poder pasar desapercibidos. También en 1995 surgieron los macro virus, desarrollados en los lenguajes macro de MS-Word o MS-Excel.

En 1998 empezaron a aparecer los virus y gusanos desarrollados en Java Scripts, Visual Basic Scripts, Controles Active X y HTML. La mayoría de estos se distribuyen via correo electrónico en archivos anexados, a través de Internet.

Definición



Un virus es un pequeño programa con instrucciones creadas exprofesamente para provocar daños o alteraciones en los archivos o áreas vitales de un sistema: sector de arranque, MBR o Master Boot Record, Tabla de Particiones. Se le denominan virus ya que al igual que las especies biológicas son pequeños, se autoreproducen e infectan a un ente receptor desde un ente transmisor (archivos o áreas vitales del sistema).

Se les conoce con el nombre de virus de computadoras, virus informáticos, cibernéticos o

electrónicos y para efectos de esta página informativa simplemente los denominaremos Virus.

Un virus informático es un programa de computadora, tal y como podría ser un procesador de textos, una hoja de cálculo o un juego. Obviamente ahí termina todo su parecido con estos típicos programas que casi todo el mundo tiene instalados en sus computadoras. Un virus informático ocupa una cantidad mínima de espacio en disco (el tamaño es vital para poder pasar desapercibido), se ejecuta sin conocimiento del usuario y se dedica a autorreplicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible.

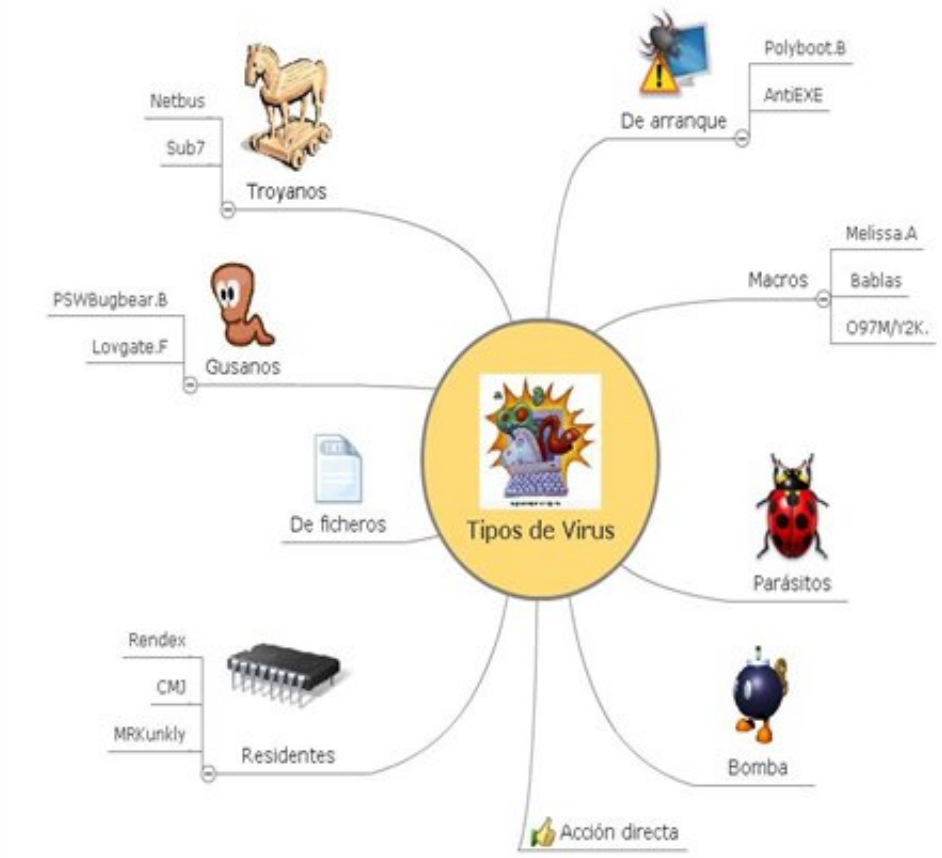
Clasificación

La clasificación de los virus informáticos, basada en el daño que causan y efectos que provocan.

- **Caballo de Troya:** Es un programa dañino que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este ultimo. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.
- **Gusano o Worm:** Es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, se copia así mismo sucesivamente, hasta que desborda la RAM, siendo ésta su única acción maligna.
- **Virus de macros:** Un macro es una secuencia de ordenes de teclado y mouse asignadas a una sola tecla, símbolo o comando. Son muy útiles cuando este grupo de instrucciones se necesitan repetidamente. Los virus de macros afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y actuaran hasta que el archivo se abra o utilice.
- **Virus de sobreescritura:** Sobrescriben en el interior de los archivos atacados, haciendo que se pierda el contenido de los mismos.
- **Virus de Programa:** Comúnmente infectan archivos con extensiones .EXE, .COM, .OVL, .DRV, .BIN, .DLL, y .SYS., los dos primeros son atacados más frecuentemente por que se utilizan mas.
- **Virus de Boot:** Son virus que infectan sectores de inicio y booteo (Boot Record) de los diskettes y el sector de arranque maestro (Master Boot Record) de los discos duros; también pueden infectar las tablas de particiones de los discos.
- **Virus Residentes:** Se colocan automáticamente en la memoria de la computadora y desde ella esperan la ejecución de algún programa o la utilización de algún archivo.
- **Virus de enlace o directorio:** Modifican las direcciones que permiten, a nivel interno, acceder a cada uno de los archivos existentes, y como consecuencia no es posible localizarlos y trabajar con ellos.
- **Virus mutantes o polimórficos:** Son virus que mutan, es decir cambian ciertas partes de su código fuente haciendo uso de procesos de encriptación y de la misma tecnología que utilizan los antivirus. Debido a estas mutaciones, cada generación de virus es diferente a la versión anterior, dificultando así su detección y eliminación.
- **Virus falso o Hoax:** Los denominados virus falsos en realidad no son virus, sino cadenas de mensajes distribuidas a través del correo electrónico y las redes. Estos

mensajes normalmente informan acerca de peligros de infección de virus, los cuales mayormente son falsos y cuyo único objetivo es sobrecargar el flujo de información a través de las redes y el correo electrónico de todo el mundo.

- **Virus Múltiples:** Son virus que infectan archivos ejecutables y sectores de booteo simultáneamente, combinando en ellos la acción de los virus de programa y de los virus de sector de arranque.



2. **CAUSA Y EFECTO**

Ciclo de vida

El ciclo de vida de un virus empieza cuando es creado y termina cuando es completamente erradicado. El siguiente esquema describe cada etapa:

- **Creación.** Hasta hace poco tiempo, crear un virus requería el conocimiento de un lenguaje de programación. Hoy en día cualquier persona con un conocimiento básico de programación puede crear un virus.
- **Replicación.** Los virus típicamente se replican por un largo periodo de tiempo antes de que estos se activen, permitiendo un basto tiempo para su esparcimiento.
- **Activación.** Los virus con rutinas de daño se activarán cuando ciertas condiciones son cubiertas, por ejemplo, en cierta fecha o cuando los usuarios infectados realizan una

acción en particular.

- **Descubrimiento.** Cuando un virus es detectado y aislado, este es enviado a el ICSA en Washington, D.C., para ser documentado y distribuido a los desarrolladores de software antivirus.
- **Asimilación.** En este punto, los desarrolladores de software antivirus modifican su software para que este pueda detectar el nuevo virus.
- **Erradicación.** Si suficientes usuarios instalan software de actualización para la protección antivirus, cualquier virus puede ser limpiado.No todos los virus han desaparecido completamente, pero muchos han dejado de ser una amenaza mayor.

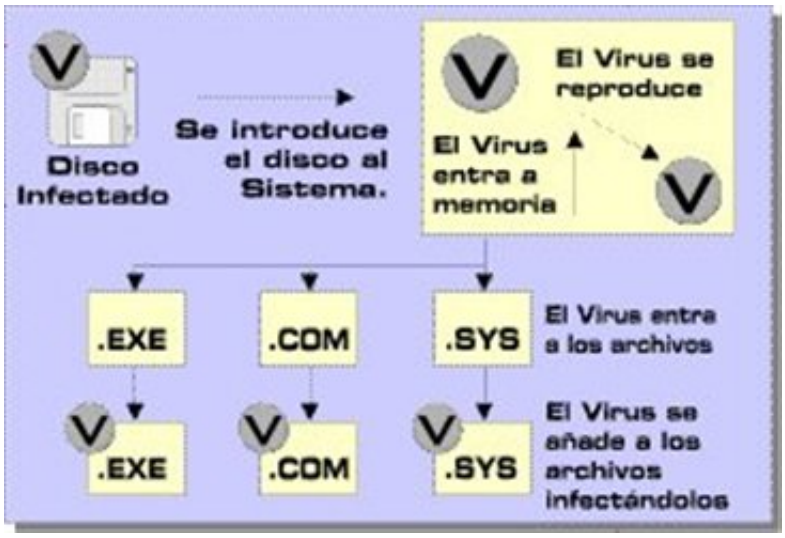
¿Como se produce la infección?

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. Estos se propagan cuando las instrucciones que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos o a través de redes informáticas.

El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un ordenador está simplemente conectado a una red infectada o se limita a cargar un programa infectado, no se infectará probablemente. Un usuario no ejecuta conscientemente un código informático potencialmente nocivo como si nada; sin embargo, los virus engañan frecuentemente para ser ejecutado.

Estas infecciones son mucho más frecuentes en PC que en sistemas profesionales de grandes computadoras, porque los programas de los PC se intercambian fundamentalmente a través de discos flexibles o de redes informáticas no reguladas.

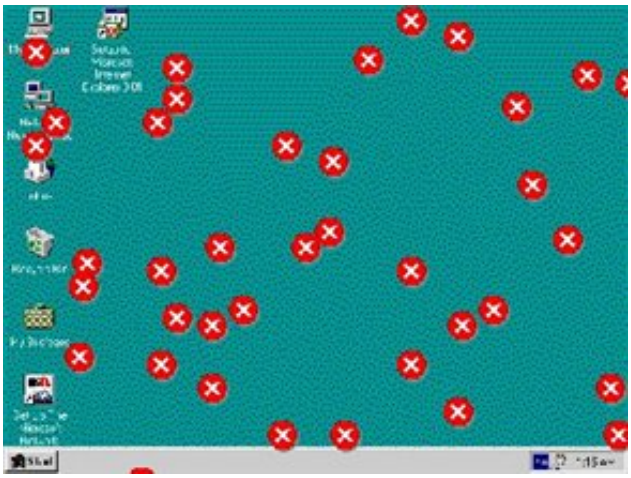


Daños que ocasionan

Se pueden clasificar en dos tipos:

Los daños al sistema a nivel de software

- Modificación de programas para que no funcionen
- Modificación de programas para que funcionen incorrectamente
- Eliminación de programas, datos, archivos, entre otros
- Consumir espacio del disco duro progresivamente
- Hacer que el sistema funcione con más lentitud
- Robo de información personal y confidencial
- Imposibilita el acceso a funciones del sistema Hace que el sistema no arranque correctamente



Los daños al computador a nivel de hardware

- Borrado de la información contenida en el BIOS
- Quemado del procesador por información errónea del sensor de temperatura, la cual obviamente ha sido establecida intencionalmente por el mismo virus
- Estropeo del disco duro por hacer que lea datos repetidamente en el mismo sector

Prevención

Para prevenir la infección de virus informáticos se deben tener en cuenta los siguientes detalles:

- **Copias de seguridad:** Realice copias de seguridad de sus datos. Éstas pueden realizarlas en el soporte que desee, disquetes, unidades de cinta, etc. Mantenga esas copias en un lugar diferente del ordenador y protegido de campos magnéticos, calor, polvo y personas no autorizadas.
- **Copias de programas originales:** No instale los programas desde los disquetes originales. Haga copia de los discos y utilícelos para realizar las instalaciones.
- **No acepte copias de origen dudoso:** Evite utilizar copias de origen dudoso, la mayoría de las infecciones provocadas por virus se deben a discos de origen desconocido.
- **Utilice contraseñas:** Ponga una clave de acceso a su computadora para que sólo usted pueda acceder a ella.
- **Anti-virus:** Tenga siempre instalado un anti-virus en su computadora, como medida general analice todos los discos que desee instalar. Si detecta algún virus elimine la instalación lo antes posible.
- **Actualice periódicamente su anti-virus:** Un anti-virus que no está actualizado puede ser completamente inútil. Todos los anti-virus existentes en el mercado permanecen residentes en la computadora pata controlar todas las operaciones de ejecución y transferencia de ficheros analizando cada fichero para determinar si tiene virus, mientras el usuario realiza otras tareas.

3. **TÉCNICAS Y ESTRATEGIAS DE PROGRAMACIÓN DE VIRUS / TIPOS DE VIRUS**

Infector rápido / lento

Se le denomina infector rápido a un virus cuando está activo en la memoria infecta no solamente a los programas cuando son ejecutados sino a aquellos que son simplemente

abiertos para ser leídos. Como resultado de esto sucede que al ejecutar un explorador o un verificador de la integridad.

Esta técnica usa la función 3dh de la interrupción 21h para abrir un archivo ejecutable en forma muy rápida, empezando preferentemente con el COMMAND.COM y ubicándose en clustersvacios detrás de un comando interno, por ejemplo DIR, de tal modo que no solamente no incrementa el tamaño del archivo infectado sino que además su presencia es inadvertible. Puede darse el caso además, de que cuando se ejecuta un archivo EXE o COM éste no es infectado, en cambio sus archivos relacionados tales como OVL o DBF's son alterados. Si bajo esta técnica se ha decidido atacar a las áreas del sistema el código viral reemplaza a los 512 bytes del sector de arranque y envia el sector original a otra posición en el disco, pero a su vez emulará al verdadero, y al ser un "clon" de boot le será muy fácil infectar a la FAT y al Master Boot Record o a la Tabla de Particiones, imposibilitando el acceso al disco.

En cambio existe el infector lento que se refiere a un virus que solamente infecta a los archivos en la medida que éstos son ejecutados, modificados o creados, pero con una salvedad: puede emplear también parte de la técnica del infector rápido pero sin la instrucción de alteración o daño inmediato al abrirse un archivo.

Con la interrupción 1Ch del TIMER su autor programa una fecha, la misma que puede ser específica o aleatoria para manifestarse. Mientras tanto el virus permanece inactivo y encriptado en el archivo o área afectada esperando su tiempo de activación. Los virus del tipo "infector lento" suelen emplear rutinas de anti-detección sumamente eficientes, algunas de las cuales inhabilitan a las vacunas de los antivirus mas conocidos.

Estrategia Parse

Esta técnica consiste en instruir al virus para que infecte ocasionalmente, por ejemplo, cada 10 veces que se ejecute un programa. Otras veces, infecta únicamente a los archivos de menor extensión y al infectarlos en forma ocasional se minimiza la posibilidad de descubrirlo fácilmente. Por otro lado, el contador de ejecuciones de los archivos infectados con virus que emplea esta modalidad, tiene por lo general más de una rutina de auto encriptamiento. La técnica "parse" no es tan comunmente usada, pero sus efectos y estragos son muy lamentables.

Función desactivadora

Un virus que emplea la técnica del túnel intercepta los manipuladores de la interrupciones del DOS y el BIOS y las invoca directamente, evadiendo de este modo cualquier actividad de monitoreo de las vacunas antivirus. Aunque no existen, por ahora, gran cantidad de estas especies virales, existe la tendencia a incrementarse, habiéndose descubierto virus que usan originales artimañas para infectar a un sistema sin ser descubiertos. Todos estos tienen rutinas que en forma muy rápida se superponen a los IRQ's ocupados por las vacunas logrando desactivarlas para acceder directamente a los servicios del DOS y del BIOS tomando absoluto control del sistema y sin restricción alguna.

Las especies virales tipo "tunneling" emplean estas rutinas para saltear y sobrepasar a algunas de las vacunas residentes en memoria. Del mismo modo, algunos antivirus suelen utilizar esta técnica en su necesidad de "by-pasear" un virus nuevo y desconocido que podría estar activo cuando se está explorando un sistema.

Virus polimórficos (mutantes)

Es una técnica que consiste en variar el código virico en cada infección (más o menos lo que hace el virus del SIDA en los humanos con su capa protéica). Esto obliga a los antivirus a usar técnicas heurísticas ya que como el virus cambia en cada infección es imposible localizarlo buscandolo por cadenas de código. Esto se consigue utilizando un algoritmo de encriptación que pone las cosas muy difíciles a los antivirus. No obstante no se puede codificar todo el código del virus, siempre debe quedar una parte sin mutar que toma el control y esa es la parte más vulnerable al antivirus. La forma más utilizada para la codificación es la operación lógica XOR. Esto es debido que esta operación es reversible:

7 XOR 9 = 2

2 XOR 9 = 7

En este caso la clave es el número 9, pero utilizando una clave distinta en cada infección se obiene una codificación también distinta. Otra forma también muy utilizada consiste en sumar un numero fijo a cada byte del código vírico.

Virus en java

La tecnología empleada en este virus tiene varias ventajas. La forma multi-componente de infección permite al virus esconder su código en los archivos infectados: su longitud crece en muy pequeños valores y después de una ligera observación el código insertado pareciera no ser dañino. La combinación del llamado starter-main también le permite a su autor, "actualizar" el virus con nuevas versiones al reemplazar el código principal en su servidor. Cabe mencionar que este virus o cualquier virus de Java se puede propagar y reproducir en condiciones limitadas. La protección estándar de seguridad de los navegadores cancela cualquier intento de acceder a las unidades de disco o recoger (download) archivos como una aplicación Java, aún en modo remoto. Consecuentemente el virus puede ser propagado únicamente cuando es ejecutado en un archivo de disco, como una aplicación Java, al usar el Java machine.

Virus anexado

El virus anexado (attached) no es una técnica de programación de virus, es una nueva modalidad de difundirlo. Con el incremento del intercambio de información por correo electrónico, a causa de la gran demanda de uso de los servicios de Internet, los desarrolladores de virus han hallado una nueva forma de difundir sus creaciones. Ella consiste en enviar un mesaje de correo con un archivo anexado o adjunto, el cual al ser abierto ejecuta el virus con consecuencias de daño inmediato a los sistemas de los usuarios, que por motivos de curiosidad cometan el error de abrir estos archivos.

Los virus suelen venir en documentos (.DOC), archivos comprimidos en formato ZIP, ejecutables EXE, en controles Activex de archivos HTML, Visual Basic Scripts o archivos con extensión .SHS y si además contienen instrucciones de auto-enviarse a la Libreta de Direcciones del software de correo del usuario, su propagación tendrá un efecto multiplicador.

Macro virus

Los macro-virus representan una de las amenazas más importantes para una red. Actualmente son los virus que más se están extendiendo a través de Internet. Representan una amenaza tanto para las redes informáticas como para los ordenadores independientes. Su máximo peligro está en que son completamente independientes del sistema operativo o de la plataforma. Es más, ni siquiera son programas ejecutables. Los macro-virus son pequeños programas escritos en el lenguaje propio propio de un programa. Así nos podemos encontrar con macro-virus para editores de texto, hojas de cálculo y utilidades especializadas en la manipulación de imágenes.

4. **DELINCUENTES INFORMÁTICOS**

Piratas

Pirata informático es quien adopta por negocio la reproducción, apropiación o acaparación y distribución, con fines lucrativos, y a gran escala, de distintos medios y contenidos de los que no posee licencia o permiso de su autor, generalmente haciendo uso de un ordenador. Siendo la de software la práctica de piratería más conocida.

Hacker

El término hacker trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.Hacker, usando la palabra inglesa, quiere decir divertirse con el ingenio, usar la inteligencia para hacer algo difícil. No implica trabajar solo ni con otros necesariamente. Hacker es toda aquella persona con elevados conocimientos informáticos independientemente de la finalidad con que los use.

Hacker Famoso Kevin Mitnick

Cracker

Los crackers (crack=destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc. Esos son los crackers. Adolescentes inquietos que aprenden rápidamente este complejo oficio.

Fred Cohen: Cracker Famoso

Phreaker

El phreaker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

Famoso Phreaker: Tsutomu Shimomura

5. **VIRUS FAMOSOS**

A continuación se presentará una lista de los virus informáticos más famosos en la historia:

1. **Creeper.** Se trata del primer virus de la historia. Nació en 1971 y dejó huella porque infectó los computadores PDP-11 conectadas a Arpanet. Una de las características de Creeper es que mostraba un mensaje que infectaba el sistema y decía: "*Soy el más aterrador (creeper); atrápame si puedes*". Fue creado por Robert Thomas Morris.
2. **Friday 13 o Jerusalem:** Fue creado en el 1988 y borraba todos los archivos del ordenador infectado.
3. **Barrotes:** El primer virus español conocido. Cuando lograba ingresar al ordenador se mantenía inactivo hasta el 5 de enero y ese día mostraba una serie de barras en la pantalla.
4. **CascadeorFallingLetters:** Fue desarrollado en Alemania en el 1980 y hacía que todas las letras de la pantalla cayeran como si estuvieran en una cascada.
5. **CIH o Chernobyl:** Nació en Taiwán en el 1998 y le tomó solamente una semana para reproducirse a través de miles de ordenadores.
6. **Melissa:** Uno de los primeros virus que utilizó el famoso mensaje Aquí tienes el documento que me pediste no se lo muestres a nadie más para propagarse.
7. **ILoveYou o Loveletter:** Desarrollado en Filipinas en el año 2000 y con el *subject*ILoveYou infectó millones de ordenadores de todo el mundo, incluso llegó al Pentagono. Según las compañías de antivirus ha sido el más peligroso de todos los tiempos
8. **Klez:** Infectaba sólo a computadoras los días número 13 de meses impares y nació en Alemania en el año 2001.
9. **Nimda:** Su nombre es *admin* si se lo lee de atrás hacia adelante y podía generar permisos de administrador en los ordenadores infectados. Se lo vio por primera vez el 18 de septiembre del 2001 en China.
10. **SQLSlammer:** Infectó a más de medio millón de ordenadores desde el 25 de enero del 2003.

11. **Blaster:** Uno de los virus más conocidos de la historia que explotaba una vulnerabilidad de Windows. Fue creado en agosto del 2003.

1. **Sobig:** Generó en el verano del 2003 más de 1 millón de infectados y la variante F del mismo era la más dañina.
2. **Bagle:** Fue uno de los virus con más variantes de la historia y apareció el 18 de enero del 2004.
3. **Netsky:** Otro de los más peligrosos de la historia. Fue desarrollado en Alemania y usaba una vulnerabilidad del Internet Explorer.
4. **Conficker:** Uno de los más recientes. Nació en noviembre del 2008 y lo raro era que si tenías el teclado configurado en ucraniano no afectaba al infectado.

6. **ANTIVIRUS**

Definición

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.

Función / operación

Normalmente, los antivirus monitorizan actividades de virus en tiempo realy 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.

Diferencias entre antivirus

Existen muchos antivirus en el mercado algunos de ellos son junto a sus características:

- **McAfee:** El sistema de seguridad McAfee ofece diferentes herramientas como por ejemplo el personal firewall plus, virus scan, privacyservice y secutiry center. Cada una de ellas es para diferentes necesidades de negocio o personales.
- **Sophos:** Con este software el equipo puede tener escaneados programados o en tiempo real, eliminando las posibilidades de que los virus se extiendan o dañen los datos almacenados. Usuarios remotos y de portátiles ya no tienen por qué ser considerarse un punto débil y con RemoteUpdate se actualiza automaticamente sin necesidad de preocuparse por ello.
- **Panda Software:** Ofrece herramientas para plataformas comwindows y linux. Con herramientas que evitan la propagación de códigos maliciosos que utilizan la vulnerabilidad, parándolos directamente en la puerta de entrada del correo electrónico a la empresa y reduciendo, de esta manera, las alertas que los usuarios reciben o la saturación de los buzones de los servidores. Tiene una version especial para universitarios un área en la que podrán utilizarse las nuevas y exclusivas herramientas gratuitas desarrolladas por Panda Software para la lucha contra los virus informáticos.
- **Symantec:** Es una de las empresas lideres en cuanto a software antivirus se refiere, scanea el correo electronico y el trafico de la web. Ofrece soluciones de seguridad globales ya sea empresariales y para usuario domestico.
- **BitDefender:** La gama BitDefender proporciona protección antivirus para los puntos esenciales de acceso a una red, protegiendo las puertas de enlace, los servidores de

Internet, de correo y de archivos y también incluye soluciones antivirus para los usuarios individuales.

- **NOD32 de eset:** NOD32 Anti-Virus System logra un adecuado balance entre el desarrollo actual de los sistemas anivirus y la protección efectiva contra los peligros potenciales que amenazan tu computadora, ejecutándose sobre distintos sistemas operativos como Microsoft Windows 95 / 98 / Me / NT / 2000 / XP, así como en una importante variedad de servidores de correo basados en ambientes UNIX.

Norton Vs McAfee

Entre las principales diferencias entre estos antivirus están:

- **Norton Antivirus 2004** Norton AntiVirus es la última herramienta de Symantec para protegerse de todo tipo de virus, applets Java, controles ActiveX y códigos maliciosos. Como la mayoría de los antivirus, el programa de Symantec protege la computadora mientras navega por Internet, obtiene información de disquetes, CD`s o de una red y comprueba los archivos adjuntos que se reciben por email.

- **McAfee VirusScan 7** McAfee VirusScan es una de las herramientas de seguridad más conocida por los usuarios de todo el mundo. Esta nueva versión protege a la PC de posibles infecciones a través del correo electrónico, de archivos descargados desde Internet y de ataques a partir de applets de java y controles ActiveX.Trae una nuevo motor de búsqueda y un potente filtro para Internet que permite bloquear el acceso a sitios Web no deseados. Incluye una función llamada "Safe&Sound" que automáticamente realiza copias de seguridad de los documentos mientras están abiertos.

Cada usuario posee su opinión y según la necesidad se puede determinar cuales características prefieren de un antivirus sobre otro en el momento de su escogencia.

CONCLUSION

Un virus es un programa pensado para poder reproducirse y replicarse por sí mismo, introduciéndose en otros programas ejecutables o en zonas reservadas del disco o la memoria. Sus efectos pueden no ser nocivos, pero en muchos casos hacen un daño importante en el ordenador donde actúan. Pueden permanecer inactivos sin causar daños tales como el formateo de los discos, la destrucción de ficheros, etc.

Es necesario tomar medidas preventivas para luchar con los virus informáticos que son una realidad diaria, molesta y en su mayoría nociva y para ello es necesario identificar que es un virus, como se propaga, medidas preventivas y en el último caso como se eliminan. Los virus son programas nocivos que contienen cargas que generan daños y bloqueos en el sistema y redes y que en la mayoría de casos los usuarios por desconocimiento alojan o trasladan. Pero para luchar contra estos existen antivirus que son programas o aplicaciones con la finalidad de detectarlos, bloquearlos, no permitir el acceso de ellos y eliminarlos.

Es importante en todos los ámbitos, especialmente en el empresarial tener planes de contingencia y más en el sistema informático que por su gran auge tiene puertas abiertas implementando y actualizando los programas de antivirus también conocidas como vacunas, y donde los avances nos ofrecen una gran gama de estas como vacunas de solo detección que actualizan archivos infectados pero no pueden eliminar el virus, vacunas de Detección y desinfección: son vacunas que detectan archivos infectados y que pueden desinfectarlos entre otros tantos. El mercado nos ofrece varios anti virus; cortafuegos, antiespias, antipop-ups antispam etc. y están al alcance de cualquier usuario.

GLOSARIO

1. **Encriptación:** es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

2. **Virus Falsos:** Son mensajes de correo que por lo general nos advierten de algún virus que no existe. Casi siempre nos indica que debemos buscar un archivo y si se encuentra en nuestra pc debemos borrarlo ya que es un virus, lo que en realidad estaremos haciendo es eliminar un archivo fundamental para el correcto funcionamiento de nuestro sistema operativo.

3. **Joke Programs:** Un programa que cambios o interrumpe el comportamiento normal de un ordenador, por ejemplo, haciendo clic con el ratón en sentido inverso.Programas de broma son los programas que cambiar o interrumpir el comportamiento normal del ordenador para crear una distracción general o molestia.

4. **Dialer:** tipo de software que crea una conexión a una red sin informar completamente al usuario sobre el costo que realmente tiene conectar a esa red.

5. **Adware:** es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad web al computador después de instalar el programa o mientras se está

utilizando la aplicación. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en inglés.

6. **Spam:** es correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

7. **Cookie:** son una pequeña pieza de información enviada por un sitio web, las cuales son almacenadas en el navegador del usuario del sitio, de esta manera el sitio web puede consultar dicha información para notificar al sitio de la actividad previa del usuario.

8. **Spyware:** es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

9. **Combinación:** es una secuencia ordenada de signos (que pueden ser letras y/o números) sólo conocida por uno o pocos individuos y que permite abrir o poner en funcionamiento a determinados mecanismos.

10. **Macro:** es una serie de instrucciones que se almacenan para que se puedan ejecutar de manera secuencial mediante una sola llamada u orden de ejecución. Dicho de otra manera, una macroinstrucción es una instrucción compleja, formada por otras instrucciones más sencillas. Esto permite la automatización de tareas repetitivas.

11. **Caballo de Troya:** es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.Para que un programa sea un "troyano" sólo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua (derivado del latín significa "no hace daño").

12. **Gusano:** es un código maligno (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.

RECOMENDACIONES

- Realizar charlas informativas en donde los estudiantes puedan conocer la importancia de tener un antivirus actualizado y con licencia.

- Informar al público en general sobre el daño que causa los virus informáticos.

- Realizar simulacros para orientar a las personas sobre las consecuencias que pueden causar algunos virus informáticos no solo al software, hardware, sino información sensitiva en el computador.

- Explicar porque razón no todos los programas antivirus pueden detectar al 100% todos los virus.

- Comentar sobre la forma como los virus informáticos pueden infectar celulares móviles y otros dispositivos que se conecten al computador.

BIBLIOGRAFIA

_____. Historia de los virus informáticos. http://pozarica.ar.tripod.com/Virus.html

_____. Ciclo de Vida de un virus. http://www.elimparcial.com/edicionimpresa/Hoy/Informatica/528513.as

_____. ¿Qué es un cracker? http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php

_____. Piratas informáticos. http://html.rincondelvago.com/piratas-informaticos_1.html

BAEZ, H. 2011. Los daños que causan los virus informáticos. http://anti-haker.blogspot.com/2009/09/los-danos-que-causan-los-virus_11.html

GATES, W. (1976) ¿Hackers un problema para la sociedad? (1era edición). Estados Unidos: Osborne

GONCALVES, G. Virus informáticos. http://www.monografias.com/trabajos12/virudos/virudos.shtml

LOPEZ, C. Antivirus. http://www.monografias.com/trabajos27/secuware-antivirus/secuware-antivirus.shtml

MERLAT, M.; PAZ, G.; SOSA, M.; MARTINEZ, M. (1999) Seguridad Informática (hackers). España

PEÑEN, A. Virus informáticos. http://html.rincondelvago.com/virus-informaticos_3.html