Gusanos, Troyanos, Camaleones , Bombas de Tiempo ..... ¿Qué son?

Gusano ó Worm

Son programas que tratan de reproducirse a si mismo, no produciendo efectos destructivos sino el fin de dicho programa es el de colapsar el sistema o ancho de banda, replicándose a si mismo.

La diferencia fundamental con respecto a los virus es que no pretenden infectar ficheros. El gusano se replica y envía copias para propagarse si encuentra una conexión a una red (generalmente Internet).

Los gusanos han experimentado un crecimiento extraordinario, por la facilidad de propagación y de creación en comparación de un virus en ensamblador, capaz de infectar ejecutables, residente en memoria o polimórfico, por ejemplo. Usan el correo electrónico como vía de propagación, como adjuntos al email o en el cuerpo del mensaje.

Algo más de 300 bytes conocidos como "Slammer" pusieron al borde del colapso buena parte de Internet en enero de 2003. También usan: Ingeniería social, su propio motor de correo, aprovechan fallos de software muy utilizado: por ej. **ejecución en vista previa**, fallos IIS, SQL; **propagación por redes locales**; propagación por redes p2p; a través de **IRC** o similar; escondidos en el HTML del correo; e incluso directamente en páginas de Internet, puertos desprotegidos (Opaserv, Hai).

Los primeros gusanos agotaban los recursos del ordenador y saturaban las redes y/o los servidores. Hoy son criaturas muy complejas con código de virus y troyanos al mismo tiempo, capaces de actualizarse o completarse descargando plug-ins (añadidos) de Internet.

Emplean el correo electrónico, otros el IRC (mIRC y Pirch), la mayoría están escritos en VBS (Visual Basic Script) o están orientados a Windows 32 (API de Windows).

Cada vez son más frecuentes los gusanos que aprovechan todo para propagarse. También abundan los híbridos, que mezclan características de dos o de los tres tipos fundamentales de "malware".

También usan: Ingeniería social, su propio motor de correo, aprovechan fallos de software muy utilizado: por ej. **ejecución en vista previa**, fallos IIS, SQL; **propagación por redes locales**; propagación por redes p2p; a través de **IRC** o similar; escondidos en el HTML del correo; e incluso directamente en páginas de Internet, puertos desprotegidos (Opaserv, Hai).

Caballo de Troya ó Camaleones

En referencia al legendario caballo de Troya son programas que permanecen en el sistema, no ocasionando acciones destructivas sino todo lo contrario suele capturar datos generalmente password enviándolos a otro sitio, o dejar indefenso el ordenador donde se ejecuta, abriendo agujeros en la seguridad del sistema, con la siguiente profanación de nuestros datos.

El caballo de Troya incluye el código maligno en el programa benigno, mientras que los camaleones crean un nuevo programa y se añade el código maligno.

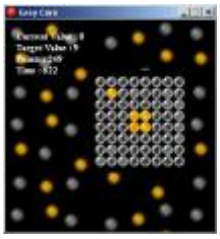
Bombas Lógicas ó de Tiempo

Programas que se activan al producirse un acontecimiento determinado. la condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o un estilo técnico Bombas Lógicas), etc... Si no se produce la condición permanece oculto al usuario.

Retro Virus

Este programa busca cualquier antivirus, localiza un bug (fallo) dentro del antivirus y normalmente lo destruye

¿Qué es BugWare?



Bug-ware es el termino dado a programas informáticos legales diseñados para realizar funciones concretas. Debido a una inadecuada comprobación de errores o a una programación confusa causan daños al hardware o al software del sistema.

Muchas veces los usuarios finales aducen esos daños a la actividad de virus informáticos. Los programas bug-ware no son en absoluto virus informáticos, simplemente son fragmentos de código mal implementado, que debido a fallos lógicos, dañan el hardware o inutilizan los datos del computador.

El término "bug" fue asociado a interferencias y malfuncionamiento desde mucho tiempo antes de que existieran los ordenadores 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.

"bug", traducido literalmente del inglés como "bicho", adquiere otro significado cuando hablamos de informática. Esta otra acepción se refiere a elementos y circunstancias en el software o hardware, involuntarios e indeseados, que provocan un malfuncionamiento.

A lo largo de los años este término se ha popularizado y hoy día se utiliza comúnmente para referirse a los errores en los programas informáticos. La relación con la seguridad informática es directa, ya que muchas de las vulnerabilidades están asociadas a "bugs".

Tipos de Virus según su actuación

Existen una variedad de virus en función de su forma de actuar o de su forma de infectar clasificados de la siguiente manera.

Acompañante

Estos virus basan su principio en que MS-DOS, ejecuta el primer archivo COM y EXE del mismo directorio. El virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar.

Después de ejecutar el nuevo archivo COM creado por el virus y cede el control al archivo EXE.

Archivo

Los virus que infectan archivos del tipo *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT. Este tipo de virus se añade al principio o al final del archivo. Estos se activan cada vez que el archivo infectado es ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados.

Este tipo de virus de dividen el dos:

Virus de **Acción Directa** que son aquellos que no se quedan residentes en memoria y se replican en el momento de ejecutar el fichero infectado y los virus de **Sobrescritura** que corrompen el fichero donde se ubican al sobrescribirlo.