

Mini Turorial
Informativo
sobre los Caballos
de Troya

www.virtualmon.net

Escrito por Getrux – Getrux@gmail.com

Introducción

Esto es un mini-tutorial explicativo, donde se da información sobre los troyanos, funcionamiento etc. Está destinado a un público no experto en la materia.

Con esto quiero decir que se podría decir mucho más sobre los troyanos y ser más específicos, pero lo que intento es hacer algo sencillo y fácil de entender.

¿Qué son los troyanos? ¿Cómo funcionan? ¿Para qué sirven?

Se le llama troyano a un archivo que se esconde en un ordenador y permite acceso a usuarios externos no autorizados.

Hay que señalar que un troyano puede ser programado para cumplir muchas funciones y actuar en ocasiones como un virus u otro tipo de archivo malicioso. Pero tan sólo actuaría como tal, ya que no es un virus.

Un caballo de troya está compuesto por dos archivos: el cliente.exe y el servidor.exe. El servidor se le llama al archivo que tiene como finalidad infectar el ordenador de la “víctima”, alojándose en su ordenador y ocultándose, en ocasiones, reproduciéndose.

El cliente es el archivo desde donde se controla el servidor, normalmente es la parte “gráfica”, visible para el usuario (aunque no tiene porque ser gráfica).

Entremos un poco en materia y dejemos las definiciones por un momento.

Voy a intentar explicar como funciona de la manera más comprensible posible.

Funcionamiento Troyanos de conexión directa.

Hoy en día este tipo de conexión no se hace utilizar apenas, ya que no son factibles con los routers, sólo con los módems; ya explicaré el porqué.

El servidor se envía a la víctima de tal manera que la víctima lo ejecute, para eso hay varios engaños como hacerle creer que es un juego o imagen, es decir, **ingeniería social**

Una vez la “víctima” ejecuta el servidor este no muestra ninguna interfaz gráfica haciendo al usuario creer que no ha pasado nada, la verdad es que la aplicación que acaba de ejecutar sigue activa en el administrador de tareas y seguramente haya podido hacer copias de si mismo en la unidad C:\.

Sigamos, al ejecutar el servidor lo que hará es abrir un puerto y dejarlo a la escucha para recibir órdenes. Con eso el servidor ya habría cumplido por el momento y ahora le tocaría interactuar al cliente.

En el cliente se pondría la Ip de la víctima y se conectaría al servidor a través del puerto que abrió el servidor.

Una vez se estableció la conexión podría mandar todo tipo de órdenes para el cual el servidor ha sido programado y así “controlaría” el ordenador de la víctima.

Como dije antes este tipo de troyanos no sirven hoy en día para los usuarios que utilizan routers, ya que no permite conexiones de entrada y la denegaría.

Pero la solución ha sido fácil. Si el cliente no puede conectarse al servidor con los routers..., hagamos que los servidores se conecten con los clientes, y así aparece la conexión inversa.

Funcionamiento Troyanos de conexión inversa

El mecanismo es el mismo que el anterior de conexión directa, lo que cambia que esta vez el servidor al ser ejecutado intentará conectarse con la Ip, puerto; el cual fue configurado y el Cliente abrirá el puerto y se mantendrá a la escucha esperando que el servidor se conecte. Una vez establecida la conexión ya tienes bajo control el ordenador de la víctima.

Los troyanos han podido ser programados para que cumplan funciones de “broma” por ejemplo para que mueva el ratón, abra la bandeja de cdrom, apague el monitor, etc.

Por lo contrario, pueden ser programados para explorar el sistema y así robar información, datos, modificarlos, borrarlos, etc.

En estudio que se hizo luz el día de 10/05/07. Demuestra que la mayoría de troyanos creados hoy en día están específicamente programados para robar dinero, es decir obtención de beneficios económicos, robos de cuentas bancarias, etc.

Después de esto podréis imaginar que también pueden ser programados para que cumplan la función de un virus, estropeando componentes del ordenador o cualquier cosa que el programador haya sido capaz de hacer.

En definitiva, un troyano es muy versátil

Protección contra los troyanos

La mejor manera de protegerse contra los troyanos, es vigilar los archivos que abriís, por ejemplo: No pueden mandarte una imagen y tener extensión .exe

Por cierto es recomendable activar las extensiones, ya que algunos “Windows” están configurados para

que no muestren las extensiones de los archivos y sólo mostrar el nombre. Eso se puede configurar en Herramientas, opciones de carpeta, ver, y por ahí sale para ocultar las extensiones, la desmarcas.

Tener los antivirus actualizados al día y sobre todo tener un Firewall. El Firewall detectaría que un archivo quiere conectarse a otro ordenador, y vosotros denegando la conexión, no podrían hacer nada.