Mini manual de conceptos y ejemplos de gusanos; troyanos y bombas logicas.

By ZERO.CRACKER

Gusanos:

Un worm o gusano informático es similar a un virus por su diseño, y es considerado una subclase de virus. Los gusanos informáticos se propagan de ordenador a ordenador,.Un gusano informático se aprovecha de un archivo o de características de transporte de tu sistema, para viajar.Lo más peligroso de los worms o gusanos informáticos es su capacidad para replicarse en tu sistema,Generalmente, la contaminación ocurre de una manera discreta y el usuario sólo nota el problema cuando el ordenador presenta alguna anormalidad.

Ejemplos de gusanos mas famosos: Sasser,confiker,blaster,lovgate y un gusano de linux
net-worm.linux.adm

Troyanos:

Un troyano informático está tan lleno de artimañas como lo estaba el mitológico caballo de Troya del que se ha tomado el nombre.
A primera vista el troyano parece ser un programa útil, pero en realidad hará daño una vez instalado o ejecutado en tu ordenador. Los que reciben un troyano normalmente son engañados a abrirlos porque creen que han recibido un programa legítimo o archivos de procedencia segura.
Cuando se activa un troyano en tu ordenador, los resultados pueden variar. Algunos troyanos se diseñan para ser más molestos que malévolos (como cambiar tu escritorio agregando iconos de escritorio), mientras que otros pueden causar daño serio, suprimiendo archivos y destruyendo información de tu sistema,robando cuentas de bancos de paypal etc... ademas de cuentas de facebook etc...

Algunas de las operaciones que se pueden llevar a cabo en el ordenador remoto son:

•Utilizar la máquina como parte de una botnet(por ejemplo para realizar ataques de denegación de servicio o envio de spam
•Instalación de otros pŕogramas

•Robo de información personal: información bancaria, contraseñas, códigos de seguridad.
•Borrado, modificación o transferencia de archivos (descarga o subida).
•Ejecutar o terminar procesos
•Apagar o reiniciar el equipo.
•Monitorizar las pulsaciones del teclado (keyloggers)
•Realizar capturas de pantalla
•Ocupar el espacio libre del disco duro con archivos inútiles.
•Borra el disco duro

Ejemplos de troyanos famosos: SPYNET es uno que uso yo xd,netbus,back orifice, bifrost, bandook.

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). Se cree que hay bombas logicas en el code fuente de windows

Ejemplos de acciones que puede realizar una bomba lógica

•Borrar información del disco duro
•Mostrar un mensaje
•Reproducir una canción
•Enviar un correo electrónico
•Apagar el monitor

Con ellos se pueden camuflar troyanos,keyloggers modificando el code fuente del troyano se le puede añadir a una parte del codigo fuente del troyano code de una bomba logica asi despues de haber robados datos se puede teclear una tecla que no se use del todo y asi borrar los datos de la inclusion.