T-ZINE

Trojan Magazine

BY ANTRAX

ANTRAX@E-R00T.NET

CONFIGURACION

Bueno, ahora llega la parte en la que comenzaremos la configuración del troyano que queramos utilizar.

Es bueno tener un tipo de idea de los troyanos existentes, de cuales son los que más se utilizan, etc.

En mi opinión personal, el mejor es el Bifrost. Siempre es bueno tener la ultima versión. En el caso del Bifrost es la 1.2.1D que es la versión privada pero que ya es publica.

Tambien existen otros muy buenos como lo son el Poison Ivy, Spy-Net, Nuclear RAT, y otros.

Es bueno saber primero que nada lo que deseamos hacer con la pc que queramos infectar, para tener una idea de lo que vamos a hacer con el troyano.

Como por ejemplo hay troyanos como el Nuclear RAT que tiene la opción de explorar los discos que están en una Red LAN.

Pasare a explicar como se configura alguno de los troyanos mas conocidos en la red.

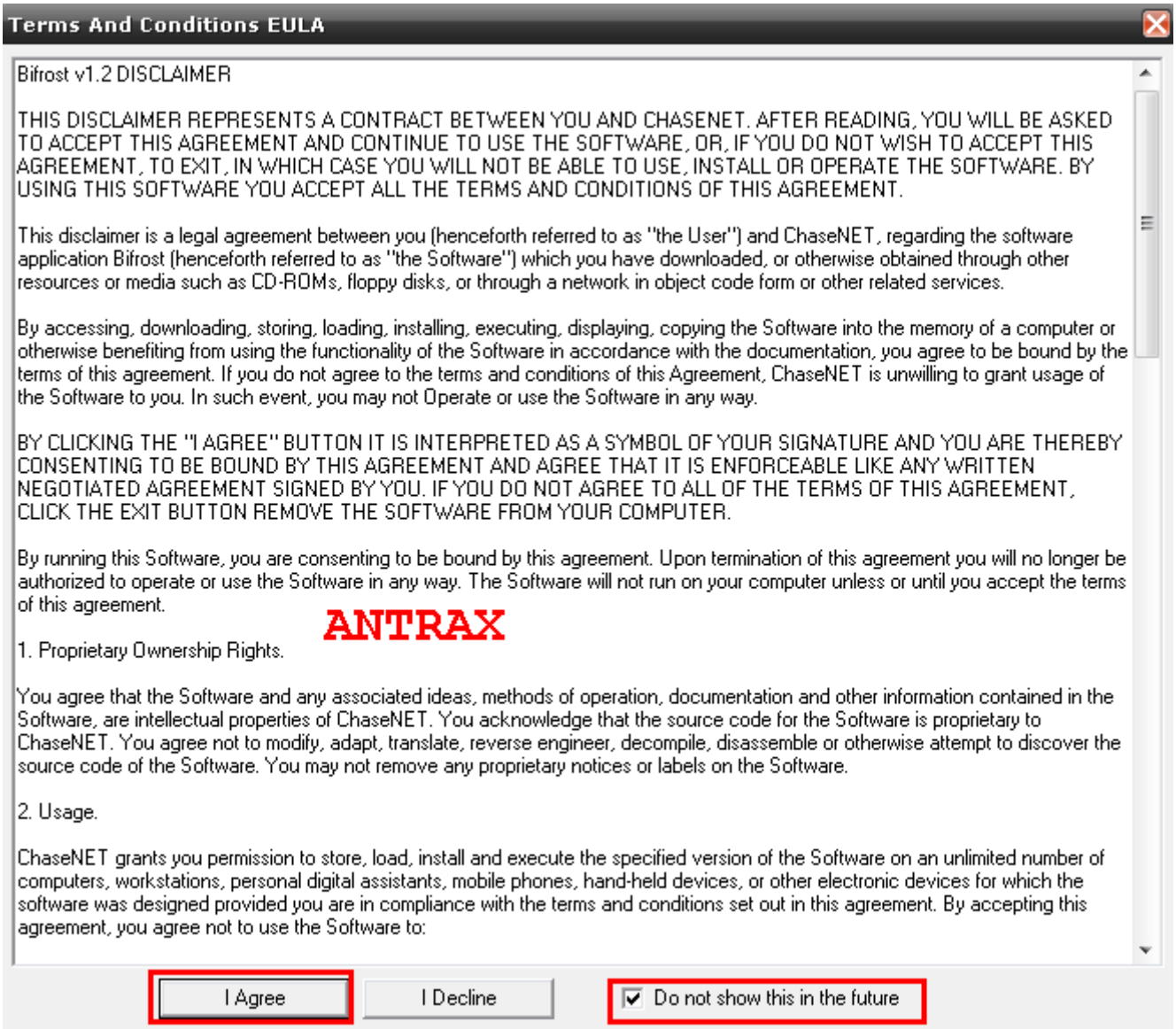
Comenzare por el Bifrost.

BIFROST

Bueno, lo que debemos hacer es abrir el cliente de el Bifrost. Para esta demostración utilizare la versión 1.2.1D.

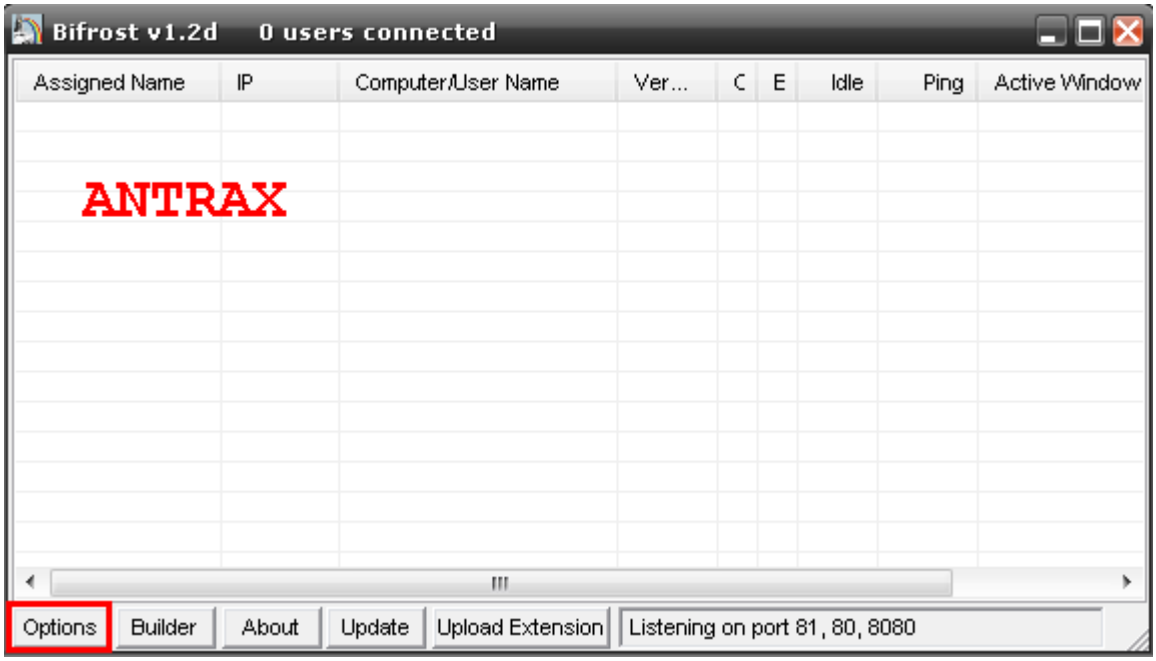
Abrimos el cliente, que es el que esta en rojo.

La carpeta Computers es en donde se almacenaran los archivos que descarguemos de la pc que hayamos infectado, y el server es el que les enseñare a editar para que lo envíen a quien quieran infectar.

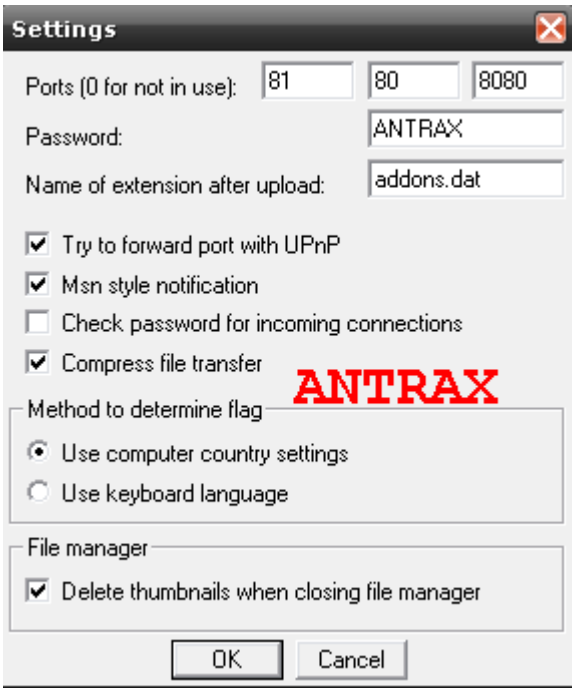


La primera vez que abrimos el troyano aparecerá esto, tildamos el cuadrito en donde dice “Do not show this in the future” para que no vuelva a aparecer y hacemos click en I Agree.

Seguido a esto, se abrirá el cliente.



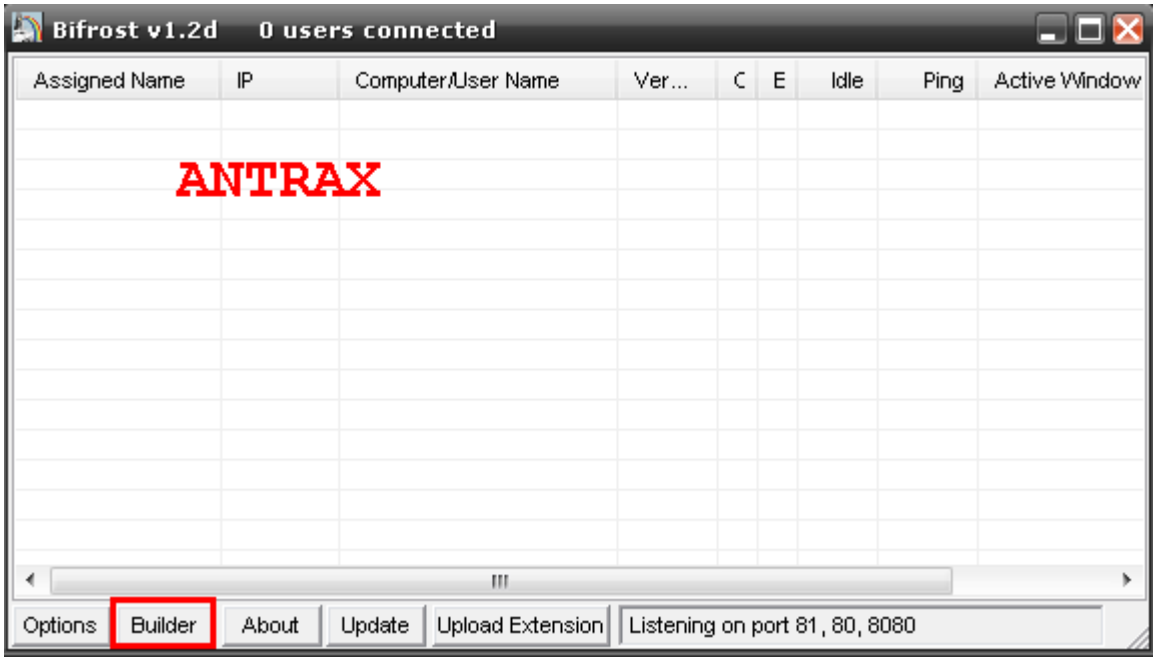
Damos click en Options como muestra la imagen.



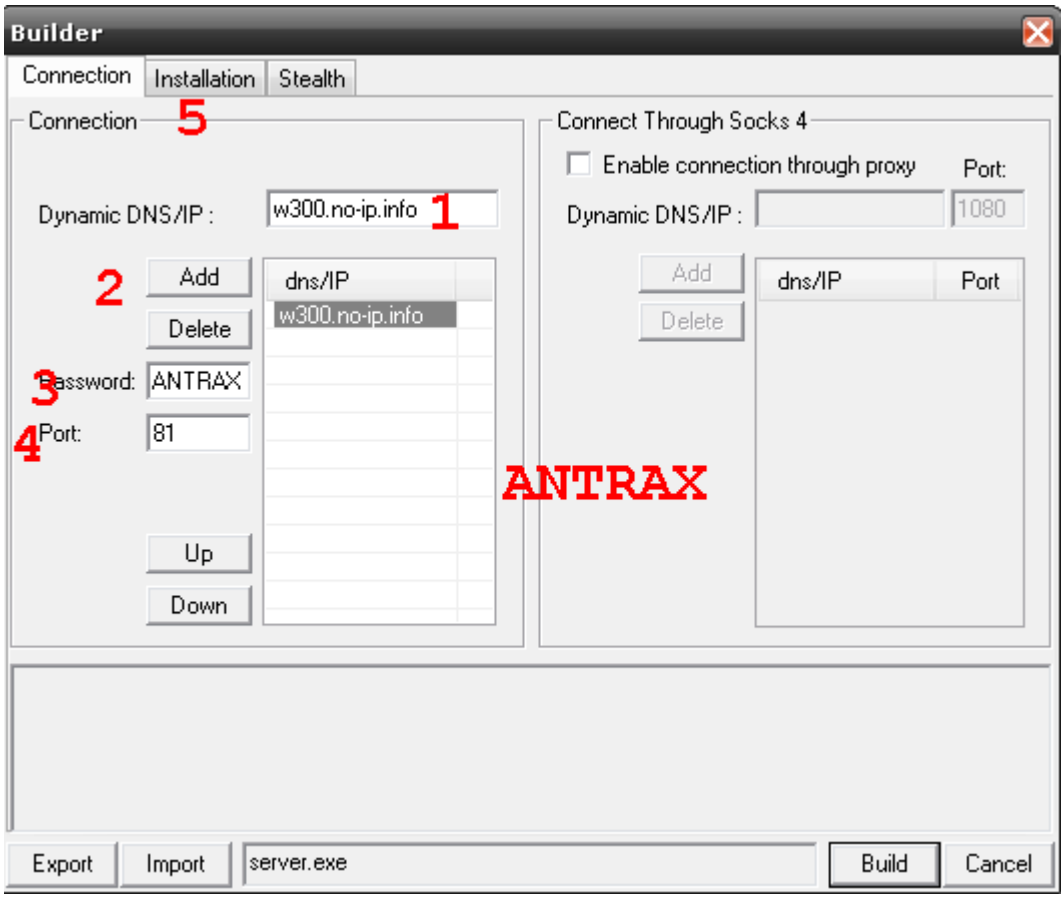
Aquí solo ponemos los puertos que tengamos abiertos en nuestro Router. En caso de no tenerlos deberas buscar en google como abrirlo o pidiendo ayuda en algún foro.

En el password deben poner alguna contraseña que deseen.

Una vez completado todo esto, dar click en OK.



Ahora vamos al botón Builder para editar el servidor.



Seguir los pasos en orden para evitar equivocarse.

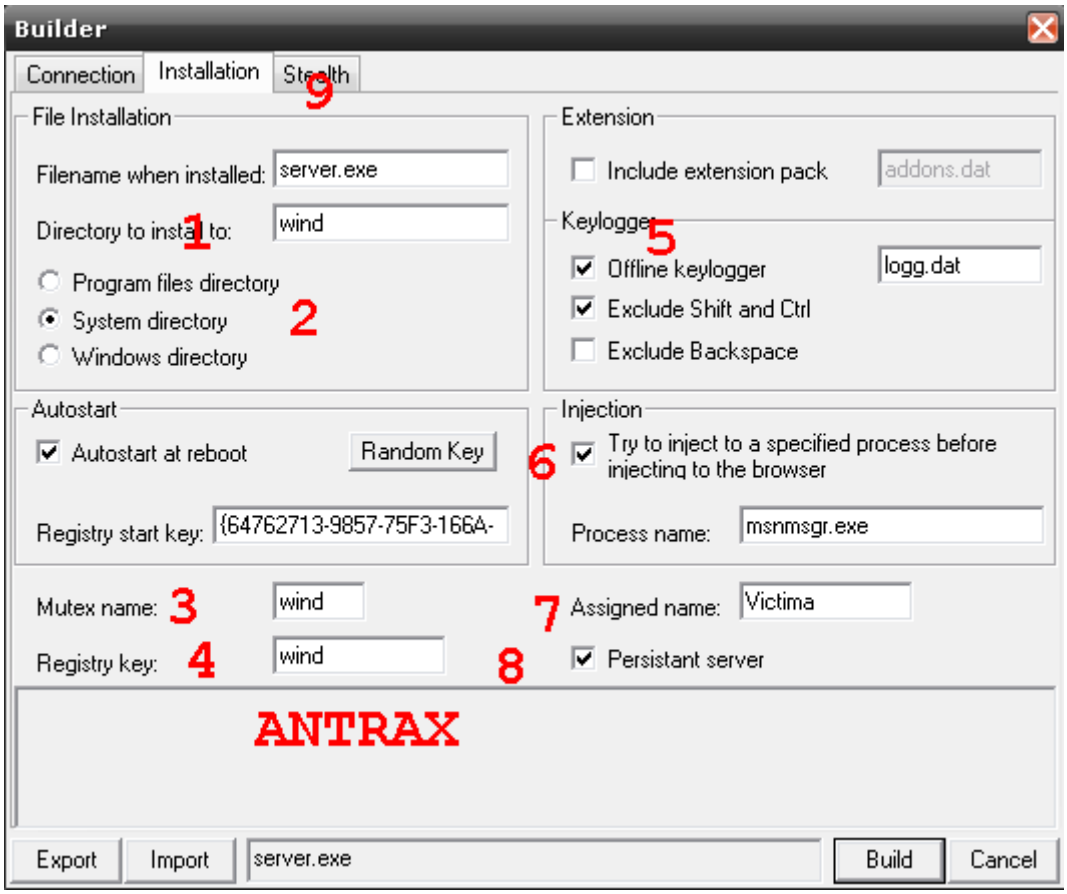
1) Escribir la no-ip que crearon para ustedes

2) Click en Add para que aparezca en la lista como muestra la imagen

3) Escribir la misma password que escribieron en la configuración del cliente

4) Escribir el mismo puerto que escribieron en el cliente. Solo escribir el primero

5) Click en la pestaña Installation



1) Escribimos un nombre para que el server se oculte en dicho directorio.

2) Tildamos en que parte del sistema queremos que se oculte el server. En este caso puse la carpeta de System

3) En mutex name se lo cambiamos por alguno que pase desapercibido.

4) Lo mismo que en el 3

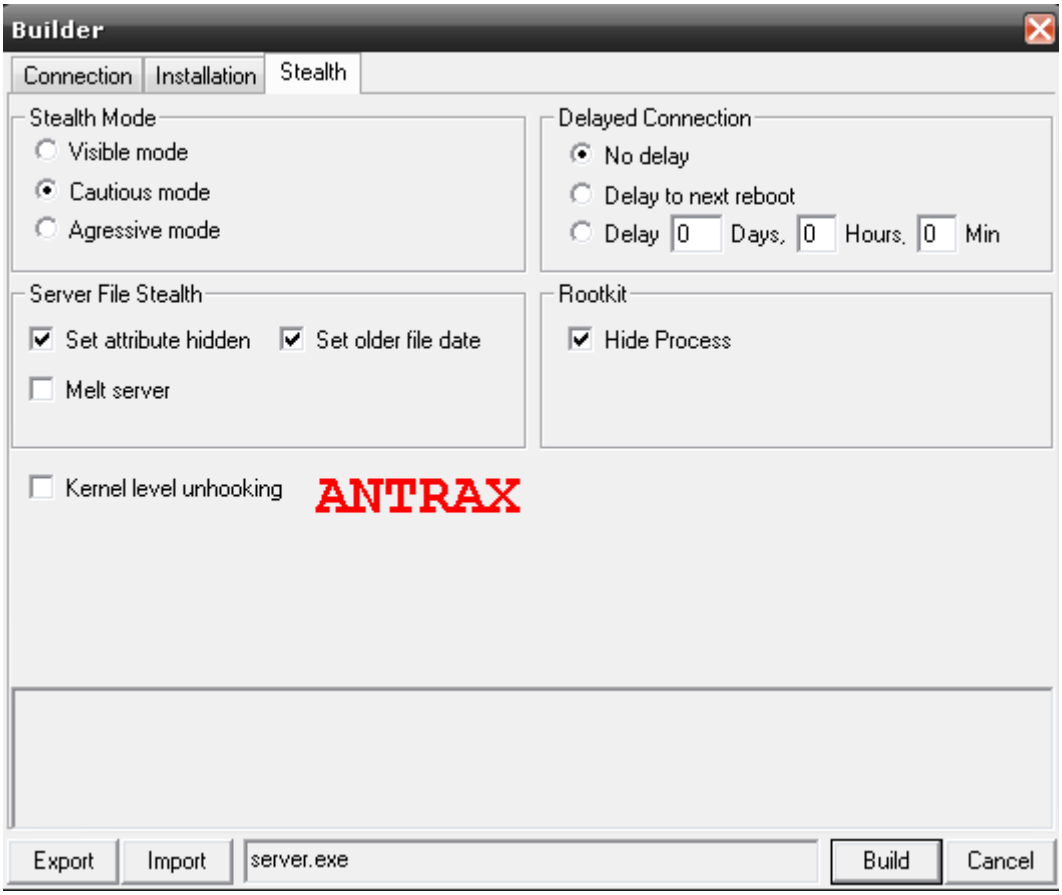
5) Activamos el Offline Keylogger

6) Activamos la opción para que se inyecte en algún proceso.

7) Si quieren le pueden poner algún nombre al server para cuando infecten a alguien sepan diferenciarla.

8) Activamos esta opción que es fundamental para que no se pierdan las victimas cuando se reinicia la pc

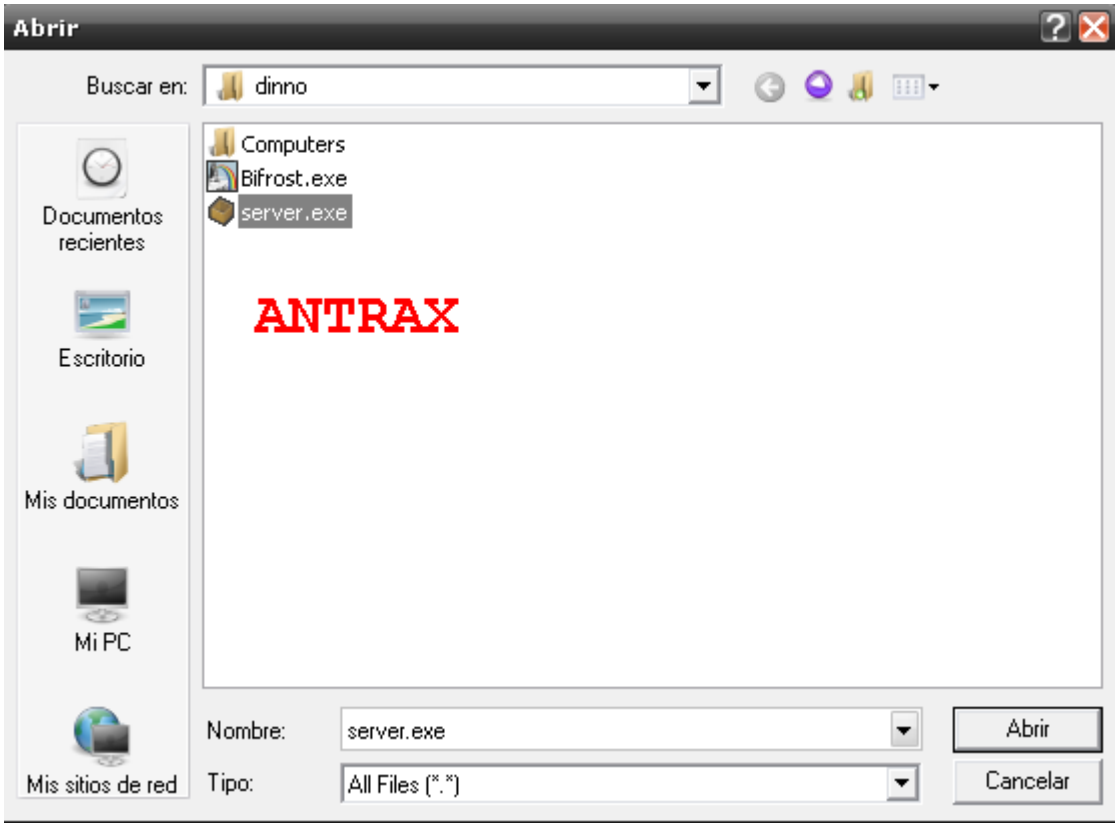
9) Pasamos a la siguiente y ultima pestaña de configuración.



Aquí es todo un poco mas personalizado. Esto trata de cuando queremos que comience a actuar el servidor, de que modo queremos que actue, etc

Yo tilde esas opciones por que son las que mas me gustan. En especial Hide Process para ocultar el proceso en el cual se inyecto el servidor.

Una vez hecho todo esto, le damos click en Build y saldrá algo como esto:



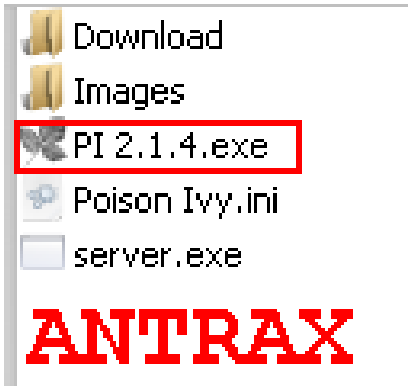
Seleccionamos el Server.exe y damos click en Abrir.

Si muestra un cartel como el siguiente, es por que todo salió bien

Si aparece algún tipo de error, es por que debes quitar el antivirus o desactivarlo.

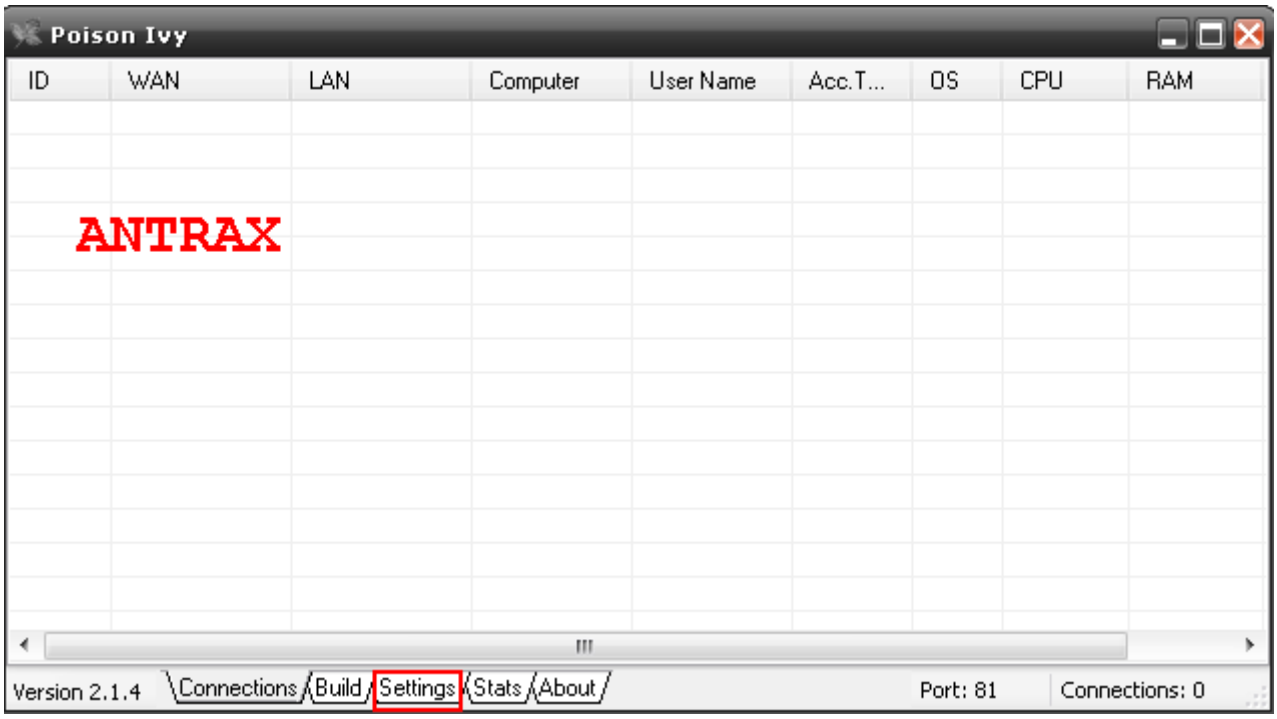
Una vez hecho esto, ya tendremos el servidor listo para enviarlo.

POISON IVY

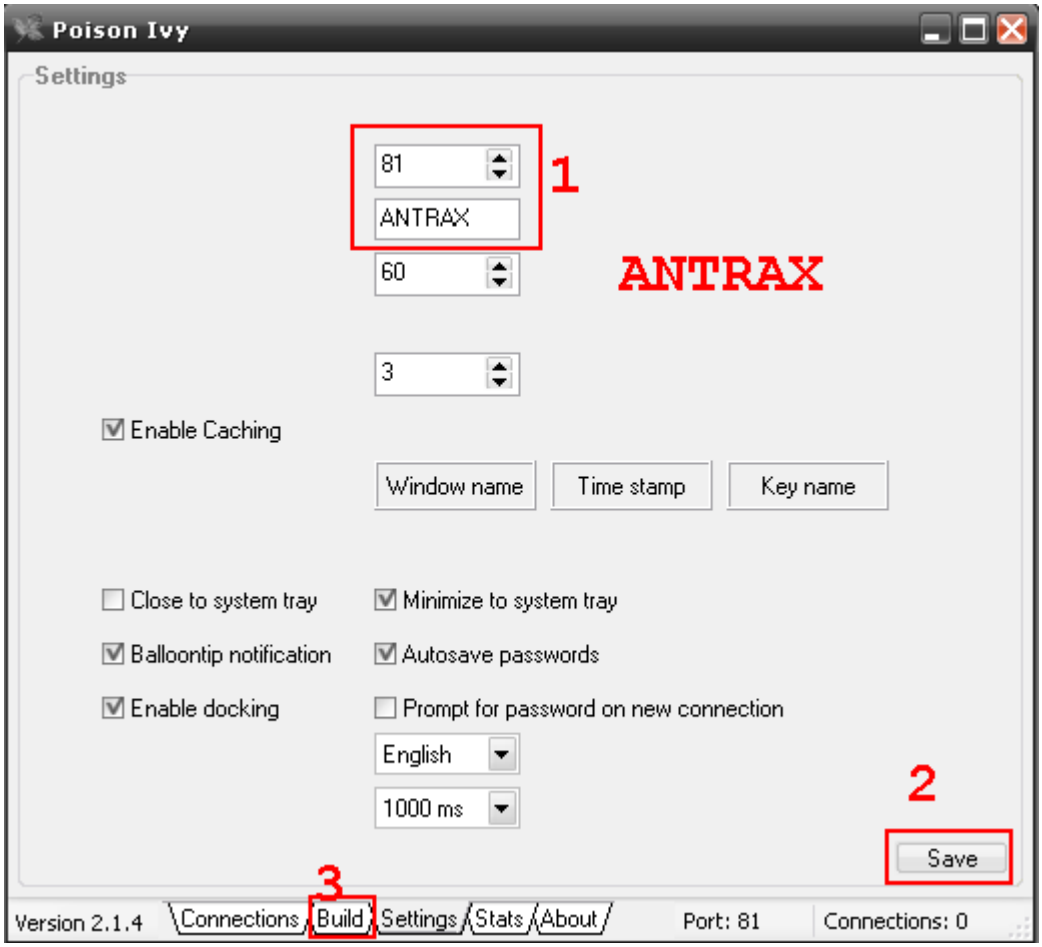


Para este manual usare la versión privada mas reciente del Poison Ivy.

Abrimos el cliente, y veremos algo como lo siguiente:



Ahora nos dirijimos a Settings para configurar el cliente.

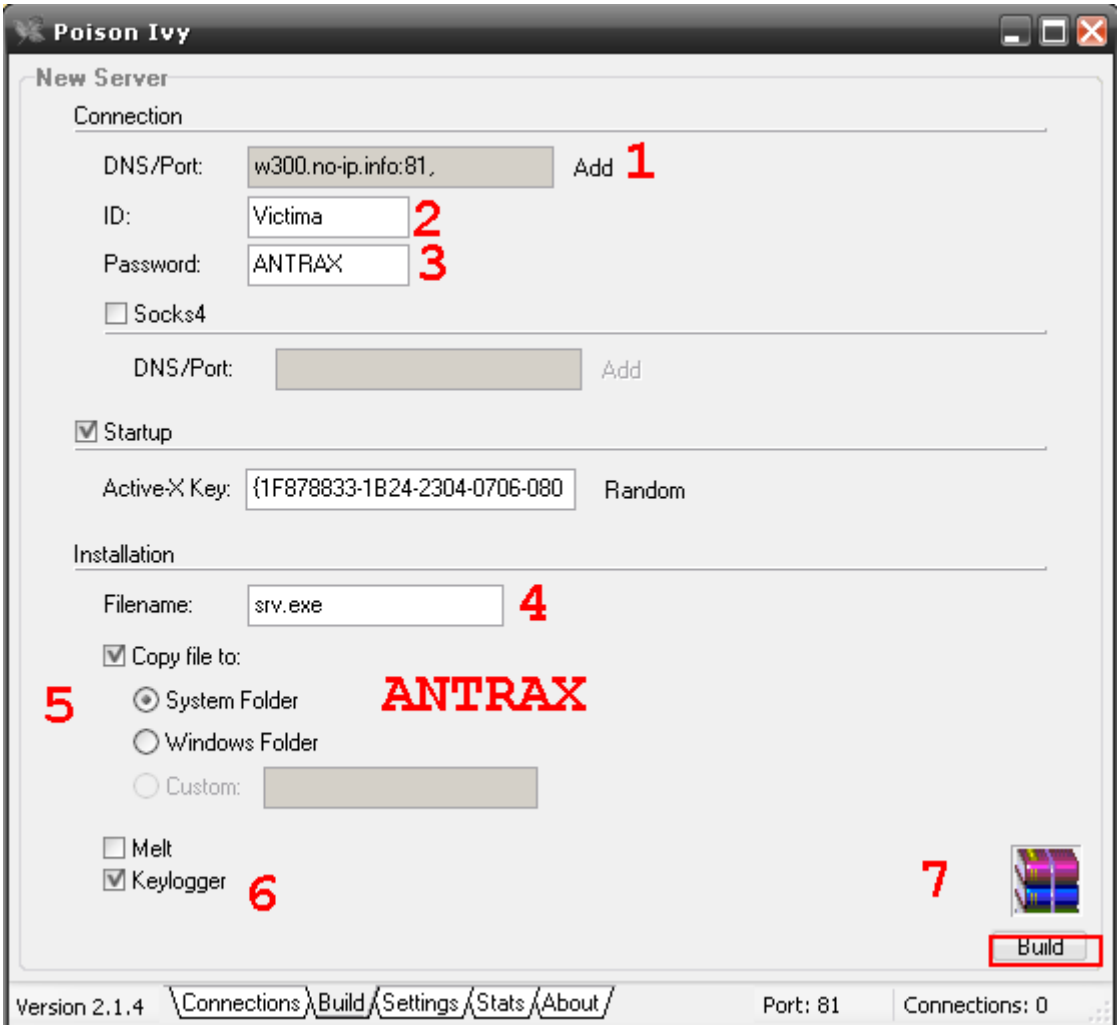


Para la configuración de el cliente es muy fácil al igual que la del Bifrost.

1) Escribimos el puerto que tengamos abierto y una password.

2) Damos click en Save

3) Pasamos a Build para configurar el servidor



1) Damos click en Add y ponemos nuestra no-ip seguida de nuestro puerto abierto.

2) Si quieren pueden ponerle un nombre especifico para que diferencien a la pc que infecten

3) Escriban la misma password que escribieron en el cliente

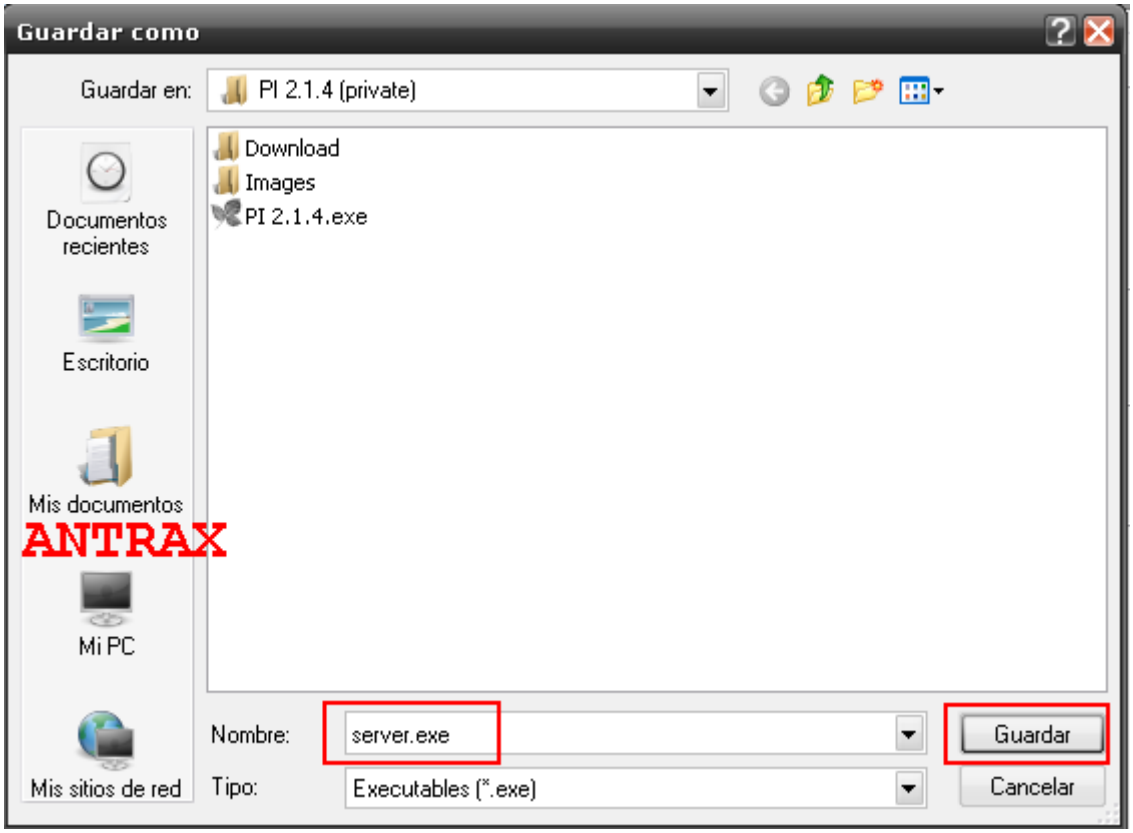
4) Pueden darle un nombre al servidor

5) Eligen en donde quieren que se instale el server, en este caso en System

6) Activamos el keylogger y si quieren pueden activar en Melt para que el servidor se derrita o desaparezca al ser ejecutado

7) Si quieren pueden ponerle un icono

8) Por ultimo click en Build



Escribimos el nombre, en este caso Server.exe. Atencion! No olvidar la extensión *.exe por que es fundamental! Lo que pueden cambiar es el nombre y ponerle el que quieran.

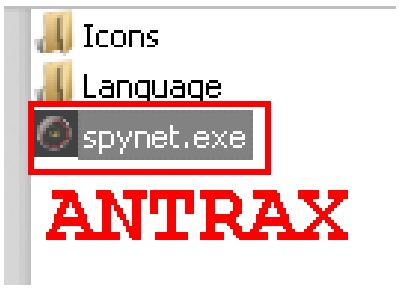
Una vez hecho click en Guardar, tendrán el server creado y listo para ser utilizado.

SPY-NET

Este troyano es el mas reciente, pero lamentablemente el creador no seguirá con el proyecto.

De todas formas es un excelente troyano y a continuación mostrare como se configura. Esta es la ultima versión 1.8.

Abrimos el cliente:



Al abrirlo, verán algo como esto:

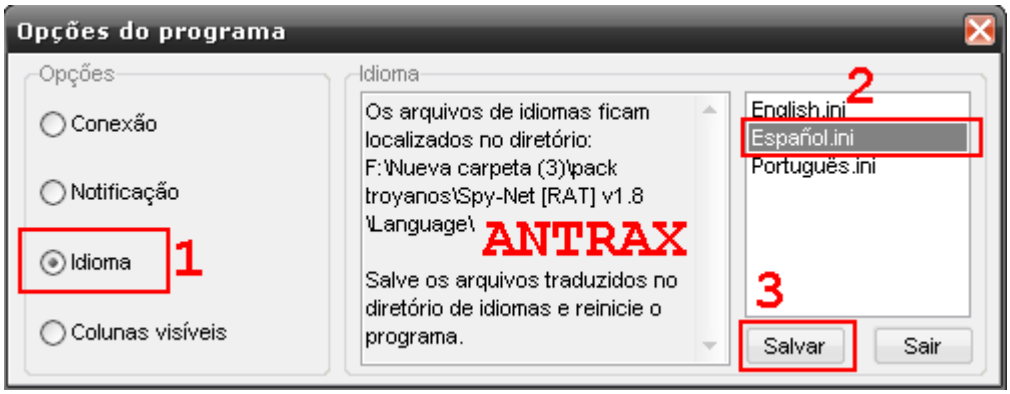
Son dos opciones de cómo quieren enviar los plugins.

Recomiendo por comodidad dejar la opción que esta puesta y darle a OK

Esto los llevara directamente al cliente:

No se asusten, el creador es portugués, ahora les enseño a como pasarlo a español.

Damos click en el botón marcado en rojo, que supuestamente dice Opciones.



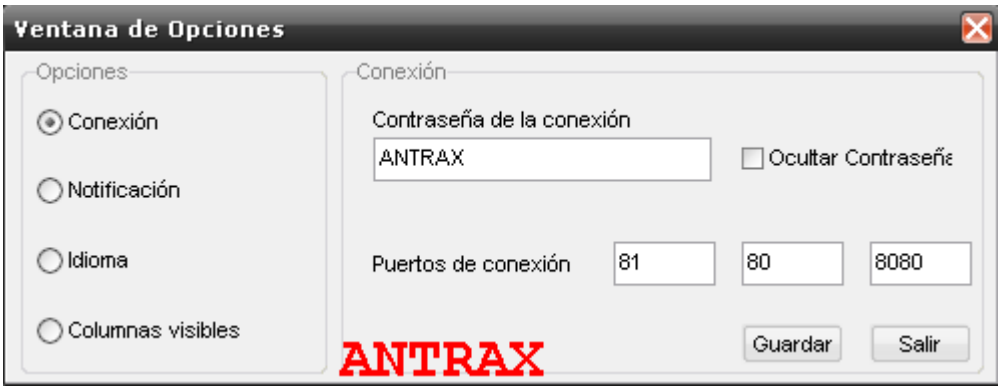
1) Click en Idioma

2) Seleccionan Español.ini

3) Click en Salvar

Listo, ya lo tenemos en español, ahora será mas fácil trabajarlo.

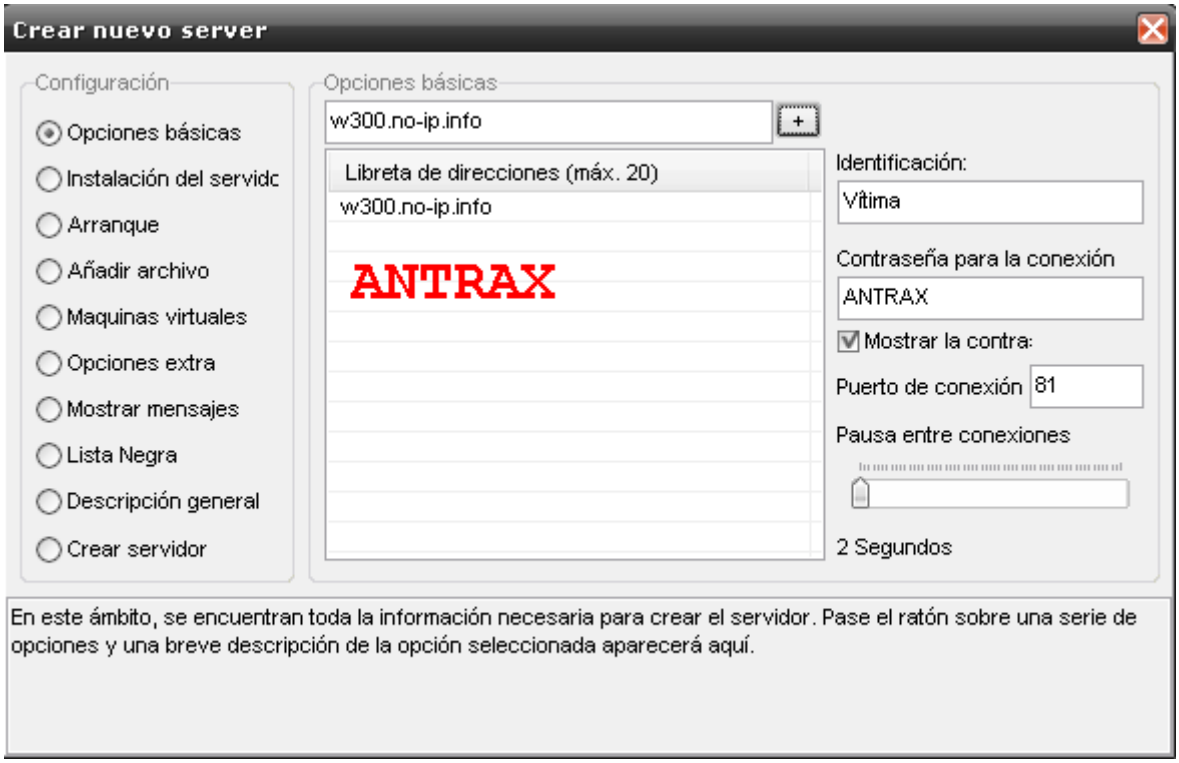
Vamos nuevamente a opciones. Para configurar el cliente.



Ponemos una contraseña que queramos, y escribimos los puertos que tengamos abiertos en nuestro Router.

Una vez hecho vamos a Guardar.

Ahora vamos a Nuevo para crear el servidor.



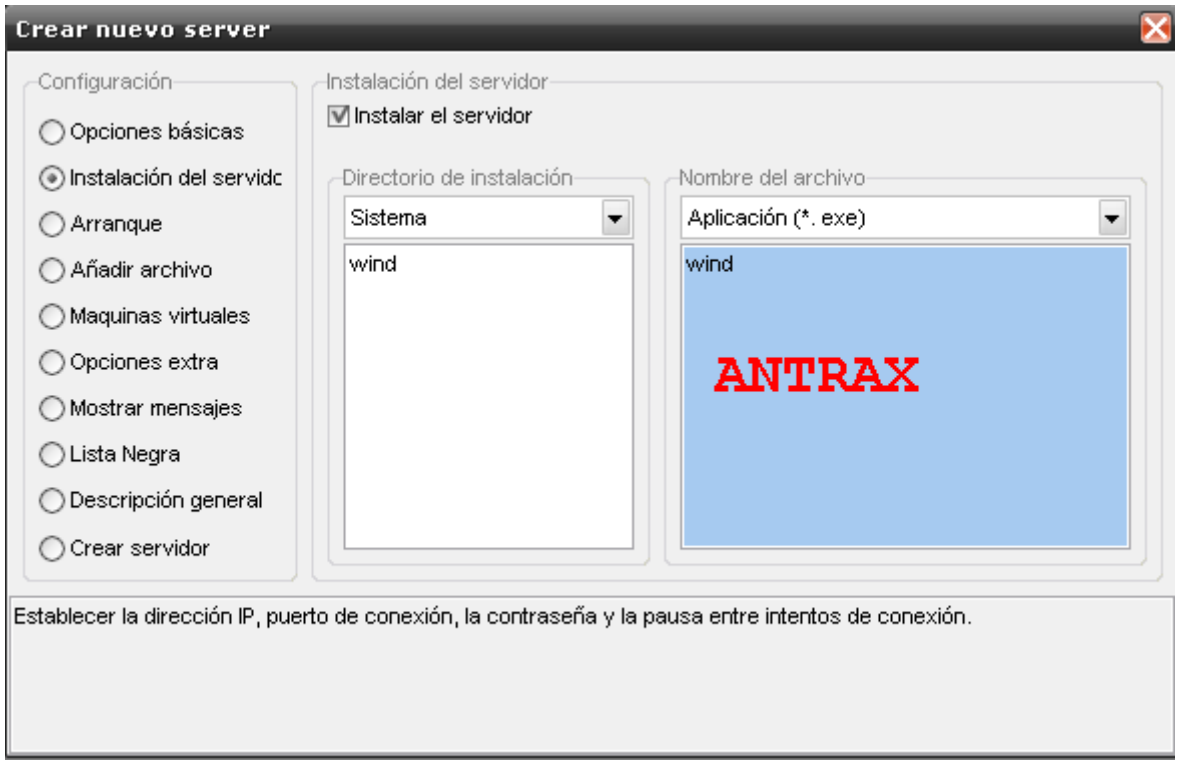
Lo que debemos hacer aquí, es agregar nuestra no-ip en la lista.

Si quieren en donde dice Victima pueden cambiarle el nombre para identificar a la pc a la cual infectaran

En la contraseña, deben poner la misma que en la configuración del cliente.

Y por ultimo ponen el puerto que tengan abierto, recuerda que debe ser el primero que colocaste en el cliente.

Pasamos a la segunda opción:

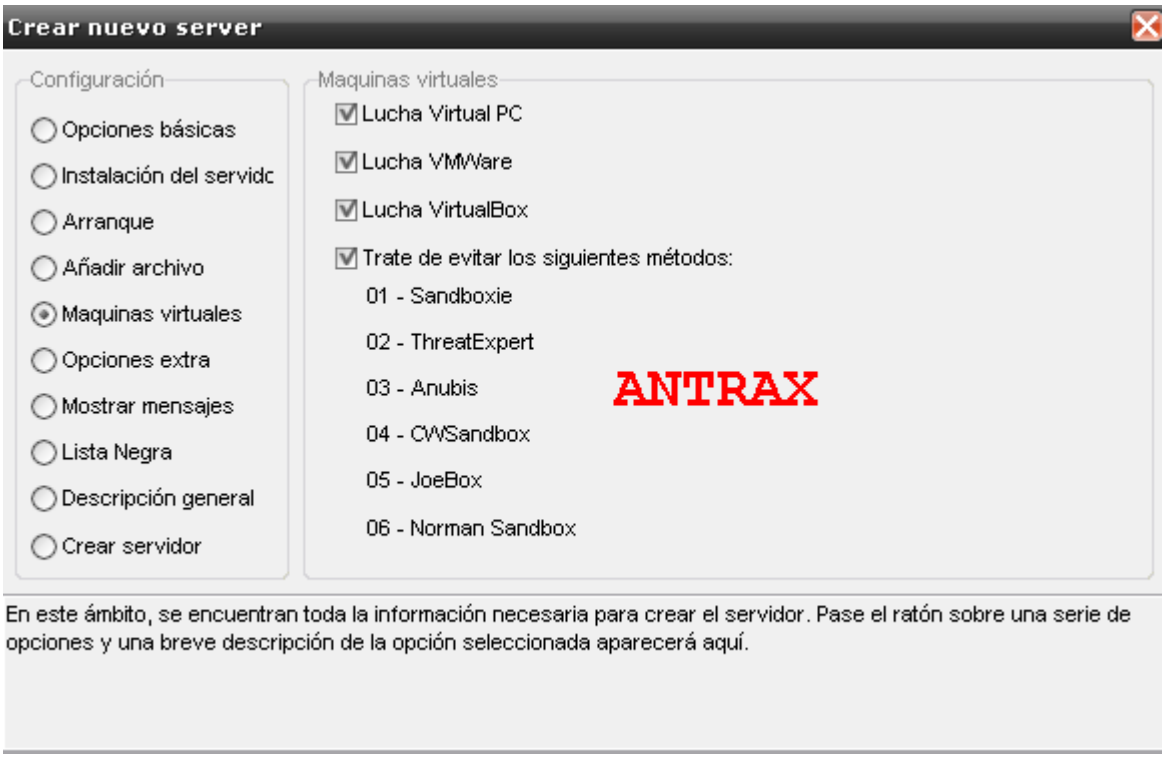


Aca es en donde se instalara el servidor en la pc que infectamos. En este caso se instalara con el nombre en una carpeta que se llama wind dentro de system, y el server se llamara wind.exe

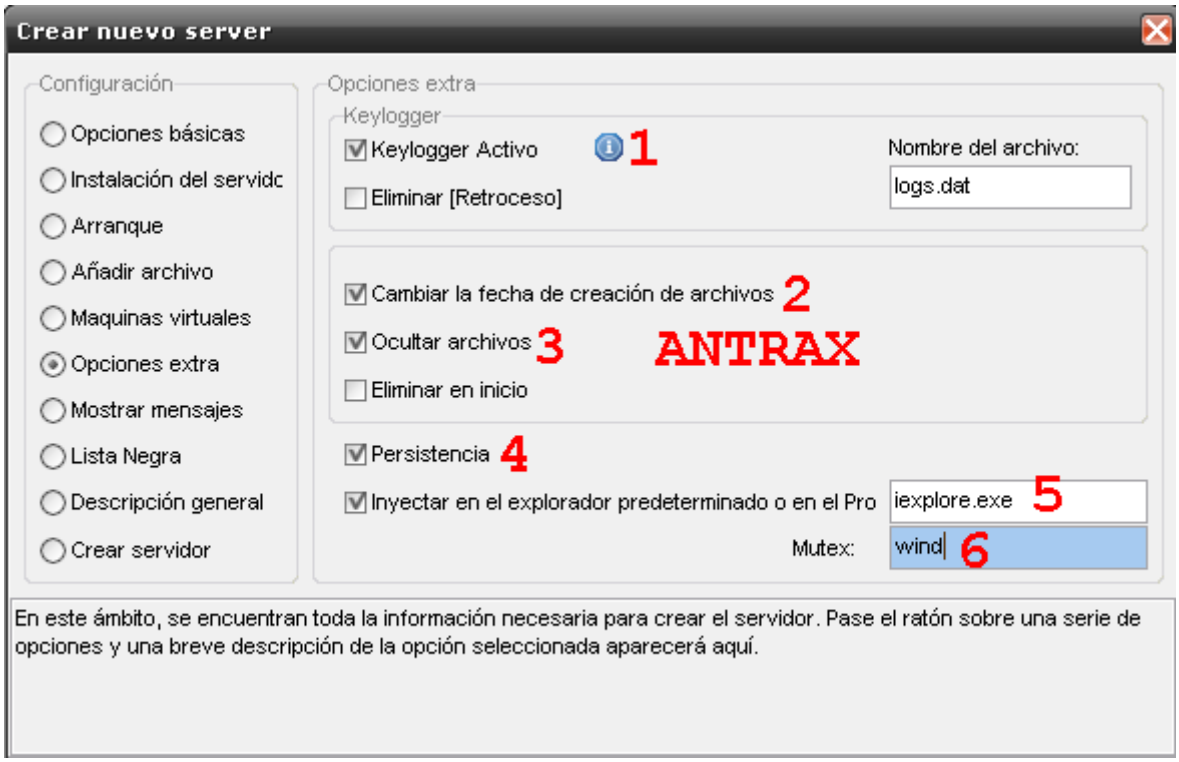
Pasamos a la siguiente

Aca es la información que le damos al server para que se guarde en el inicio de la pc. En otras palabras queda guardado en el registro para que el servidor arranque junto cuando se enciende la pc.

Ahora pasamos a la opción Maquinas Virtuales.



Aquí personalmente tildo todo, esto es para evitar ser descubiertos. En caso de que el server sea analizado, no puedan encontrarle nada malo.



1) Activamos el Keylogger

2) Cambiamos la fecha de los archivos para evitar ser descubiertos

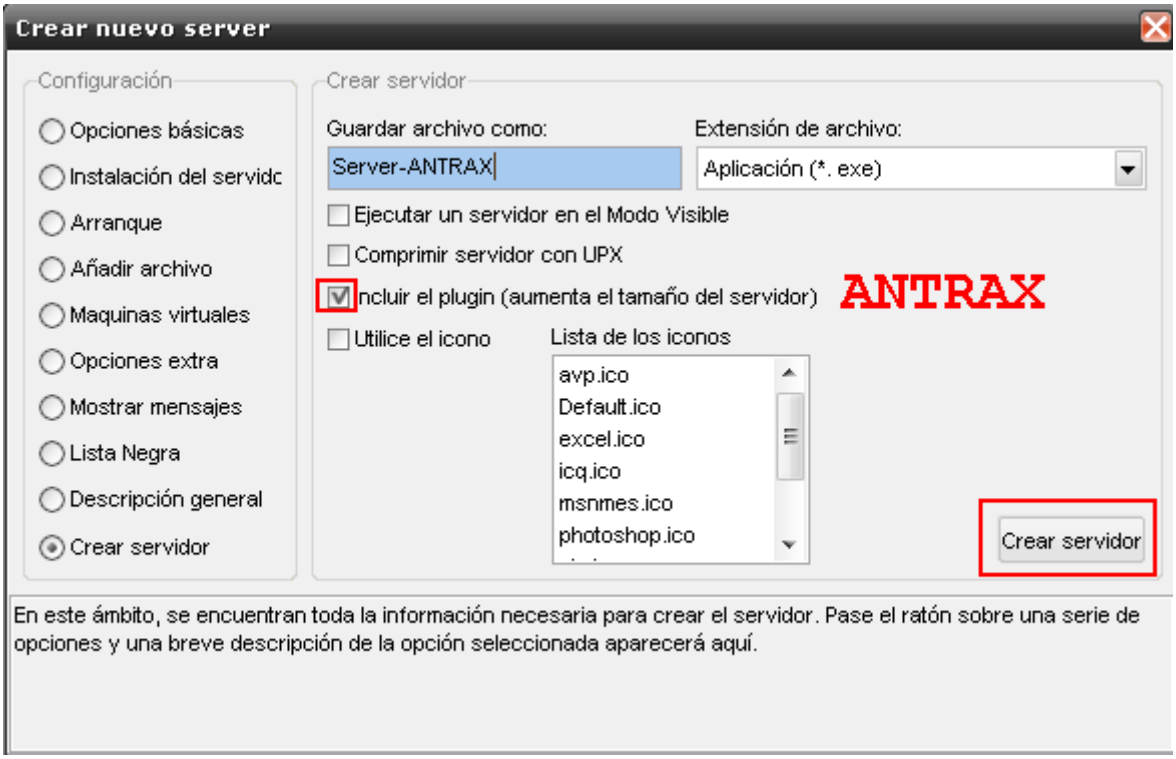
3) Ocultamos los archivos para evitar ser visualizados

4) Agregamos la persistencia para que no se pierda la conexión cuando reinicia la pc

5) Inyectamos el servidor en el proceso que deseen

6) Cambiamos el nombre del mutex por alguno que confunda

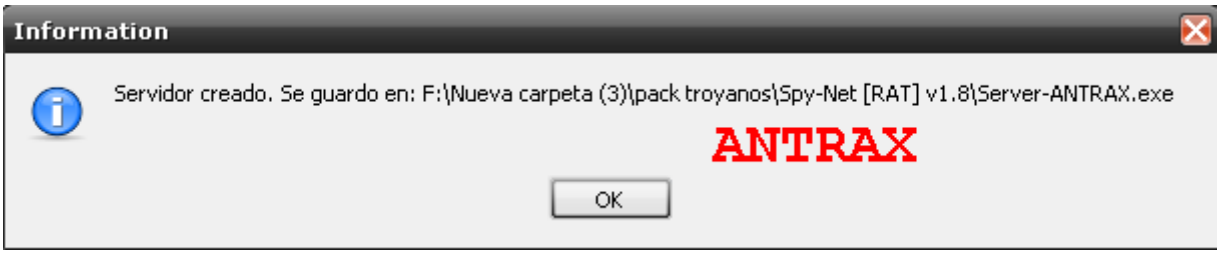
Por ultimo vamos a la ultima opción para crear el servidor



Tildamos la opción marcada en rojo. Si quieren también pueden modificarle el icono.

Damos click en crear servidor

Si muestra el siguiente cartel, salió todo bien

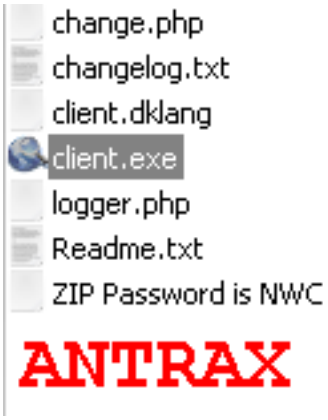


Sino les aparece, saquen el antivirus o desactívenlo, pero es recomendado desinstalarlo.

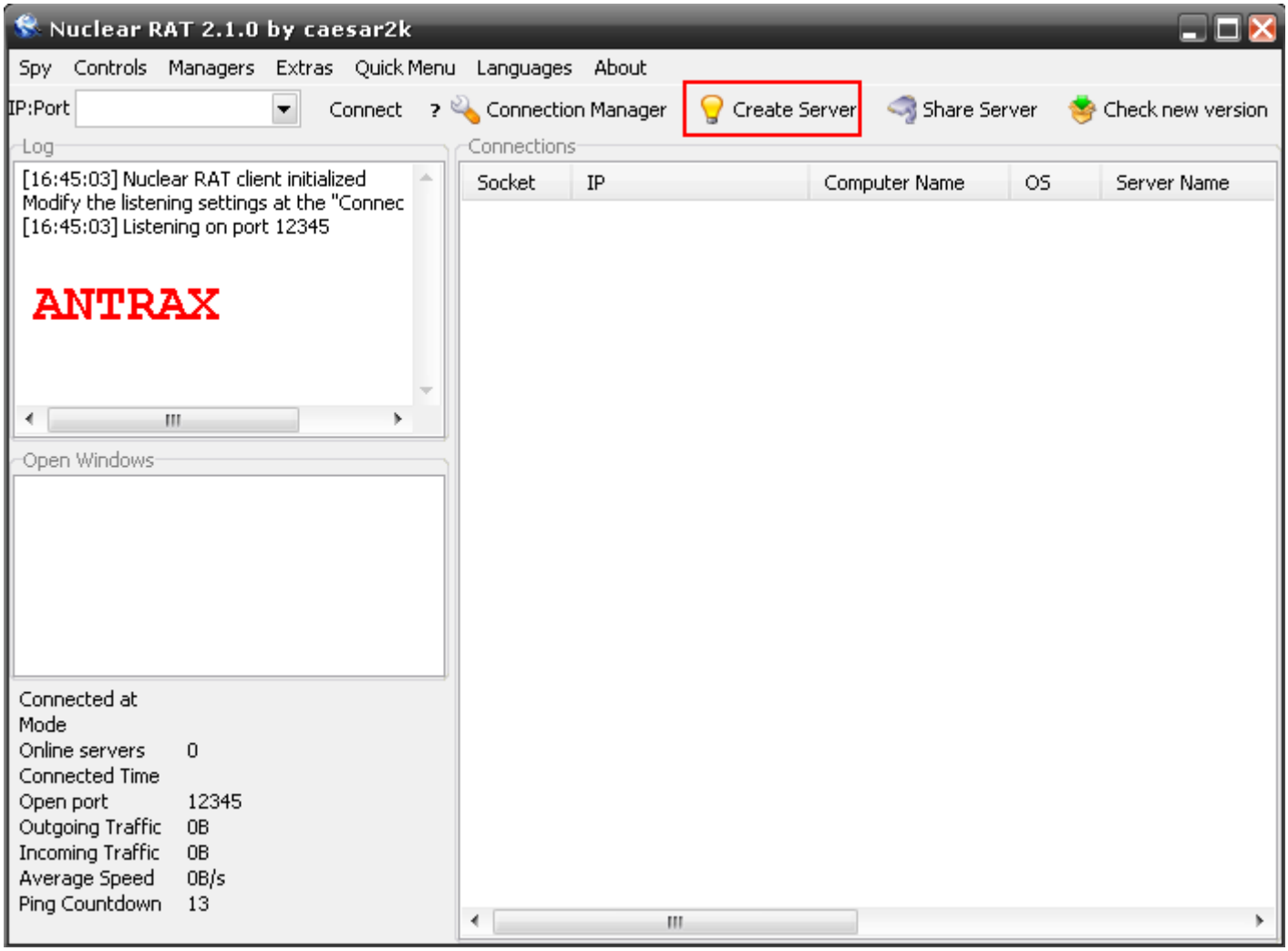
NUCLEAR RAT

Este es otro famosísimo troyano, tiene opción de explorar la Red LAN, es por eso que este viejo troyano se ha hecho famoso. Tambien es de conexión hibrida. Esto quiere decir que puede ser de conexión directa e inversa.

Les mostrare como se configura a continuación:



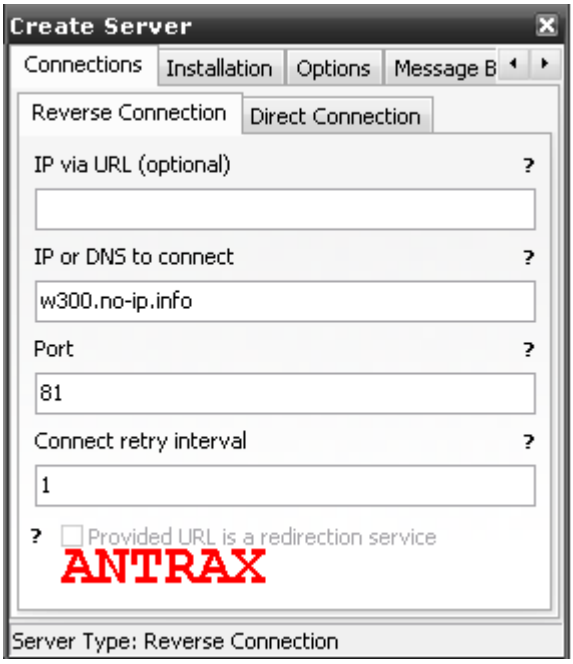
Abrimos el cliente, y tendremos algo como esto.



Así se ve el cliente

Aquí no se configura el cliente. Asique pasaremos a la configuración del server.

Vamos a la opción del foquito que dice: “Create Server”

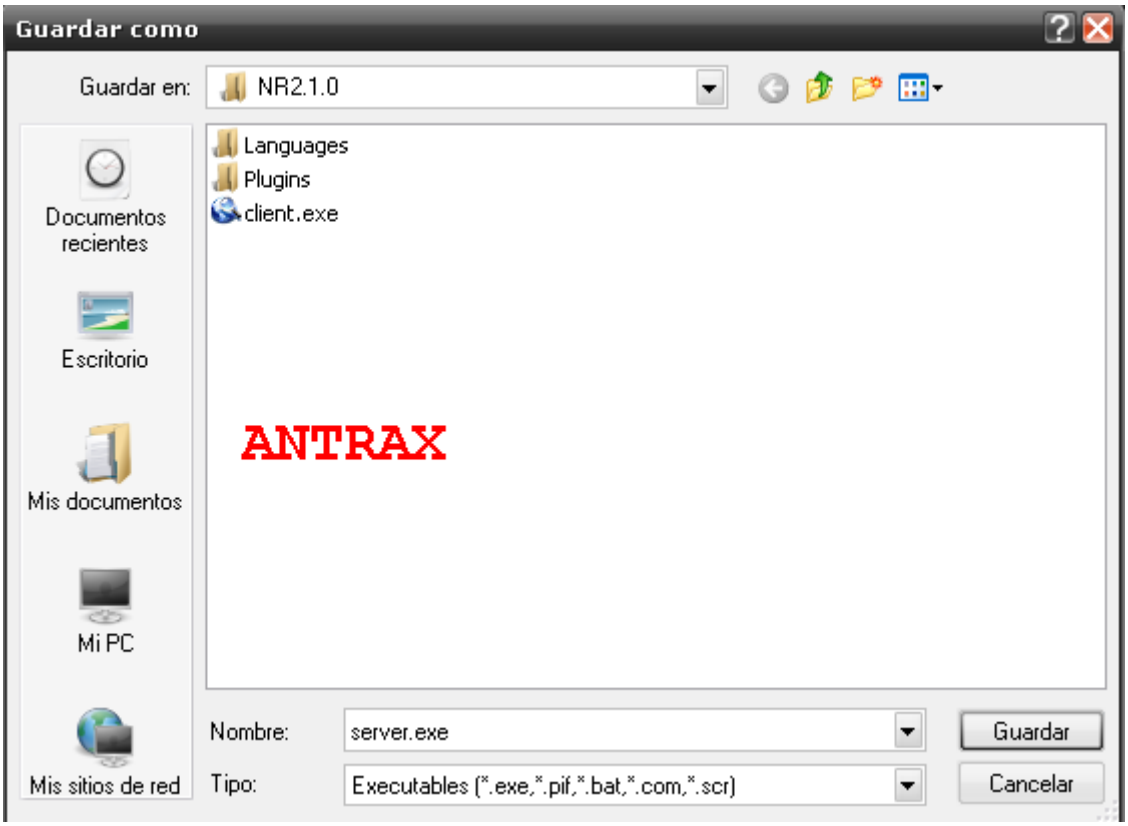


Aquí ponemos la no-ip de nosotros y el puerto que tengamos abierto.

El resto de las opciones son opcionales.

Aclaro que esto es para la configuración de conexión Inversa!

Luego presionamos las flechitas, hasta llegar a Build



Como muestra la imagen, escribimos el nombre del server, el que deseen y con la extensión *.exe, y le damos a guardar.

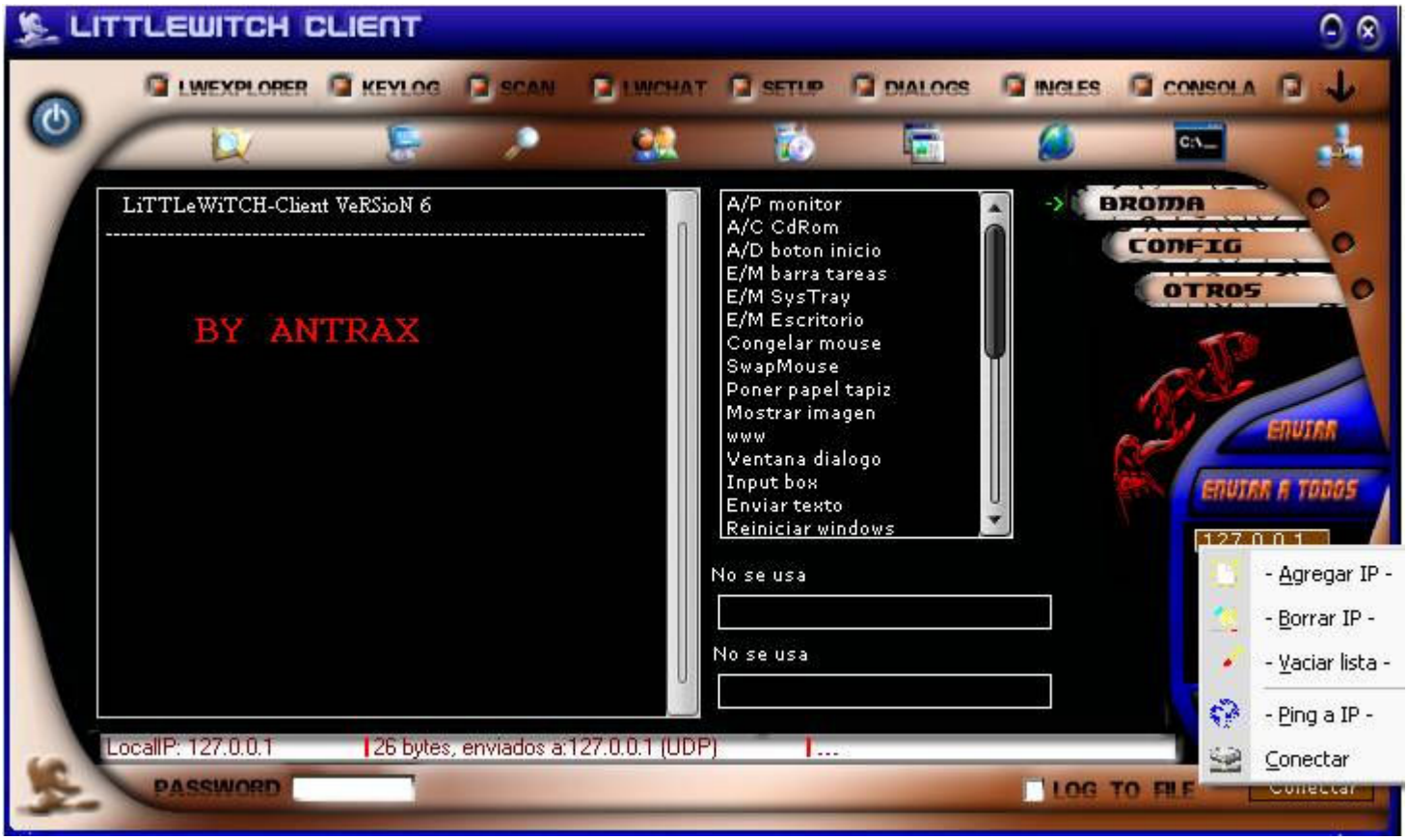
Y ya estaría listo el servidor para enviar.

LITTLE WITCH

Bueno, este es un troyano Argentino. Solo Funciona en redes LAN

Al abrir el cliente, nos encontraremos con lo siguiente:

Cargara la interfaz, y nos mostrara el cliente

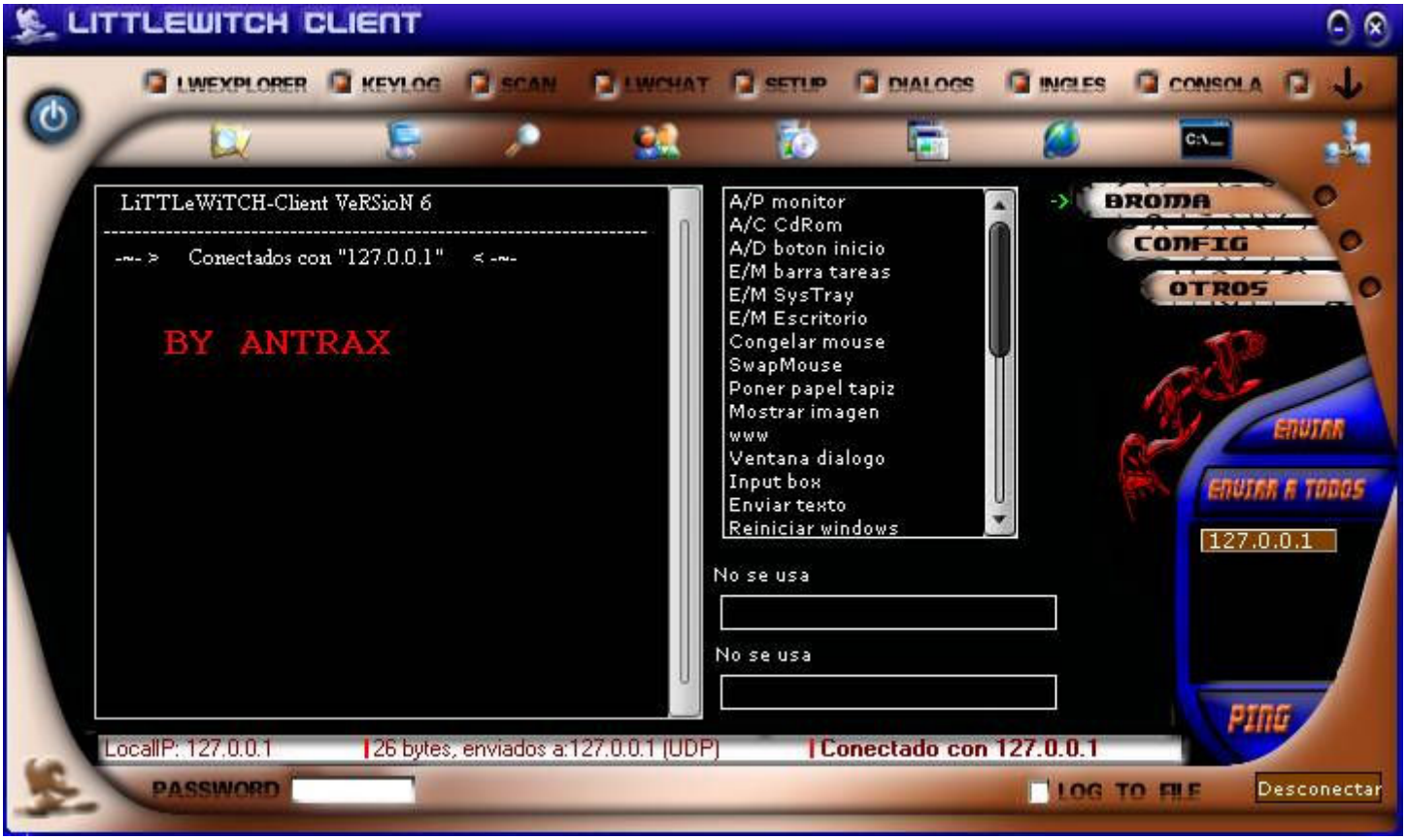


Este troyano es de conexión directa, asique debemos poner la IP de la PC a la cual infectamos.

En este caso puse 127.0.0.1 ya que infectare mi propia PC.

Una vez enviado el server, el cual viene con el cliente ya creado que se ve de la siguiente manera:

Una vez enviado el server y ejecutado, vamos nuevamente al cliente, y damos click en conectar, que se encuentra en la esquina inferior derecha.



Como verán, dice: Conectados con "127.0.0.1" Esto quiere decir que ya estamos conectados correctamente con la PC que infectamos.

Las opciones las tienen en el menú de arriba y a la derecha en donde dice: Broma, Config, Otros...

TURKOJAN

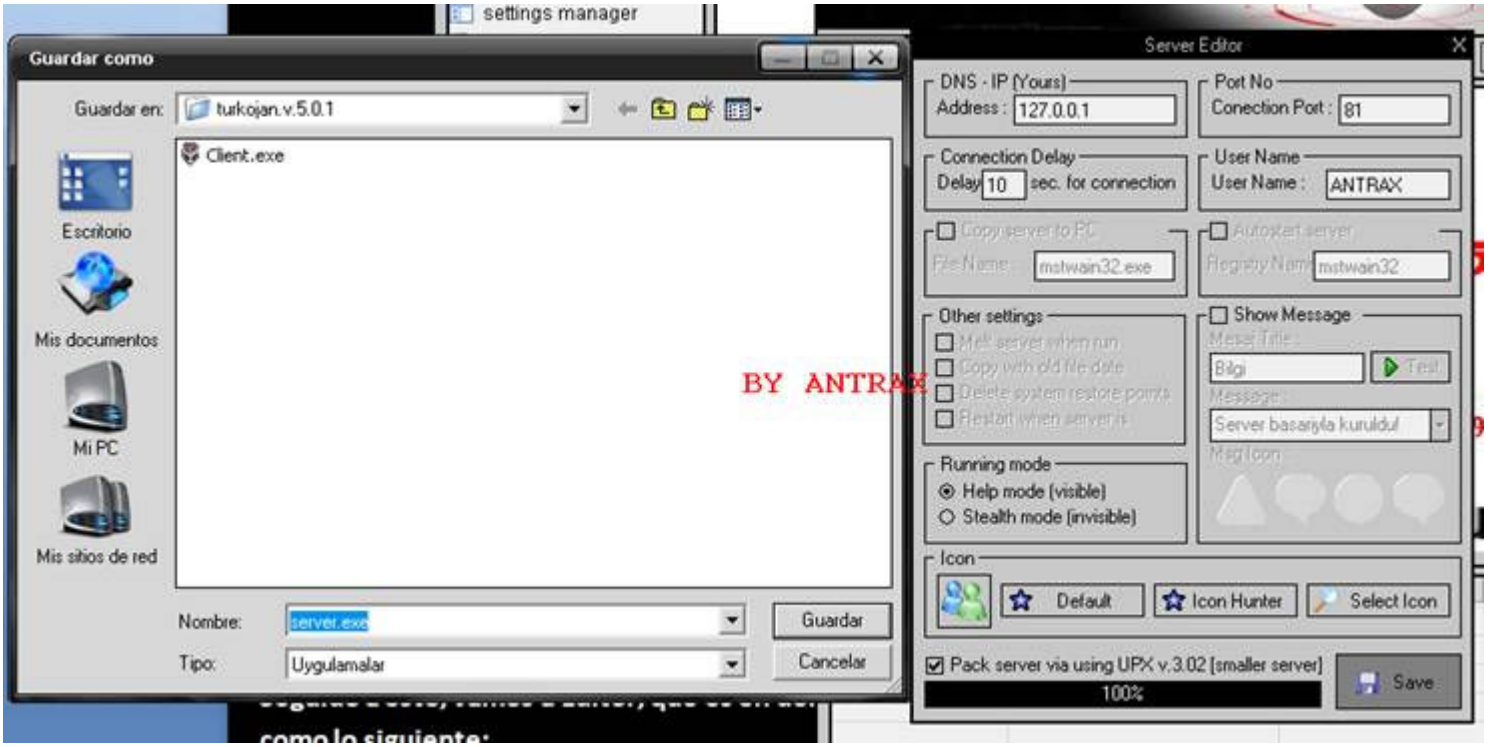
Bueno, este es un troyano muy conocido y muy viejo.

Aquí les traigo la versión 5 de este troyano, que fue editado desde el source por VozR.

Les dejo un pantallazo de cómo se ve:

Bueno, lo primero que haremos será ponerlo en ingles, por que sino no se entiende nada…

Seguido a esto, vamos a Editor, que es en donde se creara el server. Al hacerle click, veremos algo como lo siguiente:



Como pueden ver a la derecha, nos da para poner el DNS - IP, ahí es en donde ponemos la IP o la NO-IP, En Conection Port, el puerto que tengamos abieto. En User Name, ponemos el nombre con el que identificaremos a la victima. Y por ultimo pueden cambiar el icono si quieren para ocultar un poco el server. Luego de haber configurado todo eso, le damos a Save, y se abrirá una ventana para gurdar el server.

Una vez creado, si todo esta correcto, veremos un cartel asi:

Y tendremos el server Creado:

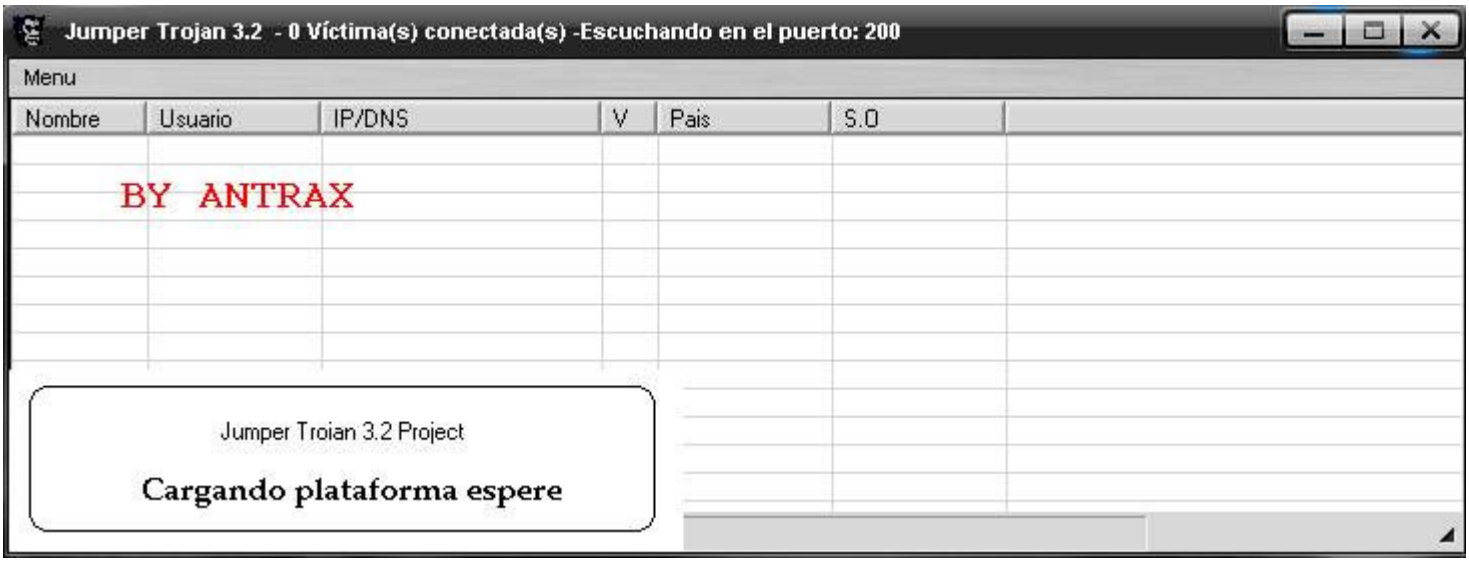
Al ejecutarlo, si todo es correcto, se conectara al cliente:

Las opciones las tienen en el panel de la izquierda.

BIOHAZARD - JUMPER

Es de interfaz sencilla, opciones básicas, es cryptable, estable y mas indetectable que el resto por haber sido privado y poco usado por la gente.

JUMPER 3.2



JUMPER 3.7


Jumper Trojan 3.7.0 - 0 Víctima(s) conectada(s) -Escuchando en el puerto: 1100
Herramientas
Welcome To Paradise
Control Remoto
Discos duros
Aplicaciones instaladas
Procesos
RemoteShell
Chat
Juegos
Espionaje
Teclado
Captura de pantalla
Contraseñas
Captura WebCam
Server
Información
Notas del servidor
Estatidisticas
Cerrar Server
Desinstalar Server
Optiones
Cambiar nombre
Estabilidad
jumper-Trojan 3.7
BY ANTRAX
Coded By Margera
Status:
Nombre
Usuario
IP/DNS
V
Pais
S.O
Tipo Cuenta

JUMPER 4

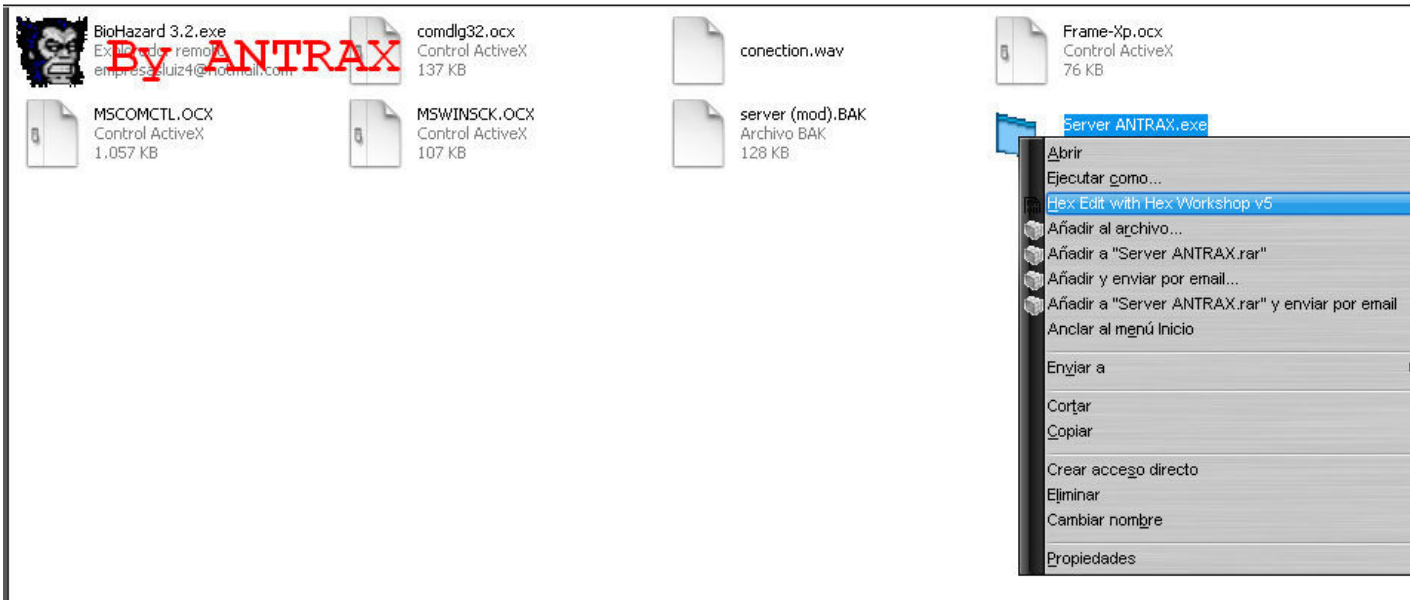

Jumper Remote Administration Tool Trojan 4.0 - CRACKED BY ANTRAX www.e-r00t.net
CODED By Margera
Nombre
Usuario
IP/DNS
V
Pais
S.O
Estatidisticas de conexion
Registrado c0m4dr3j4@hotmail.es / 2008
0 victimas conectadas

Bueno, este troyano fue privado hasta que lo hice publico por razones que no voy a decir.

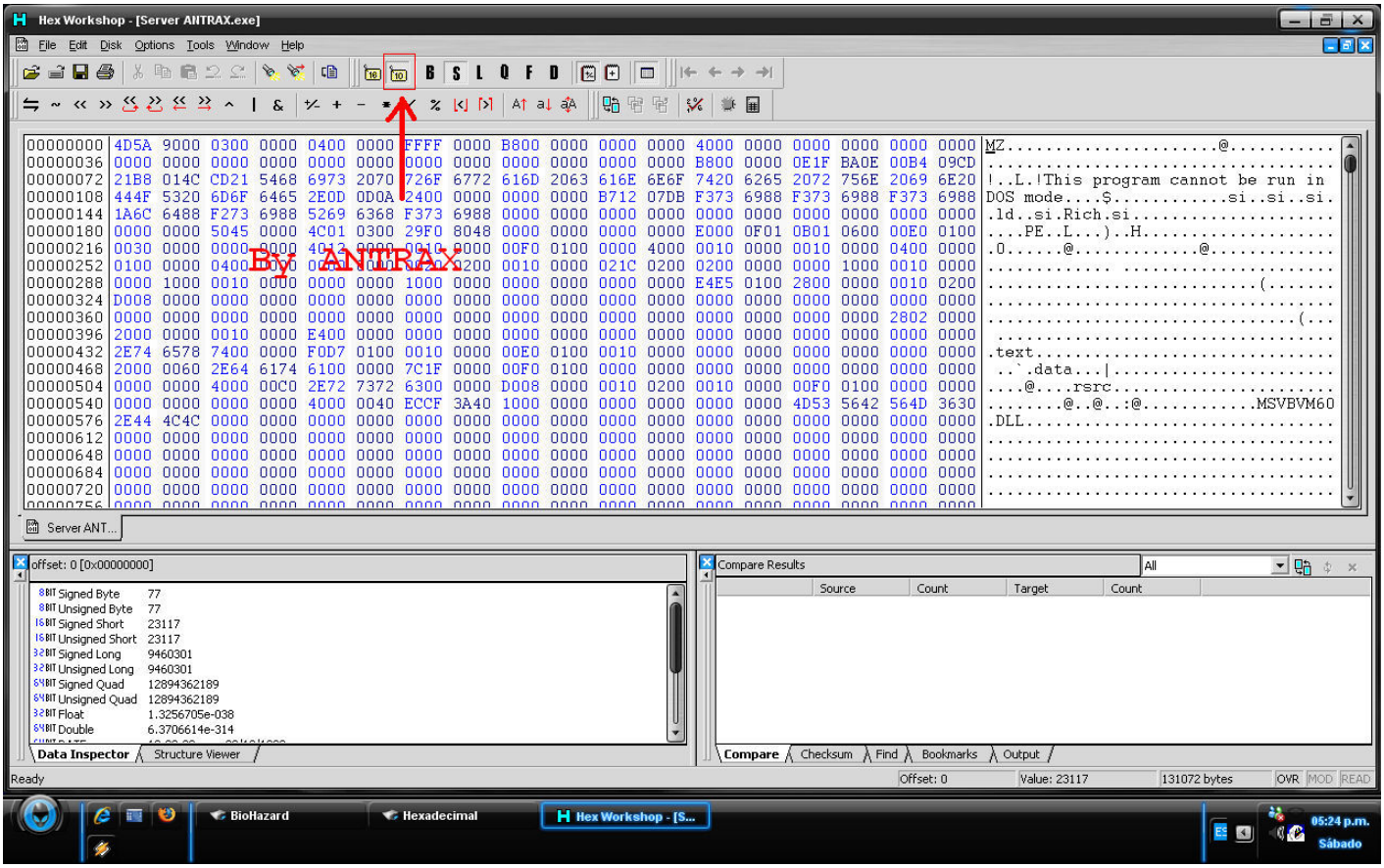
Para poder usar estos troyanos privados es necesario crackearlos o editarlos.

Para Crackearlo o Editarlo, necesitaremos un Editor Hexadecimal. Yo aconsejo utilizar el Hex WorkShop, que es el que utilizo siempre y el que utilizare en este tutorial.
Primero que nada abrimos la carpeta contenedora del server
Seleccionamos

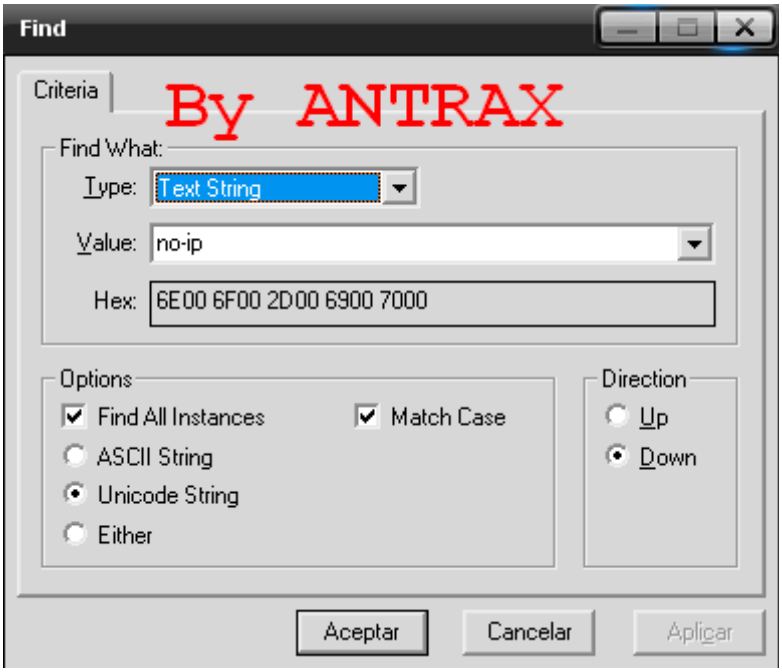
Seleccionamos con el otro botón al Server, en este caso es el Server ANTRAX.exe y presionamos en la opción "Hex Edit with Hex Workshop v5".



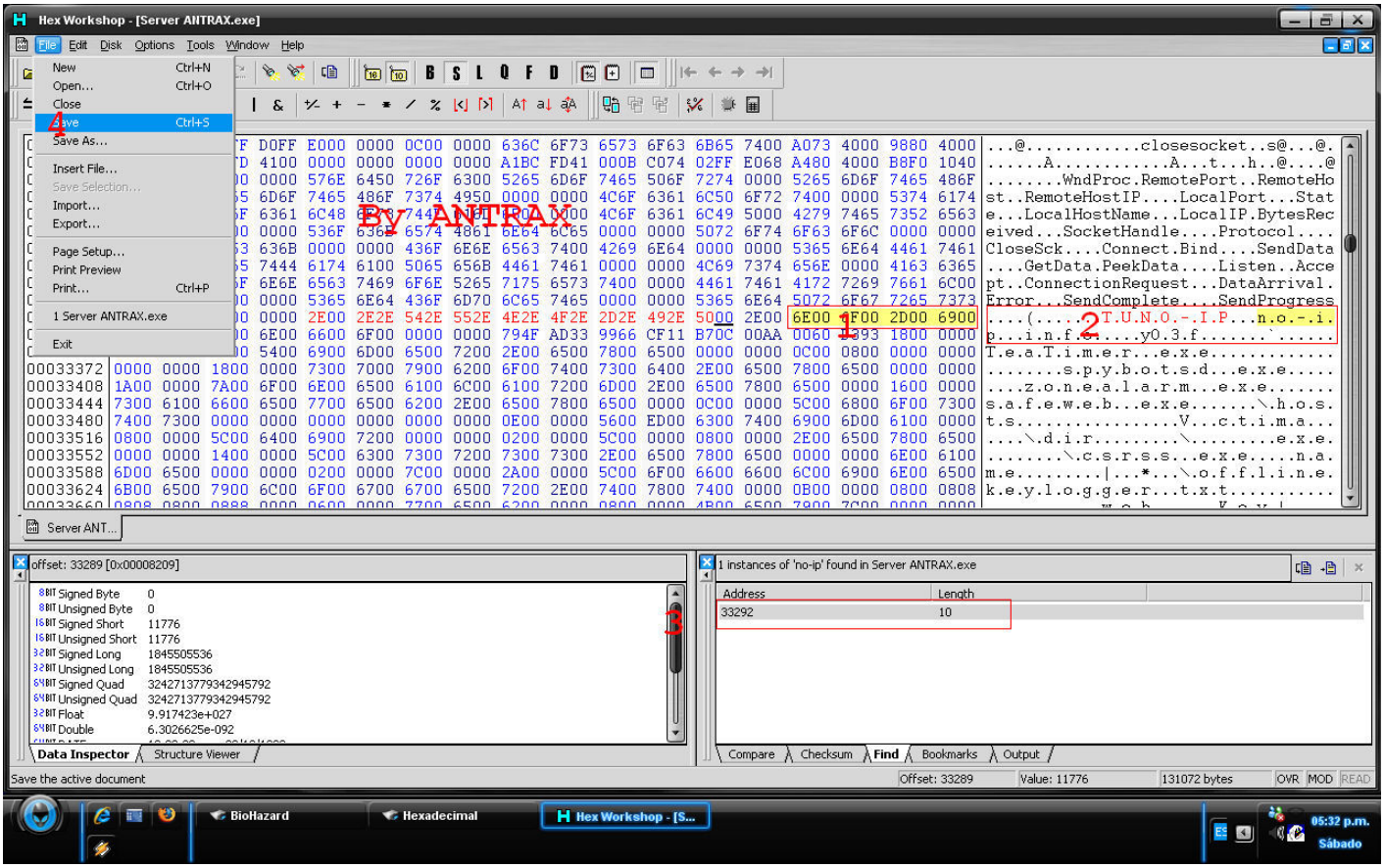
Una vez seleccionada, se abrirá el Editor Hexadecimal con todos los Offsets. La imagen se ve un poco pequeña, pero esta seleccionada la opción que tiene un 10 (decimal).



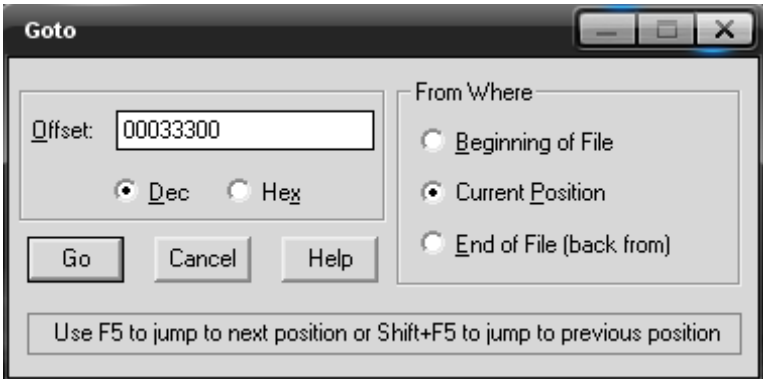
Seguido a esto presionamos “CTRL + F5” y nos aparecerá un cartel, que sirve para Buscar un Offset. En el cartel que aparecerá para la búsqueda. Y debemos seleccionar las opciones como muestra la imagen:



Una vez escrito esto y seleccionada las opciones correspondientes, presionamos Aceptar, y nos enviara al Offset que aparece la NO-IP.



En donde esta el 3, es en donde aparece el resultado de nuestra Busqueda.
Hacemos Click en el, y nos llevara al Offset.
En donde esta el 1, es en donde esta la búsqueda respectiva.
En donde esta el 2, es lo que tenemos que modificar.
Para modificarlo, como muestra la imagen, debe ir nuestra no-ip separada por puntos.
Por ejemplo: p.e.p.i.t.o...n.o.-.i.p...i.n.f.o
En donde están los tres puntos, quiere decir que el punto del medio es un punto que en verdad es. En este caso, la no-ip es: pepito.no-ip.info.
Seguido a esto, presionamos Archivo>Guardar como muestra el numero 4.
Esto es todo. Aunque en algunas ocaciones, cuando buscamos la no-ip no aparece… en estos casos hacemos lo siguiente.
Abrimos el server con el editor. Y en vez de presionar “CTRL + F”, presionamos “CTRL + G” esto es para buscar un Offset.

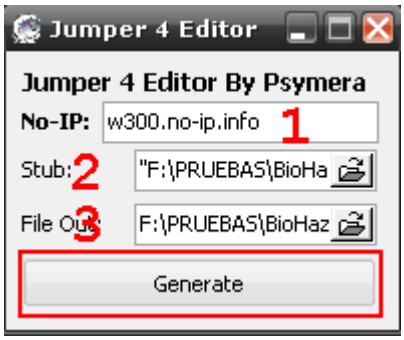


En Offset, escribimos “00033300” que es en donde se encuentra la no-ip que debemos cambiar. Y presionamos en GO.
Y esto nos llevara al Offset de la no-ip y por ultimo lo modificamos. Como enseñe mas arriba.

Con esto el servidor queda listo para que conecte con el cliente.

Tambien existe un editor de server para el jumper 4

Es muy fácil usarlo:



1 - Ponemos nuestra no-ip

2 - En Stub ponemos el server

3 - En File Out guardamos el server editado. Con la extensión *.exe

Y por ultimo en Generate

Con eso tendremos listo el server editado.
