INICIACIÓN

¿Hay alguien que no tiene ni el más elemental conocimiento del funcionamiento de un troyano?. Bueno, para todos ha existido la primera vez. Nadie nace aprendiendo. Voy a tratar de explicarles paso a paso cómo deben manejar un troyano sin que su ordenador accidentalmente quede infectado. Como el propio título indica, ésta es la sección para principiantes.

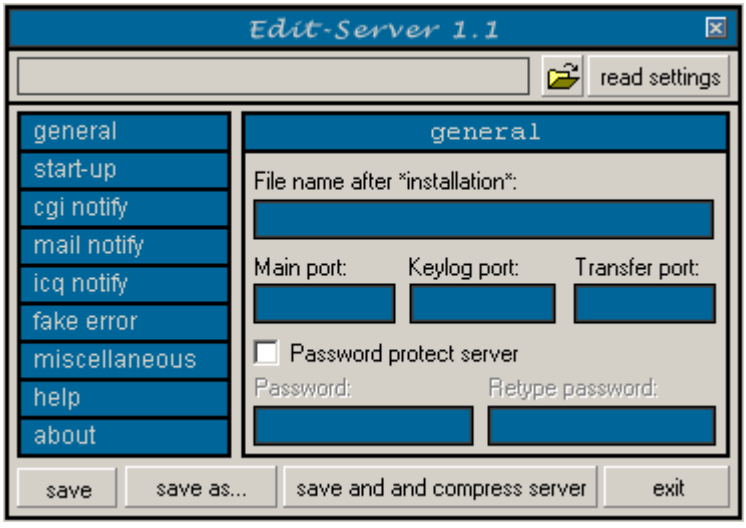
Esta sección sólo está destinada a las personas que no tienen ni la más elemental idea de cómo manejar un troyano. No trataré de explicarlo todo porque cada troyano tiene su propio mecanismo, pero sí les orientará a Ustedes para que por ejemplo se libren de infectarse accidentalmente con estos "engendros" informáticos.

He bajado un troyano de esta web, ¿qué hago ahora?.

Generalmente los troyanos constan de tres partes: Cliente, Servidor y Editor. A nosotros la parte que nos interesa es el Cliente y también el Editor (si es que el troyano la trae, puesto que no es obligatorio). Las traducciones al inglés son muy fáciles, así que nunca tendremos problemas para identificar ambas partes. Extraigamos todos los archivos del Zip a una carpeta y observemos los nombres de los archivos. Previamente es conveniente deshabilitar el antivirus porque de lo contrario no seremos capaces de manejar esos archivos "infectados". Por ejemplo, vamos a descargarnos el netdevil15.zip (las imagenes que salen aquí son para la versión 1.1, pero nosotros usaremos la 1.5 que es la mas nueva, las opciones no difieren mucho):

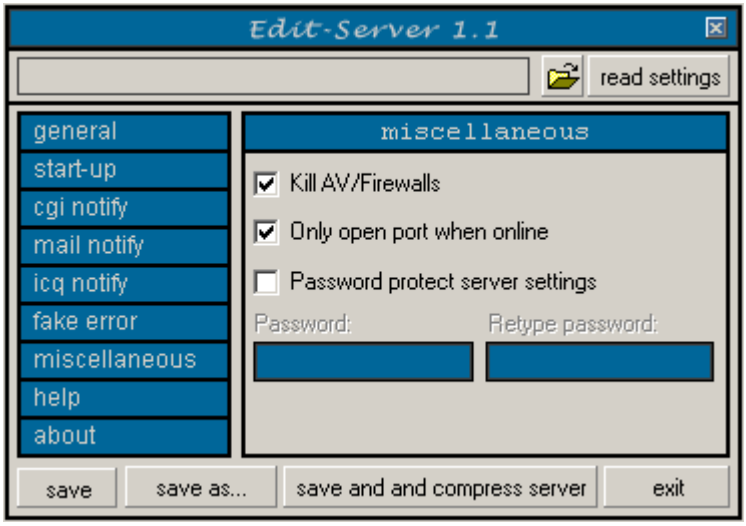
http://www.trojanfrance.com/index.php?dir=Trojans/NetDevil/&file=NetDevil%20v1.5.zip

¿Qué hacemos ahora?. Bien, una vez descomprimido y descargado en una carpeta, deberemos identificar sus componentes: el más peligroso es el servidor; no hagan clic nunca sobre él pues quedarán automáticamente infectados. El servidor es fácilmente identificable como Server.exe. El siguiente paso es identificar el Editor. En el caso de nuestro troyano es Edit-server.exe. Este archivo sí que es conveniente abrir. Tranquilos, no quedará nadie infectado aunque el antivirus así lo indique. ¡Qué no corra el pánico!. No hay ningún problema; lo que sucede es que el antivirus identifica el código en todas las partes del troyano, pero no hay peligro. Una vez abierto el Editor hay que proceder con mucho cuidado a editar el servidor. Si nos equivocamos y hacemos doble clic sobre el servidor, estaremos contaminados. Una vez abierto el editor veremos algo como esto:



Ahora tendremos que leer el servidor en nuestro editor. Para ello hacemos clic en el símbolo de la carpeta abierta que está en la parte superior derecha y buscamos el servidor; es decir, el archivo Server.exe. A

continuación pulsamos en "read settings" y ya tenemos los datos de configuración original del servidor. Ahora podemos editarlo como más nos plazca. Lo más sensato para un principiante es que no toque ninguno de los datos de configuración original salvo, si acaso, un par de ellos. Por ejemplo, sería conveniente ir a "ICQ notify" y colocar nuestra UIN y no la que viene en la configuración original que apunta hacia la UIN del creador del troyano. Asimismo también deshabilitaremos la notificación por CGI y cambiaremos si acaso la cuenta de correo electrónico hacia una nuestra (aunque en Net-Devil no lo recomiendo). Vean Ustedes ahora esta otra pantalla:



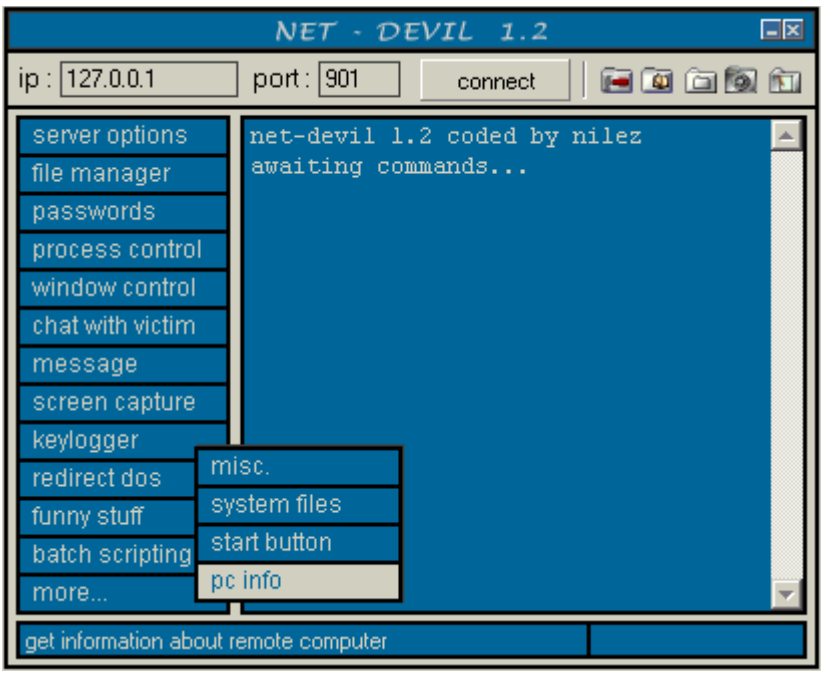
Esta pantalla la encontraremos en Miscellaneous. Si pulsamos en Kill AV/Firewalls dejaremos a la víctima sin cortafuegos ni antivirus una vez que el servidor se ejecute. Recuerden Ustedes que esto es una putada enorme, pues no tendrá antivirus otra vez la víctima hasta que no eliminen de su ordenador el troyano. Así que yo no recomiendo el uso de esta función. En cambio, la función de abajo sí es más útil porque sólo abrirá el puerto de comunicación del troyano cuando esté online. Esto minimiza el riesgo de detección y no hace daño a la víctima.

Una vez editado el servidor, deberemos grabar los cambios. Para ello tenemos dos opciones: grabarlo directamente como "save as..." (es conveniente ponerle un nombre que no levante muchas sorpresas como windowsdll.exe), o grabarlo y comprimirlo con UPX; para esto último usaremos "save and compress server". Si lo comprimimos el servidor será un 50% más pequeño, pero en cambio no se podrá editar otra vez a menos que lo descomprimamos.

Una vez listo el servidor, ya está disponible para infectar ordenadores.

He recibido una notificación de la máquina infectada, ¿qué hago ahora?

En este punto es cuando entra en funcionamiento el cliente. Vayamos a Net-Devil.exe y hagamos doble clic sobre él. Nos aparecerá una pantalla como ésta:



Aquí las posibilidades son muchas, así que no las voy a explicar todas. Además, Net-Devil es un troyano muy intuitivo que se maneja sin manual: ¡es muy fácil!. Lo que más nos interesa es el cuadro para la IP (127.0.0.1) y el del puerto de conexión (el 901 por defecto). Una vez tengamos notificada la IP de la víctima, tendremos que colocarla en el cuadro de la IP, así como el puerto. Si no hemos editado el servidor con clave, entraremos directamente al pulsar el botón "connect". Nuestra petición viajará a través de Internet hasta llegar al servidor del troyano que permanece a la escucha. A partir de este momento la máquina de la víctima estará a nuestra disposición y es por ello que deberemos ser cautos y, sobre todo, éticos. Lo ideal es no cambiar absolutamente nada en el ordenador del servidor, no utilizar nunca información privada para ningún propósito, y no usar la transferencia de archivos (File Manager) para introducir otros virus que puedan dañar el ordenador. Prueben funciones como el Keylogger, el capturador de pantallas (Screen Capture), los archivos del sistema (system files), etc, pero no dejen huellas nunca en el ordenador de la víctima. Y sobre todo, no se olviden de borrarle el servidor a la víctima una vez que ya han probado las funciones, porque si no lo hacemos otro desaprensivo podría entrar en ese ordenador y hacerle mucho daño a la víctima.

Jamás borren ningún archivo crítico del sistema, no guarden ninguna contraseña para usarla después, borren la información del Keylogger inmediatamente y no conserven nada de la víctima. Si activan la Web Cam, huyan del morbo porque en la mayoría de las ocasiones estamos viendo la actividad íntima de una persona en su propia habitación (el espacio más íntimo en la vida de una persona). Respetemos eso. Simplemente comprobemos que la Web Cam funciona bien y desconectémosla rápidamente.

Conviene que los principiantes sean enseñados en el uso de los troyanos como herramientas de aprendizaje y no como armas para dañar a la gente. Ése es el propósito que me mueve a la hora de diseñar esta página. Espero que mis "alumnos" sigan al pie de la letra mi código ético.

Autor: **Coolvibes**

Página: Indetectables.com.ar