AMENAZAS…
¿Y COMO DISMINUIR EL RIESGO?

Juan Fdo. Hurtado R.

juan.hurtado@comfenalcoantioquia.com
fhenet@yahoo.es

Comfenalco ANTIOQUIA

OBJETIVOS

- Conocer los diferentes elementos que pueden ser utilizados para afectar un sistema de información.
- Dar algunos consejos y recomendaciones para la ejecución de buenas practicas que ayuden a disminuir los posibles riesgos presentados en el computador personal y de oficina.

AGENDA

Amenazas

- Virus
- Gusanos
- Troyanos
- Bombas lógicas
- Hoax
- Keyloggers
- RootKits
- Spyware
- Spam
- Phishing

¿Cómo disminuir el riesgo?

Virus

Definición

Motivo

Ciclo de vida

Clasificación

Origen

Virus: Definición

Programa de computadora que 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. Mientras el virus se replica intenta pasar lo más **desapercibido** que puede, intenta evitar que el "**huésped**" se dé cuenta de su presencia... hasta que llega el momento de la "**explosión**". Es el momento culminante que marca el final de la infección y cuando llega suele venir acompañado del formateo del disco duro, borrado de archivos o mensajes de protesta. No obstante el daño se ha estado ejerciendo durante todo el proceso de infección, ya que el virus ha estado ocupando memoria en el computadora, ha ralentizado los procesos y ha "engordado" los archivos que ha infectado.

Virus: Ciclo de vida

- Programación y desarrollo
- Expansión
- Actuación
- Extinción o mutación (en este último caso el ciclo se repite)

Virus: Motivo

- La gran mayoría de los creadores de virus lo ven como un **hobby**, aunque también otros usan los virus como un medio de **propaganda** o difusión de sus quejas o ideas radicales, como por ejemplo el virus Telefónica, que emitía un mensaje de protesta contra las tarifas de esta compañía a la vez que reclamaba un mejor servicio, o el famosísimo Silvia que sacaba por pantalla la dirección de una chica que al parecer no tuvo una buena relación con el programador del virus.
- En otras ocasiones es el **orgullo**, o la **competitividad** entre los programadores de virus lo que les lleva a desarrollar virus cada vez más destructivos y difíciles de controlar.

Virus: Clasificación

- Los virus se pueden clasificar en función de múltiples características y criterios: según su **origen**, las **técnicas** que utilizan para infectar, los **tipos de archivos** que infectan, los **lugares** donde se esconden, los **daños** que causan, el **sistema operativo** o la plataforma tecnológica que atacan, etc.
- Todas estas clasificaciones tienen muchos puntos en común, por lo que un mismo virus puede pertenecer a varias categorías al mismo tiempo.
- Por otro lado, continuamente surgen nuevos virus que por su reciente aparición o por sus peculiares características no pueden ser incluidos inicialmente en ninguna categoría, aunque esto no es lo habitual.

Virus: Clasificación

Residentes

Acción directa

Sobreescritura

Boot o de arranque

Macro

Enlace o directorio

Encriptados

Polimórficos

Multipartites

archivo

Compañía

FAT

Virus residentes

- La característica principal de estos virus es que **se ocultan en la memoria RAM** de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos archivos y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, etc.
- Estos virus sólo atacan cuando se cumplen ciertas condiciones definidas previamente por su creador (por ejemplo, una fecha y hora determinada). Mientras tanto, permanecen ocultos en una zona de la memoria principal, ocupando un espacio de la misma, hasta que son detectados y eliminados.
- Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

Virus de acción directa

- Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y **actuar en el mismo momento de ser ejecutados**. Al cumplirse una determinada condición, se activan y buscan los archivos ubicados dentro de su mismo directorio para contagiarlos.
- Además, también realizan sus acciones en los directorios especificados dentro de la línea PATH (camino o ruta de directorios), dentro del archivo AUTOEXEC.BAT (archivo que siempre se encuentra en el directorio raíz del disco duro).
- Los virus de acción directa presentan la ventaja de que los archivos afectados por ellos pueden ser desinfectados y restaurados completamente.

Virus de sobreescritura

- Estos virus se caracterizan por destruir la información contenida en los archivos que infectan. Cuando infectan un archivo, **escriben dentro de su contenido**, haciendo que queden total o parcialmente inservibles.
- También se diferencian porque los archivos infectados no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio archivo (esto se debe a que se colocan encima del archivo infectado, en vez de ocultarse dentro del mismo).
- La única forma de limpiar un archivo infectado por un virus de sobreescritura es borrarlo, perdiéndose su contenido.
- Algunos ejemplos de este tipo de virus son: Way, Trj.Reboot, Trivial.88.D.

Virus de boot o de arranque

- Los términos **boot o sector de arranque** hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el computador.
- Este tipo de virus no infecta archivos, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los disquetes. Cuando un computador se pone en marcha con un disquete infectado, el virus de boot infectará a su vez el disco duro.
- Los virus de boot no pueden afectar al computador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los disquetes contra escritura y no arrancar nunca el computador con un disquete desconocido en la disquetera.
- Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

Virus de macro

- El objetivo de estos virus es la infección de los archivos creados usando determinadas aplicaciones que contengan **macros**: documentos de Word (archivos con extensión DOC), hojas de cálculo de Excel (archivos con extensión XLS), bases de datos de Access (archivos con extensión MDB), presentaciones de PowerPoint (archivos con extensión PPS), archivos de Corel Draw, etc.
- Las macros son micro-programas asociados a un archivo, que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas.
- Cuando se abre un archivo que contenga un virus de este tipo, las macros se cargarán de forma automática, produciéndose la infección. La mayoría de las aplicaciones que utilizan macros cuentan con una protección antivirus y de seguridad específica, pero muchos virus de macro sortean fácilmente dicha protección.
- Existe un tipo diferente de virus de macro según la herramienta usada: de Word, de Excel, de Access, de PowerPoint, multiprograma o de archivos RTF. Sin embargo, no todos los programas o herramientas con macros pueden ser afectadas por estos virus.
- Estos son algunos ejemplos: Relax, Melissa.A, Bablas, O97M/Y2K.

Virus de enlace o directorio

- Los archivos se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.
- Los virus de enlace o directorio **alteran las direcciones que indican donde se almacenan los archivos**. De este modo, al intentar ejecutar un programa (archivo con extensión EXE o COM) infectado por un virus de enlace, lo que se hace en realidad es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar.
- Una vez producida la infección, resulta imposible localizar y trabajar con los archivos originales.

Virus encriptados

- Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones.
- Estos virus se **cifran o encriptan** a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.
- Estos son algunos ejemplos de este tipo de virus: Elvira, Trile.

Virus polimórficos

- Son virus que en cada infección que realizan se **cifran o encriptan de una forma distinta** (utilizando diferentes algoritmos y claves de cifrado).
- De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.
- Algunos ejemplos de este tipo de virus son: Elkern, Marburg, Satan Bug, Tuareg.

Virus multipartites

- Virus muy avanzados, que pueden realizar **múltiples infecciones, combinando diferentes técnicas para ello**. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.
- Se consideran muy peligrosos por su capacidad de combinar muchas técnicas de infección y por los dañinos efectos de sus acciones.
- Algunos ejemplos de estos virus son: Ywinz.

Virus de archivo

- Infectan **programas o archivos ejecutables** (archivos con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.
- La mayoría de los virus existentes son de este tipo.

Virus de compañía

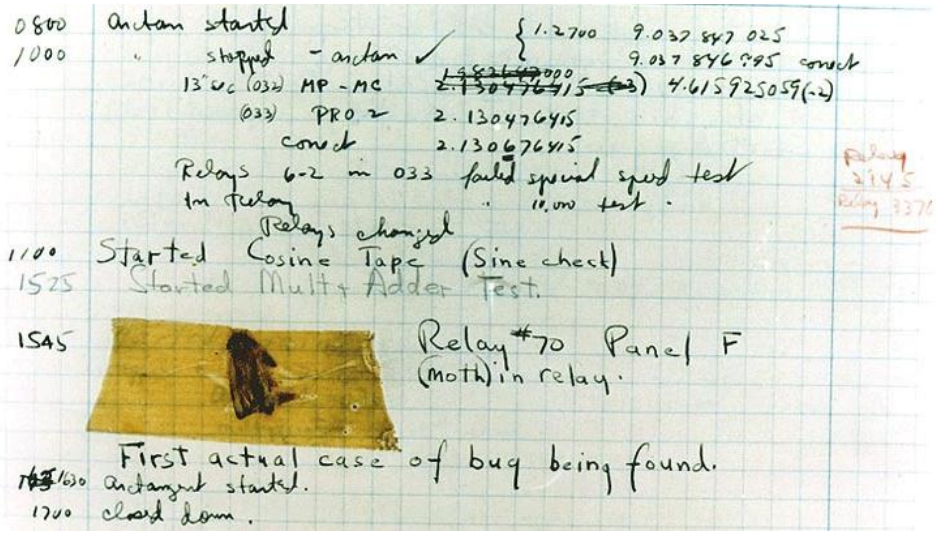
- Son virus de **archivo que al mismo tiempo pueden ser residentes o de acción directa**. Su nombre deriva de que "acompañan" a otros archivos existentes en el sistema antes de su llegada, sin modificarlos como hacen los virus de sobreescritura o los residentes.
- Para efectuar las infecciones, los virus de compañía pueden esperar ocultos en la memoria hasta que se lleve a cabo la ejecución de algún programa, o actuar directamente haciendo copias de sí mismos.
- Algunos ejemplos de este tipo de virus son: Stator, Asimov.1539, Terrax.1069.

Virus de FAT

- La **Tabla de Asignación de archivos o FAT** es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema.
- Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los archivos críticos para el normal funcionamiento del computador. Los daños causados a la FAT se traducirán en pérdidas de la información contenida en archivos individuales y en directorios completos.

Virus: Origen

- Bug-ware es el termino dado a programas informáticos legales que debido a una inadecuada comprobación de errores o a una programación confusa causan daños al hardware o al software del sistema.
- El término "bug" fue asociado a interferencias y malfuncionamiento desde mucho tiempo antes de que existieran los computadores modernos, siendo Thomas Edison uno de los primeros en acuñar este significado. Si bien fue una mujer, Grace Murray Hopper, quién en 1945 documentó el primer "bug" informático.



Virus: Origen

- En 1939, el famoso científico matemático John Louis Von Neumann, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.
- En 1949, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, 3 jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, a manera de entretenimiento crearon un juego al que denominaron **CoreWar**, inspirados en la teoría de John Von Neumann.

Virus: Origen

- Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente **disminuyendo la memoria del computador** y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachussets Technology Institute (MIT), entre otros.
- A pesar de muchos años de clandestinidad, existen reportes acerca del virus Creeper, creado en 1972 por Robert Thomas Morris, que atacaba a las famosas IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto de los software antivirus.

Virus: Origen

- En 1980 la red ArpaNet del ministerio de Defensa de los Estados Unidos de América, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. En Agosto de 1981 la International Business Machine lanza al mercado su primera computadora personal, simplemente llamada IBM PC. Un año antes, la IBM habían buscado infructuosamente a Gary Kildall, de la Digital Research, para adquirirle los derechos de su sistema operativo CP/M, pero éste se hizo de rogar, viajando a Miami donde ignoraba las continuas llamadas de los ejecutivos del "gigante azul".
- En Agosto de 1981 la International Business Machine lanza al mercado su primera computadora personal, simplemente llamada IBM PC. Gary Kildall, de la Digital Research fu buscado para adquirirle los derechos de su sistema operativo CP/M. Aparece Bill Gates, de la Microsoft Corporation y adquiere a la Seattle Computer Products, un sistema operativo desarrollado por Tim Paterson, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de PC-DOS se lo vendió a la IBM. Sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de MS-DOS.

Virus: Origen

- Keneth Thompson quien en 1969 creó el sistema operativo **UNIX**, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública presentó y demostró la forma de desarrollar un virus informático.
- En 1984 el **Dr. Fred Cohen** al ser homenajeado en una graduación, en su discurso de agradecimiento incluyó las pautas para el desarrollo de un virus. Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus, aunque hubieron varios autores más que actuaron en el anonimato.

Virus: Origen

- La verdadera voz de alarma se dio en 1984 cuando los usuarios del BIX BBS, un foro de debates de la ahora revista BYTE reportaron la presencia y propagación de algunos programas que habían ingresado a sus computadoras en forma subrepticia, actuando como "caballos de troya", logrando infectar a otros programas y hasta el propio sistema operativo, principalmente al Sector de Arranque.
- En ese año se difundieron los virus (c) Brain, Bouncing Ball y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión EXE y COM.

Virus: Origen

- El 2 de Noviembre de 1988 **Robert Tappan Morris**, difundió un virus a través de ArpaNet, (precursora de **Internet**) logrando infectar 6,000 servidores conectados a la red.
- En 1989 el virus Dark Avenger o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida técnica de infección.

Virus: Origen

- En 1991 apareció en el Perú el primer virus local, autodenominado **Mensaje** y que no era otra cosa que una simple mutación del virus **Jerusalem-B** y al que su autor le agregó una ventana con su nombre y número telefónico.
- A mediados de 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus: Los llamados macro virus tan sólo infectaban a los archivos de MS-Word.
- En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel.
- 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access.

Virus: Origen

- A principios de 1999 se empezaron a propagar masivamente en Internet los virus anexados (adjuntos) a mensajes de correo, como el macro virus Melissa.
- A fines de Noviembre de este mismo año apareció el BubbleBoy, primer virus que infecta los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato HTML.

Virus: Origen

- El 18 de Septiembre del 2001 el virus Nimda amenazó a millones de computadoras y servidores.
- Los gusanos, troyanos o la combinación de ellos, de origen alemán como MyDoom, Netsky, etc. revolucionaron con su variada técnica.
- No podemos dejar de mencionar la famosa "ingeniería social", culpable de que millones de personas caigan en trampas, muchas veces ingenuas. Los BOT de IRC y a finales del 2005 los temibles Rootkit.

Gusanos (Worms)

- Definición
  - Origen
    - Ejemplos

Gusanos: Definición

- Básicamente, los gusanos se limitan a realizar copias de sí mismos a la máxima velocidad posible, sin tocar ni dañar ningún otro archivo. Sin embargo, se reproducen a tal velocidad que pueden colapsar por saturación las redes en las que se infiltran.
- Las infecciones producidas por estos gusanos casi siempre se realizan a través del correo electrónico, las redes informáticas y los canales de Chat (tipo IRC o ICQ) de Internet. También pueden propagrase dentro de la memoria del computador.

Gusanos: Origen

- El primer gusano gestado en el centro de experimentación Xerox de Palo Alto (Palo Alto Research Center, PARC), en Estados Unidos, por John Shoch, no fue creado para fines maliciosos, sino para ayudar a Shoch en sus tareas de investigación, centradas en el control de redes Ethernet. El programa tomó el nombre de tapeworm, una referencia copiada de una novela de ciencia y ficción a la que Shoch había tenido acceso, titulada The Shockwave Rider de John Brunner.
- Una noche, dos integrantes del equipo de Shoch lanzaron el programa a la red, con la mala fortuna que al corromperse, colapsó la máquina donde estaba alojado el gusano. El gusano, en un efecto dominó, se fue replicando y fue tumbando todas las máquinas que hallaba a su paso en la red local. En primera instancia, dado que las máquinas de la red experimental tendían a colapsar a menudo, no se achacó el problema al que sería primer gusano informático de la historia. Tras un análisis, se dilucidó que el culpable era el programa de control de Shoch. En los calendarios, el año que figuraba era 1982.

Gusanos: Ejemplos

- Melissa
- Bagle.B
- Deadhat.C
- Mydoom.E

Troyanos

- Definición
- Uso
  - Tipos
- Contagio

Troyanos: Definición

- Se puede considerar un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información y/o controlar remotamente la máquina "huesped".
- Un troyano no es de por sí, un virus, 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" solo tiene que acceder y/o controlar la máquina "huesped" sin ser advertido, normalmente bajo una apariencia inocua.
- Su nombre deriva del parecido en su forma de actuar de los astutos griegos de la mitología: llegan al computador como un programa aparentemente inofensivo. Sin embargo, al ejecutarlo instalará en nuestro computador un segundo programa, el troyano.
- Estos son algunos ejemplos de Troyanos: IRC.Sx2, Trifor.

Troyanos: Uso

Los Troyanos puede utilizarse para extraer información confidencial o para hacer daño. En el contexto de la red, un Troyano suele ser más utilizado para espiar y robar información delicada (espionaje industrial). El interés del atacante podría incluir pero no estar limitado a:

- Información de Tarjetas de crédito (utilizadas a menudo para registro de dominios o compras)
- Cualquier dato de cuentas (contraseñas de correo, contraseñas de acceso telefónico, contraseñas de servicios Web, etc)
- Documentos, diseños o fotografías confidenciales
- Direcciones de correo electrónico (por ejemplo, detalles de contacto de clientes)
- Información de calendario relativa al paradero de los usuarios
- Utilización de su equipo para propósitos ilegales, como hacking, scan, flood o infiltrarse en otros equipos de la red o de Internet.

Troyanos: Tipos

- Troyanos de acceso remoto
- Troyanos que envían datos (contraseñas, pulsaciones de teclado, etc.)
- Troyanos destructivos
- Troyanos del ataque Denegación de servicio (DoS)
- Troyanos proxy
- Troyanos FTP
- Deshabilitadores de software de seguridad

Troyanos: Contagio

- **Infección mediante adjuntos**

  Es asombroso cómo muchas personas son infectadas por ejecutar un adjunto enviado a su buzón. Imagine el siguiente escenario: La persona que se ha centrado en usted sabe que tiene un amigo llamado Alex y también conoce su dirección de correo. El atacante camufla un Troyano como contenido interesante, por ejemplo, un chiste basado en Flash, y le envía un correo a usted con el nombre de su amigo. Para hacer esto, el atacante utiliza algún servidor de retransmisión de correo para falsificar el FROM del correo y hacer que parezca que quien lo envía es Alex
- **Infección por descarga de archivos desde un sitio web**

  Los Troyanos también pueden distribuirse a través de un sitio web. Un usuario puede recibir un correo con un enlace a un sitio interesante, por ejemplo. El usuario visita el sitio, descarga algún archivo que cree que necesita o quiere, y sin su conocimiento, se instala un Troyano listo para ser utilizado por el atacante. Un ejemplo reciente es el Troyano ZeroPopUp, que fue diseminado a través de una difusión spam e incitaba a los usuarios a descargar el Troyano, describiéndolo como un productor que bloquearía los anuncios pop-up. Una vez instalado el Troyano enviaría un correo a toda la libreta de direcciones del usuario infectado, promocionando la URL y el software ZeroPopUp. Como este correo se enviaba desde un amigo o compañero, uno es más dado a comprobar la URL y descargar el software.

Bombas Lógicas

- Definición
- Características
- Ejemplos

Bombas Lógicas: Definición

Las bombas lógicas son en cierta forma similares a los troyanos: se trata de código insertado en programas que parecen realizar cierta acción útil. Pero mientras que un troyano se ejecuta cada vez que se ejecuta el programa que lo contiene, una bomba lógica sólo se activa bajo ciertas condiciones, como una determinada fecha, la existencia de un archivo con un nombre dado, o el alcance de cierto número de ejecuciones del programa que contiene la bomba; así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo sin activarse y por tanto sin que nadie note un funcionamiento anómalo hasta que el daño producido por la bomba ya está hecho.

Bombas Lógicas: Características

- El tipo de actuación es retardada.
- El creador es consciente en todo momento del posible daño que puede causar y del momento que éste se puede producir.
- Este ataque está determinado por una condición que determina el creador dentro del código.
- El código no se replica.
- Los creadores de este tipo de códigos malignos suelen ser personal interno de la empresa, que por discrepancias con la dirección o descontento suelen programarlas para realizar el daño.

Bombas Lógicas: Ejemplos

- Un empleado descontento coloca una bomba lógica SiliconValley

  La bomba lógica, que actuó como un virus, afectó a cerca de 1.000 computadores -de los 1.500 que integran la red de sucursales de UBS PaineWebber en Estados Unidos-, eliminando y dañando archivos.
- Juicio por bomba lógica en España

  Un informático se despide voluntariamente del trabajo, pero antes de irse a casa instala una bomba informática, se copia programas y archivos y se lleva lectores de tarjetas magnéticas.

  El 15 de febrero de 1997 la cárcel de Can Brians, en Sant Esteve Sesrovires se quedó sin el sistema de tarjetas con microchip que usan los presos para sus compras en el economato o para sus llamadas telefónicas.

Hoax

- Definición
- Objetivos
- Categorías

Hoax: Definición

- Al margen de las divisiones anteriores, existen ciertos tipos de mensajes o programas que en ciertos casos son confundidos con virus, pero que no son virus en ningún sentido.
- El principal componente de este grupo son los hoaxes o bulos. Los hoaxes no son virus, sino mensajes de correo electrónico engañosos, que se difunden masivamente por Internet sembrando la alarma sobre supuestas infecciones víricas y amenazas contra los usuarios.
- Los hoaxes tratan de ganarse la confianza de los usuarios aportando datos que parecen ciertos y proponiendo una serie de acciones a realizar para librarse de la supuesta infección.
- Si se recibe un hoax, no hay que hacer caso de sus advertencias e instrucciones: lo más aconsejable es borrarlo sin prestarle la más mínima atención y no reenviarlo a otras personas.

Hoax: Objetivos

- Captar direcciones de correo
- Saturar la red empresarial
- Saturar los servidores de correo
- Hacer perder el tiempo

Hoax: Categorías

- Alertas sobre virus incurables
- Mensajes de temática religiosa
- Cadenas de solidaridad
- Cadenas de la suerte
- Leyendas urbanas
- Métodos para hacerse millonario
- Regalos de grandes compañías

Keyloggers

- Definición

- Tipos

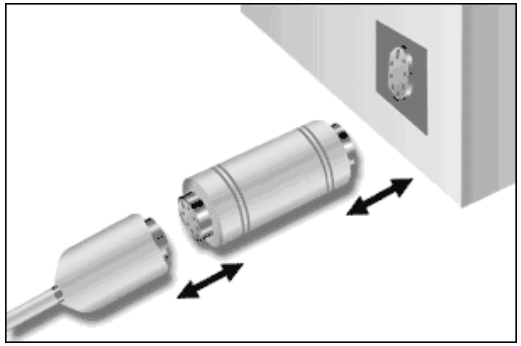
Keyloggers: Definición

El keylogger es un diagnóstico utilizado en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un archivo o enviarlas a través de Internet.

Keyloggers: Tipos

El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software.

- Hardware.
  Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado (lo que los hace inmediatamente disponibles pero visibles si un usuario lo revisa) y al teclado mismo (que no se ven pero que se necesita algún conocimiento de como soldarlos).



Keyloggers: Tipos

- Software

  Escribir aplicaciones para realizar keylogging es trivial y, como cualquier programa computacional, puede ser distribuido a través de un troyano o como parte de un virus informático o gusano informático. Se dice que se puede utilizar un teclado virtual para evitar esto, ya que sólo requiere clics del ratón. Sin embargo, las aplicaciones más nuevas también registran pantallazos que anulan la seguridad de esta medida.

  Ejemplos:

  - Perfect Keylogger 1.6.2
  - Keylogger King Pro 3.3
  - KeyLogger 3.0
  - Monitor de Actividad de teclas KeyloggerFtp

RootKits

- Definición
  - Origen
    - Objetivos
      - Tipos
        - Detección

RootKits: Definición

- El término viene de la unión de “root” y de “kit”. “Root” se refiere al usuario con máximos derechos en sistemas tipo Unix (puede ser Unix, AIX, Linux, etc). Es el superusuario, el “administrador”, en definitiva, es la expresión máxima de autoridad sobre un determinado sistema informático. Por su parte, “kit” se refiere a un conjunto de herramientas, por lo que un rootkit se puede entender como un conjunto de herramientas con categoría de administrador de un sistema.
- Los rootkits tratan de encubrir a otros procesos que están llevando a cabo acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación; o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo. La única limitación es la imaginación del creador.

RootKits: Origen

- El término "rootkit" (también se puede escribir "root kit") en sus orígenes hacía referencia a un grupo de herramientas recompiladas de Unix como ps, netstat, w o passwd que habiendo sido debidamente modificadas, ocultaban cualquier actividad del cracker. De este modo, el intruso podría mantener el control del sistema con privilegios de superusuario, pero quedando oculto a los ojos de los usuarios y administradores.
- Actualmente, el término no está restringido a los sistemas operativos basados en Unix, ya que existen herramientas similares para otros sistemas como Windows (incluso para los sistemas operativos que no utilizan cuentas de root).

RootKits: Objetivos

- Un rootkit oculta inicios de sesión (logins), procesos, archivos y registros (logs).
- Puede incluir software para interceptar datos procedentes de terminales, conexiones de red e incluso el teclado (keylogger). Los rootkits son habitualmente considerados como troyanos.

RootKits: Uso

- Un rootkit se usa habitualmente para esconder algunas aplicaciones que podrían actuar en el sistema atacado. Suelen incluir backdoors (puertas traseras) para ayudar al intruso a acceder fácilmente al sistema una vez que se ha conseguido entrar por primera vez.
- Los rootkits se utilizan también para usar el sistema atacado como "base de operaciones", es decir, usarlo a su vez para lanzar ataques contra otros equipos. De este modo puede parecer que es el sistema inflitrado el que lanza los ataques y no el intruso externo. Este tipo de ataques podrían ser de denegación de servicio (DoS), ataques mediante IRC o mediante correo electrónico (spam).
- Recientemente, algunas aplicaciones de spyware e incluso CDs comerciales con sistemas de gestión de derechos digitales (DRM) han empezado a utilizar rootkits para esconderse a sí mismos de los programas anti-spyware, haciendo su desinstalación del equipo mucho más complicada.

RootKits: Tipos

Los rootkits se pueden clasificar en dos grupos: los que van integrados en el núcleo y los que funcionan a nivel de aplicación.

- Los que actúan desde el kernel añaden o modifican una parte del código de dicho núcleo para ocultar el backdoor. Normalmente este procedimiento se complementa añadiendo nuevo código al kernel, ya sea mediante un controlador (driver) o un módulo, como los módulos del kernel de Linux o los dispositivos del sistema de Windows. Estos rootkits suelen parchear las llamadas al sistema con versiones que esconden información sobre el intruso. Son los más peligrosos, ya que su detección puede ser muy complicada.
- Los rootkits que actúan como aplicaciones pueden reemplazar los archivos ejecutables originales con versiones crackeadas que contengan algún troyano, o también pueden modificar el comportamiento de las aplicaciones existentes usando hacks, parches, cógido inyectado, etc.

RootKits: Detección

Hay varios programas disponibles para detectar rootkits.

- En los sistemas basados en Unix, dos de las aplicaciones más populares son **chkrootkit** y **rkhunter**.
- Para Windows está disponible un detector llamado **Blacklight** (gratuito para uso personal) en la web de F-Secure. Otra aplicación de detección para Windows es **Rootkit Revealer** de Sysinternals. Detecta todos los rootkits actuales comparando las funcionalidades del sistema operativo original con las que se han detectado.

  Sin embargo, algunos rootkits han empezado a añadir este programa a la lista de los cuales no deben esconderse. En esencia, eliminan las diferencias entre los dos listados, de modo que el detector no los encuentra. Pero algo tan simple como renombrar el archivo rootkitrevealer.exe hace que el rootkit ya no sepa que se está enfrentando a un detector. Será una continua batalla entre los rootkits y los antivirus.

Spyware

- Definición
- Funcionamiento
- Tipos
- Motivos
- Síntomas

Spyware: Definición

- Los programas espía, también conocidos como spyware, son aplicaciones informáticas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Los datos recogidos son transmitidos a los propios fabricantes o a terceros, bien directamente, bien después de ser almacenados en el computador.
- El spyware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento de la recogida de datos y la forma en que son posteriormente utilizados.

Spyware: Funcionamiento

Existen diferentes vías de entrada de programas espía en su computador:

- Un troyano los descarga de Internet y los instala.
- Cuando se accede a una página web, y dependiendo de la configuración de seguridad de su navegador, se solicita permiso para instalar un determinado control ActiveX, procedente de una fuente poco fiable o insegura. Si el usuario acepta, se instalan.
- Cuando se visita una página web que incluye código que explota una determinada vulnerabilidad. Si el computador es vulnerable, el malware se descarga y ejecuta automáticamente, sin necesidad de intervención del usuario.
- Están ocultos en la instalación de programas aparentemente inocuos, descargados de Internet y con licencias shareware o freeware.

Spyware: Tipos

Atendiendo a su comportamiento una vez instalados, se diferencian distintos tipos:

- **Hijackers** (literalmente, secuestradores): modifican información del usuario, como por ejemplo la página de inicio y de búsqueda del navegador, alteran los resultados de las búsquedas realizadas, etc.
- **Trackware**: programas que realizan inventarios de las aplicaciones instaladas, rastreo de itinerarios del usuario, etc. Para ello, guardan todas las búsquedas realizadas en el buscador que colocan como página de inicio, o introducen capturadores de teclado (keylogger), que registran todas las pulsaciones de teclas realizadas.

Según su forma de activarse, podemos diferenciar:

- **BHO** (Browser Helper Object): son plugins de los navegadores. Suelen ser cargados al pulsar un enlace de una página maliciosa visitada, y se ejecutarán cada vez que se abra el navegador. Pueden aparecer visibles como barras de herramientas del navegador, o permanecer ocultos mientras realizan una serie de operaciones sin conocimiento del usuario.

Spyware: Motivos

- El spyware es desarrollado por empresas que buscan obtener beneficios económicos por medios poco ortodoxos.
  - Así, recogen información de los usuarios afectados, con el fin de conocer sus gustos y preferencias. Esta información es utilizada por las propias empresas o vendidas a terceros.
  - También pueden distribuir publicidad en diferentes formatos, para promocionar productos o servicios propios o de terceras empresas.
- Banners y ventanas emergentes.
- Modificación de la página de inicio del navegador.
- Modificación de las opciones de búsqueda por defecto, o alteración de los resultados de las búsquedas realizadas.
- Instalación de programas de otras empresas, que pueden ser a su vez otros programas espía, o servir de promoción a una determinada aplicación.

Spyware: Síntomas

Hay varios síntomas que delatan la posible presencia de programas espía o adware (aunque también pueden deberse a otros problemas ajenos a los mismos):

- La aparición de nuevas barras de herramientas (Alexa, Hotbar, MyWebSearch, FunWeb, etc.) en el navegador que el usuario no ha añadido.
- El cambio repentino en la página de inicio del navegador de Internet.
- El bloqueo inesperado del navegador de Internet.
- Aparición de ventanas "pop-ups", banners publicitarios incluso sin estar conectados y sin tener el navegador abierto, la mayoría de temas pornográficos y comerciales (por ejemplo, la salida al mercado de un nuevo producto).
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Es notable que tarda mas en iniciar el computador debido a la carga de cantidad de software spyware.
- Al acceder a determinados sitios sobre el escritorio se oculta o bloquea tanto el panel de control como los iconos de programas.
- Aparición de un mensaje de infección no propio del sistema, así como un enlace web para descargar un supuesto antispyware.

Spam

- Origen
  - Definición
- Medios
  - Técnicas

Spam: Origen

- Originalmente 'Spam' se llamo al jamón con especias (Spiced Ham) producido por Hormel en 1926 como el primer producto de carne enlatada que no requería refrigeración. Esta característica hacia que estuviera en todas partes, incluyendo en los ejércitos americanos y rusos de la segunda guerra mundial.
- El spam mediante el servicio de correo electrónico nació el 5 de marzo de 1994. Este día una firma de abogados de Canter and Siegel, publica en Usenet un mensaje de anuncio de su firma legal, el cual en el primer día después de la publicación, facturó cerca de 10.000 dólares por casos de sus amigos y lectores de la red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

Spam: Definición

'Spam' entonces es la palabra que se utiliza para calificar el correo no solicitado enviado por Internet. La mayor razón para ser indeseable es que la mayoría de las personas conectadas a la Internet no goza de una conexión que no les cueste, y adicionalmente reciben un cobro por uso del buzón. Por lo tanto el envío indiscriminado de este tipo de correo ocasiona costos al lector. Contrario al 'correo basura' o Junk Mail que recibimos en nuestros buzones ordinarios (físicos, en papel!), el recibo de correo por la red le cuesta a un buen numero de personas, tanto en la conexión como en el uso de la red misma. El correo físico no tiene ningún costo para quien lo recibe.

Spam: Medios

- Por correo electrónico
- Por mensajería instantánea
- En grupos de noticias
- En foros
- Por telefonía móvil
- Por telefonía IP
- En mensajería de juegos en línea

Spam: Técnicas

- Obtención de direcciones de correo
- Envío de los mensajes
- Verificación de la recepción
- Troyanos y computadores zombis
- Servidores de correo mal configurados

Phishing

- Origen
- Definición
- Técnicas

Phishing: Origen

- El término phishing viene de la palabra en inglés "fishing" (pesca) haciendo alusión al acto de pescar usuarios mediante señuelos cada vez más sofisticados y de este modo obtener información financiera y contraseñas. Quien lo practica es conocido con el nombre de phisher. También se dice que el término "phishing" es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo.
- La primera mención del término phishing data de enero de 1996 en grupo de noticias de hackers alt.2600, aunque el término apareció tempranamente en la edición impresa del boletín de noticias hacker "2600 Magazine". El término phishing fue adoptado por crackers que intentaban "pescar" cuentas de miembros de AOL.

Phishing: Definición

Phishing es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como phisher se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea.

Phishing: Técnicas

- La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar.
- En otro método popular de phishing, el atacante utiliza los propios códigos del banco o servicio del cual se hacen pasar contra la víctima.

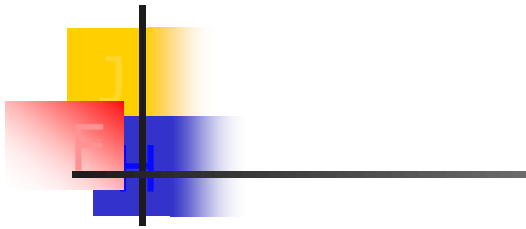
¿Cómo disminuir el riesgo?

Nada puede garantizar la seguridad del equipo de forma absoluta. No obstante, puede reforzarla si tiene en cuenta lo siguiente:

- Instalar un programa antivirus y actualizarlo periódicamente.
- Actualizar el sistema operativo y software en general con los parches de seguridad.

  http://technet.microsoft.com/es-es/security/cc184923
- Proteger tu computadora con un servidor de seguridad.
- Sospechar de los archivos o mensajes desconocidos.
- Usar los discos blandos y discos compactos con precaución.
- Realizar copias de seguridad de tus datos periódicamente.
- Asegurarse del origen antes de obtener programas a través de Internet.
- Mantenerse informado.

Conclusiones



Dudas o comentarios

Muchas gracias por su atención

Referencias

- http://www.geocities.com/ogmg.rm/QueSon.html
- http://www.pandasoftware.es/virus_info/about_virus/information3.htm
- http://www.monografias.com/trabajos15/virus-informatico/virus-informatico.shtml
- http://www.perantivirus.com/sosvirus/general/histovir.htm
- http://mssimplex.com/gusanos.htm
- http://espanol.sbc.com/news_room/connected/que_son_los_virus_o_gusanos.html

Referencias

- http://www.hispasec.com/corporate/noticias/47
- http://www.webpanto.com/article3148.html
- http://www.portalhacker.net/hacker/troyanos.php
- http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx
- http://www.gfihispana.com/es/mailsecurity/wptrojans.htm
- http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node77.html
- http://www.delitosinformaticos.com/delitos/bombalogica.shtml

Referencias

- http://es.wikipedia.org/wiki/Hoax
- http://es.wikipedia.org/wiki/Keylogger
- http://www.baquia.com/noticias.php?id=10363
- http://www.pandasoftware.es/virus_info/spyware/que_es/?sitepanda=particulares
- http://es.wikipedia.org/wiki/Spyware
- http://www.pandasoftware.es/virus_info/spyware/que_es/?sitepanda=particulares

Referencias

- http://www.geocities.com/SiliconValley/Way/4302/spam.html
- http://es.wikipedia.org/wiki/Spam
- http://es.wikipedia.org/wiki/Phishing

Melissa

- Melissa tuvo el dudoso honor de ser el primero de su especie, al menos con distribución masiva. En el mes de marzo cumplió tres años este gusano que inauguró una nueva era de infecciones. Melissa era un virus de macro para Word, su forma de activación, con característica de gusano, dado que se enviaba a los 50 primeros elementos de la lista de contactos Outlook del sistema infectado.
- El sistema de difusión es realmente simple. Sólo hay que insertar el gusano en un sistema, infectarlo, y dejar que se active. El gusano utilizará la libreta de direcciones y se enviará a N sistemas, que a su vez multiplicarán el efecto al mandarlo a cada uno de los elementos de cada uno de los sistemas atacados.
- Melissa fue el precursor de toda una nueva generación de gusanos de este tipo, que posteriormente fue seguida por otros elementos tan conocidos y dañinos como "I Love you", Hybris, Kournikova, CodeRed o Sircam.

Bagle.B

- Empezó a propagarse a gran velocidad por todo el mundo, en un mensaje de correo electrónico escrito en inglés que incluía un archivo con el icono de los archivos de audio WAV.
- Este gusano es capaz de falsificar la dirección del remitente, lo que puede confundir a los usuarios -en el caso de que dicha dirección parezca fiable-, para así conseguir que abran el archivo adjunto que contiene su código.
- Cuando es ejecutado, Bagle.B crea -en el directorio de sistema de Windows- el archivo AU.EXE, que realmente es una copia suya, e introduce una entrada en el registro de Windows para asegurar su ejecución cada vez que se reinicie el computador.
- También intenta conectarse a varias páginas web que albergan un script PHP, para así notificar a su creador que puede acceder al computador afectado a través del puerto 8866.
- Bagle.B sólo se ejecuta si la fecha del sistema es menor o igual al 25 de febrero de 2004.

Deadhat.C

- Se se difunde a través de Internet y del programa de intercambio de archivos punto a punto (P2P) SoulSeek.
- Provoca problemas de arranque, ya que borra archivos que son fundamentales para el correcto funcionamiento del equipo al que afecta.
- Además, finaliza procesos relacionados con algunos programas antivirus y firewalls, lo que deja al PC vulnerable al ataque de otro malware, y termina los procesos correspondientes a los gusanos Mydoom.A y Mydoom.B.
- También merece destacarse que Deadhat.C abre el puerto TCP 2766, permitiendo descargar archivos en el computador por medio de una conexión remota.

Mydoom.E

- Se propaga a través del correo electrónico -en un mensaje con características variables- y del programa de archivos compartidos (P2P) KaZaA. Introduce una librería de enlace dinámico (DLL) que, a su vez, crea un backdoor que abre el primer puerto TCP disponible desde el 3127 al 3198.
- Este componente permite descargar y activar un archivo ejecutable y actúa como un servidor proxy TCP, posibilitando que un hacker acceda, de forma remota, a los recursos de red.
- A partir del 14 de Febrero de 2004, este gusano finaliza sus efectos, terminando su ejecución cada vez que sea activado.

Adware

- Es una palabra inglesa que nace de la contracción de las palabras Advertising Software, es decir, programas que muestran anuncios. Se denomina adware al software que muestra publicidad, empleando cualquier tipo de medio: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc. La publicidad está asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros.
- El adware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento o falta del mismo acerca de sus funciones.