Malware World Edición IV

BY ANTRAX

Contacto: antrax.labs@gmail.com

Introducción:

Hola a todos los seguidores de la MW, soy ANTRAX.

Hoy veremos como configurar un troyano a partir de los conocimientos adquiridos en ediciones anteriores.

Importante tener en cuenta los siguientes pasos antes de continuar:

1) Abrir el DUC del NO-IP (Programita)
2) Abrir al menos 3 puertos, los que ustedes deseen.
3) Elegir el troyano que ustedes quieran

Teniendo esas 3 cosas, ya se puede continuar a configurar el troyano.

Es importante saber que cosas desean hacer para darse cuenta que troyano utilizar. Esto se debe a que todos poseen distintas funciones.

Si desean simplemente probar como funciona un troyano, les recomiendo el Bifrost que es fácil de utilizar, si lo que quieren son funciones más sofisticadas o un troyano mas completo, les recomiendo el SpyNet (De la versión 2 en adelante).

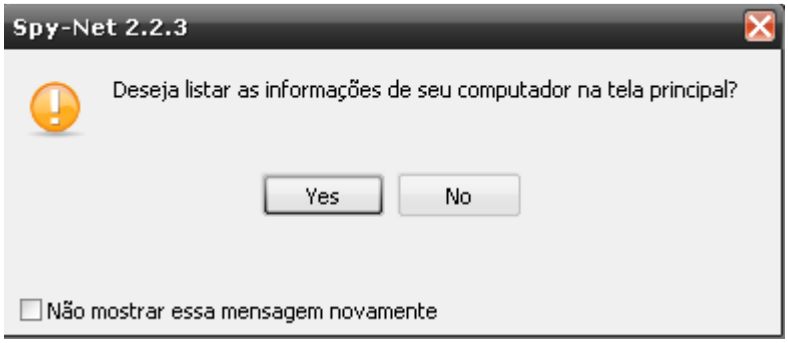
Sin nada mas que agregar, pasare a explicarles como configurar un troyano (casi todos se hacen de la misma forma). Para esta

explicación usare SpyNet que tiene muy buenas funciones como mencione antes.

Configuración de Idioma:

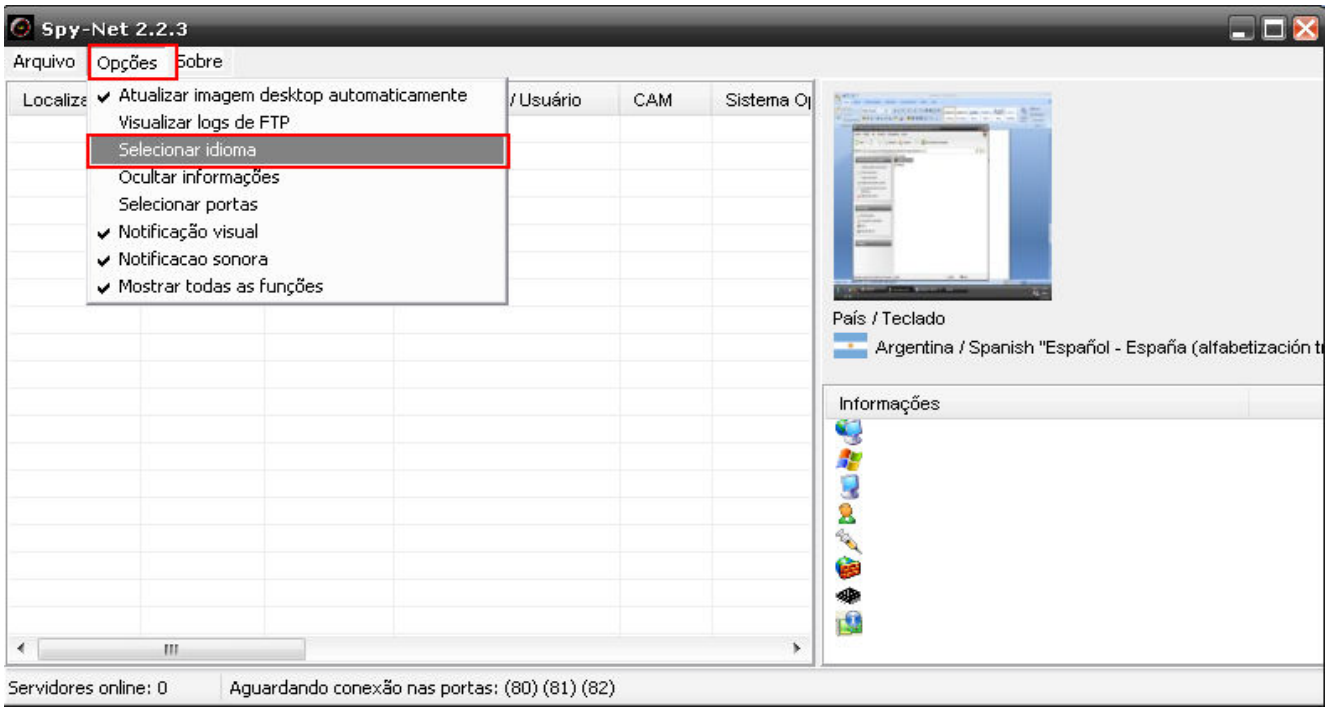
Para comenzar, el troyano viene por defecto en Portugués, para poderlo entender mejor, lo pasaremos a Español.

Ejecutamos el cliente y nos saltara el siguiente aviso:

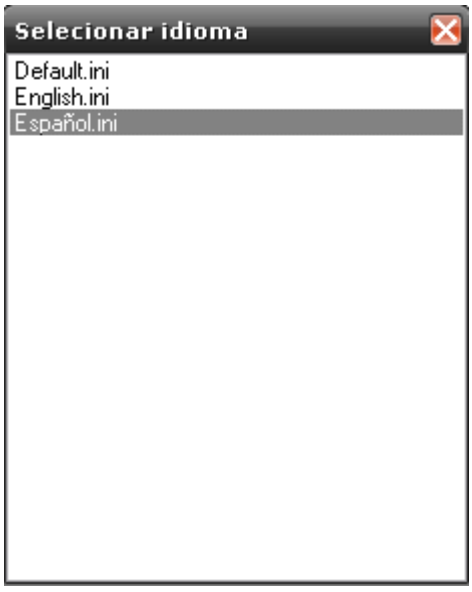


Quieres una lista de algunas informaciones sobre su equipo en la ventana principal?

Presionamos en si o en no, dependiendo lo que ustedes gusten, y veremos la pantalla principal:



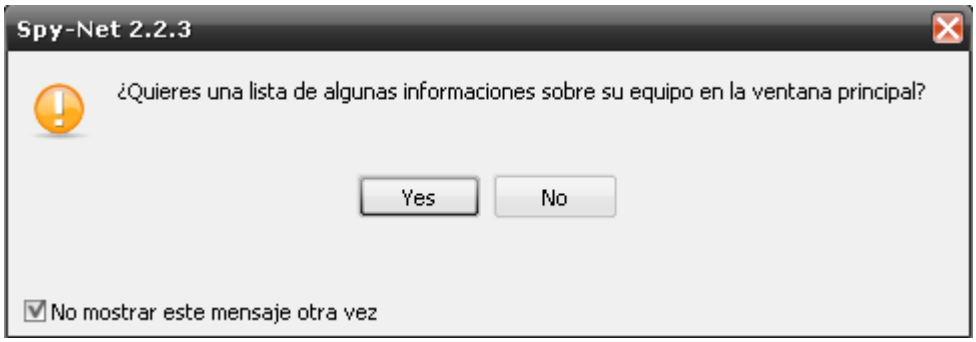
Vamos a Opções (Opciones) y luego a seleccionar idioma. Y veremos algo como esto:



Seleccionamos nuestro idioma preferente y le hacemos doble click.

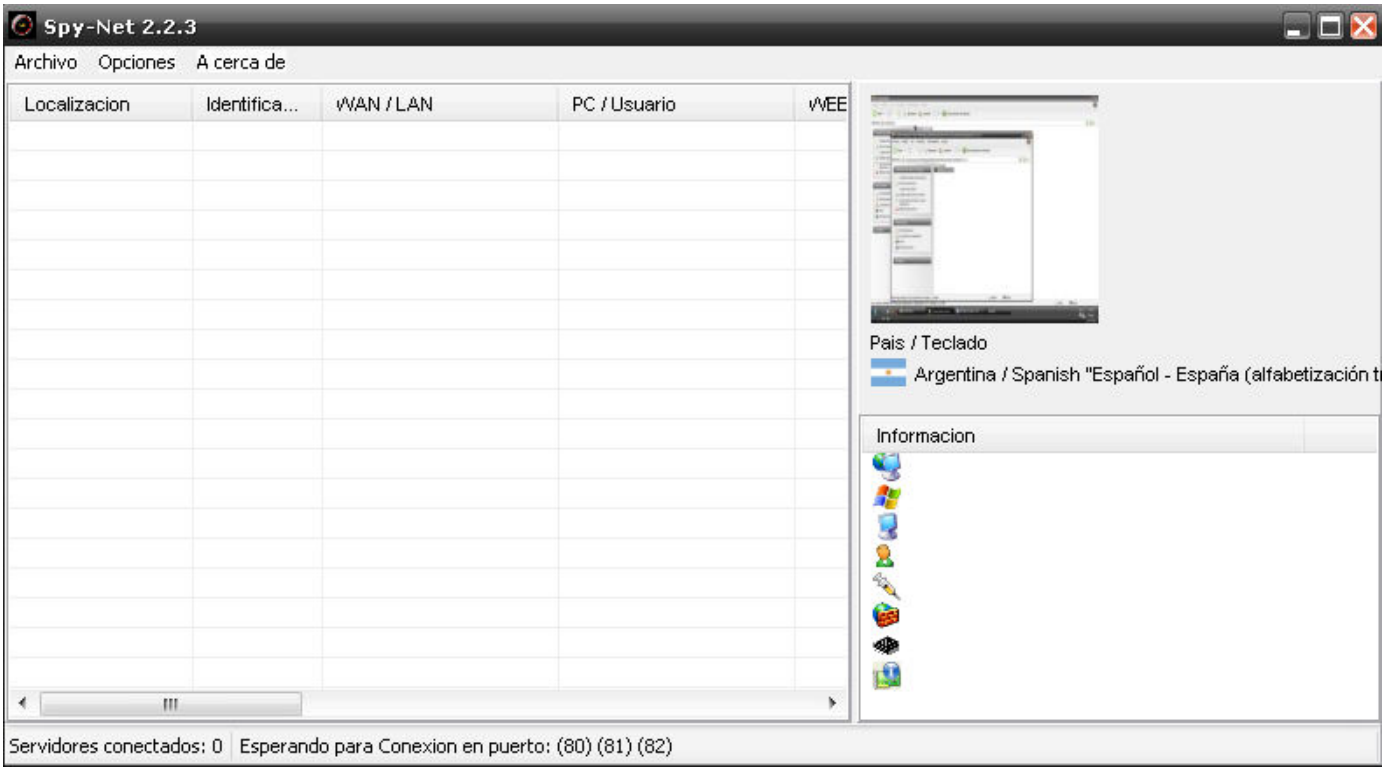
Automáticamente se pasara todo el troyano al Español.

Si lo cerramos y volvemos a abrir, veremos el cartel que apareció al comienzo:



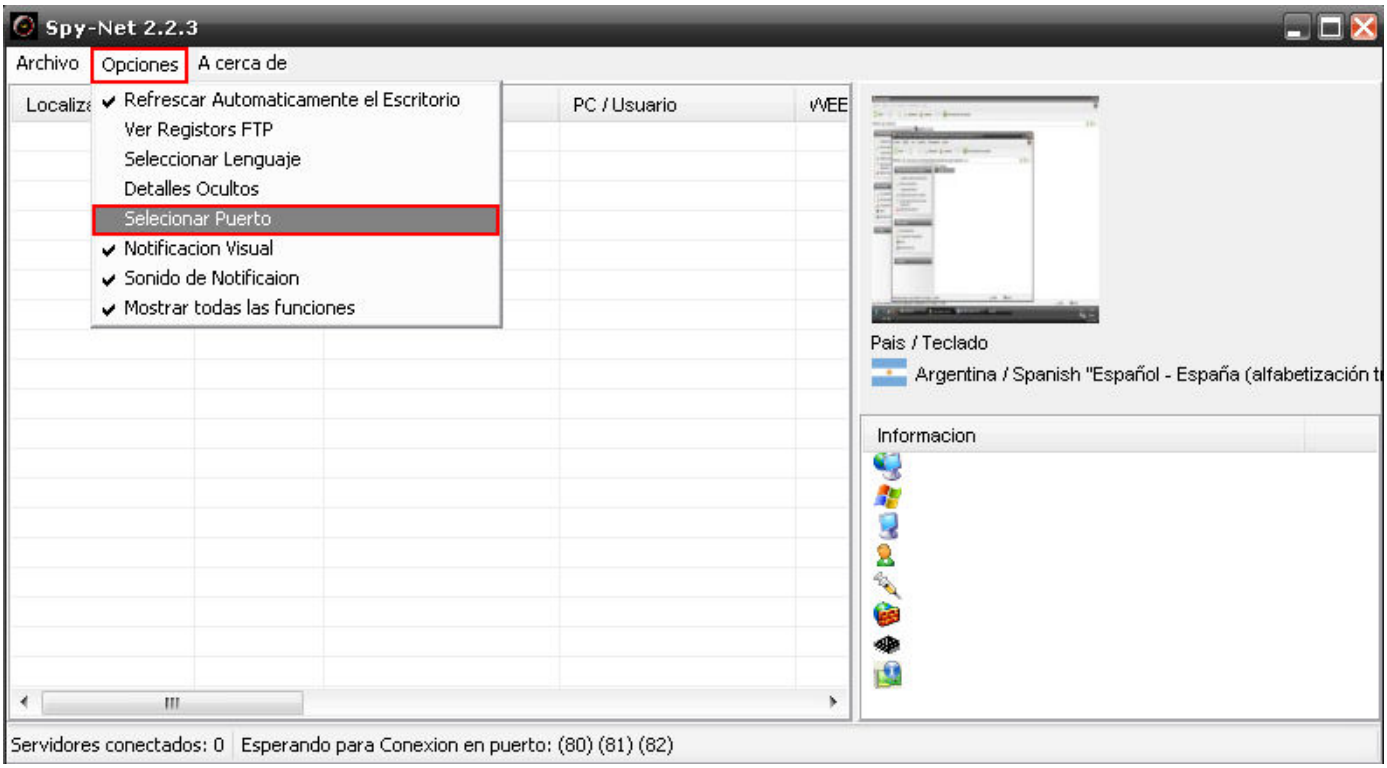
Tildamos la opción para que no muestre mas el mensaje, y damos click en Yes o en No para continuar con la configuración.

Configuración del cliente:

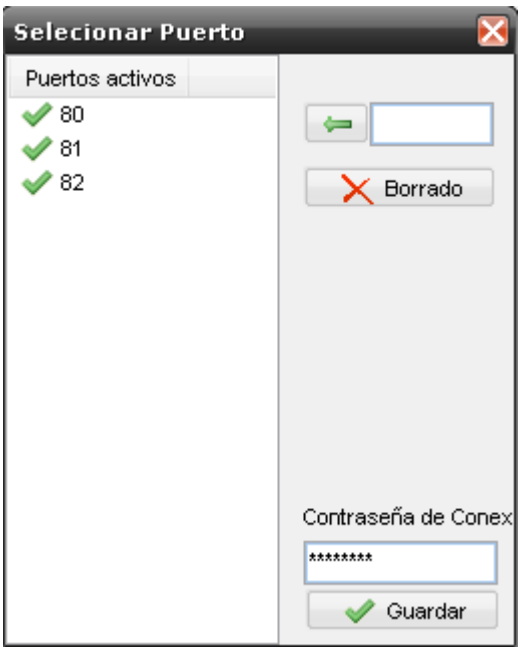


Lo primero que haremos, como en todo troyano, será configurar el puerto.

Para ello vamos a Opciones, y luego a Seleccionar Puerto.



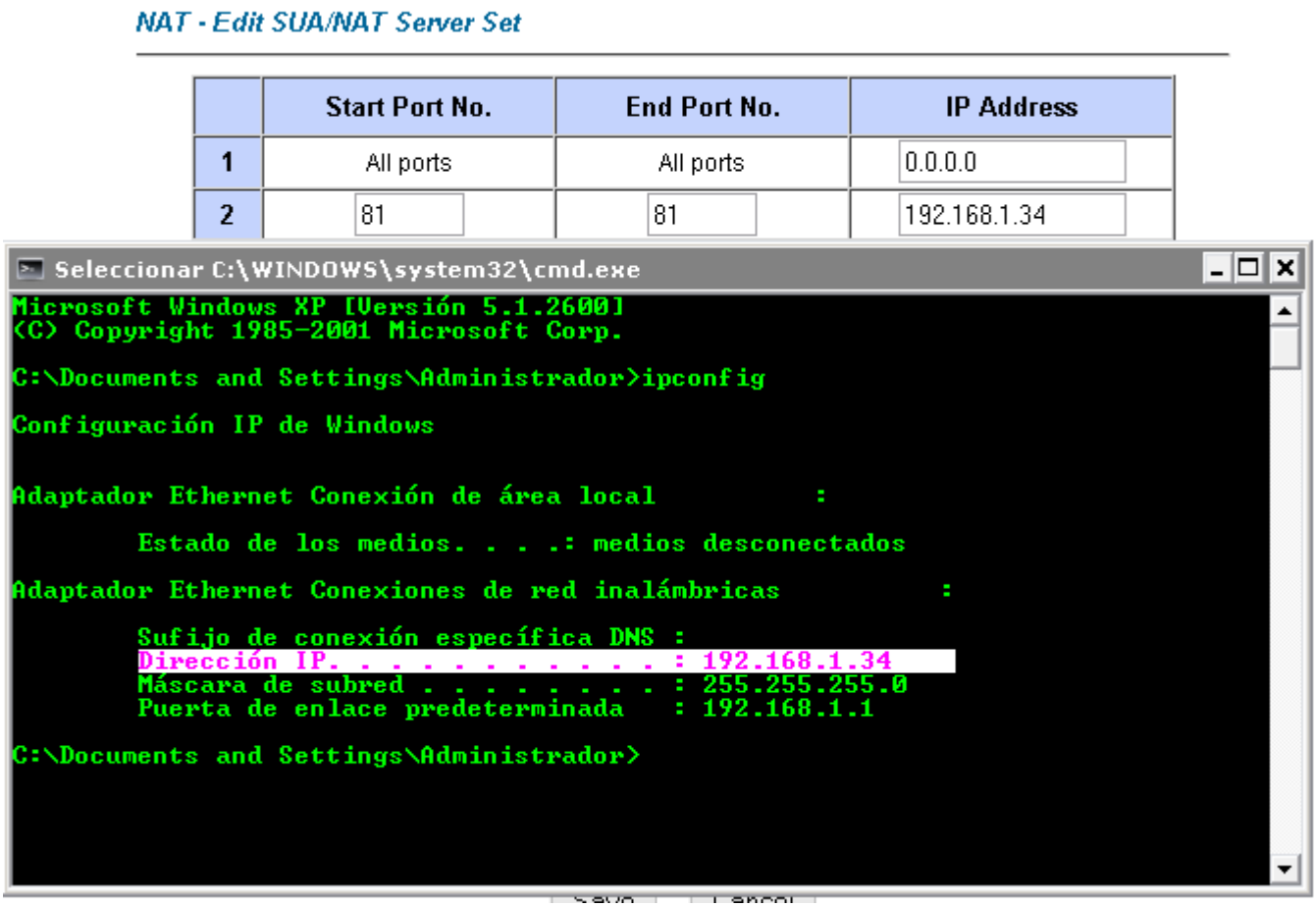
Nos aparecerá instantáneamente un pequeño cartel en donde deberemos configurar con el o los puertos que usaremos, y también una contraseña que nosotros elijamos para poder cifrar las conexiones y que no puedan robarnos las PCs infectadas.



En mi caso dejare los puertos que vienen por defecto ya que son los que yo tengo abiertos, y dejare la contraseña que viene por defecto ya que esto es solo una demostración.

Cada uno pondrá el puerto y la contraseña que mas guste y que les convenga a ustedes.

Recuerden que si utilizan router, el puerto debe estar abierto. Esto fue explicado en la tercera edición.



Demostración de la apertura de uno de los puertos

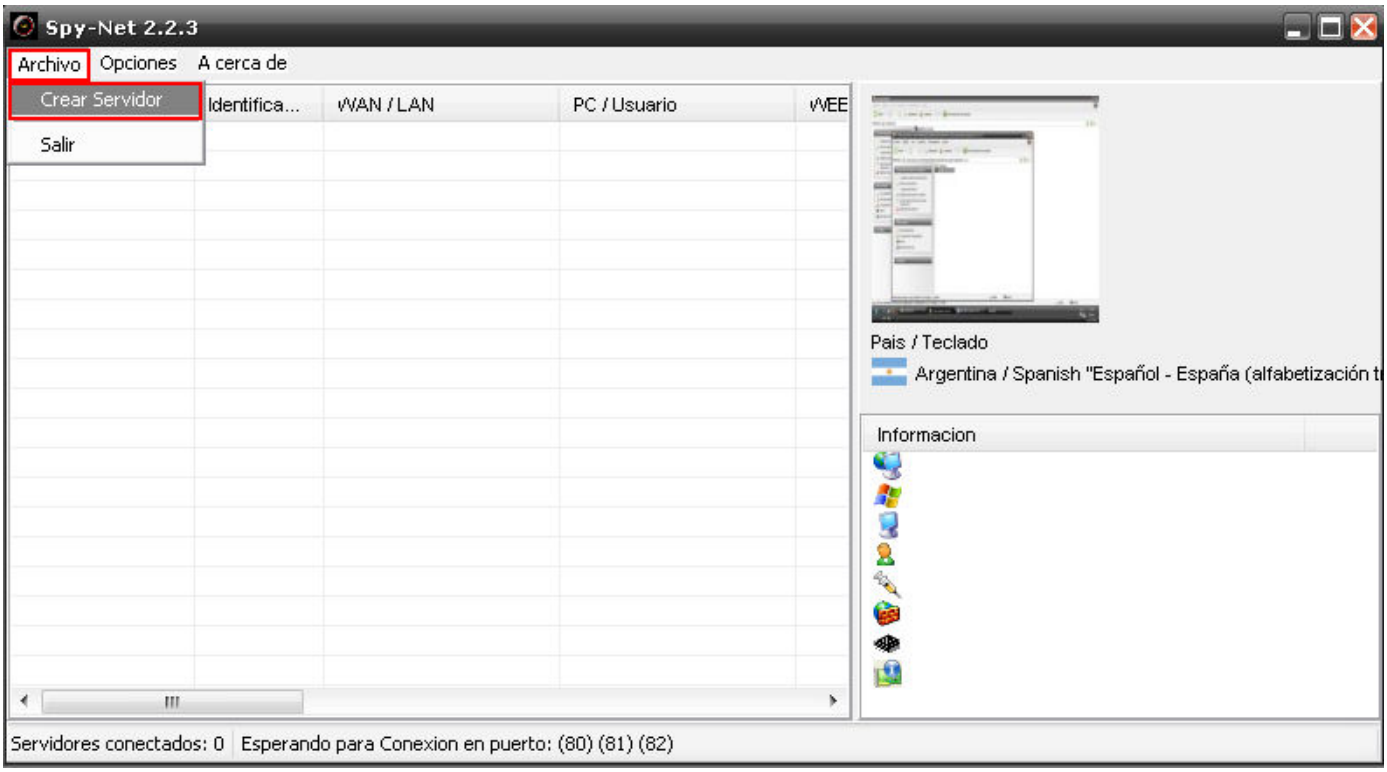
Para borrar un puerto de la lista, solo lo seleccionan, y dan click en Borrado, y el puerto desaparecerá.

En caso de que quieran añadir uno, escriben el número en la caja de texto y luego le dan a la flechita ← para que se añada a la lista.

Una vez hecho esto, damos click en guardar para proceder a la configuración del Servidor.

Configuración del servidor:

Para crear el servidor, nos situamos en la pantalla principal, y le damos a Archivo y luego a Crear Servidor.



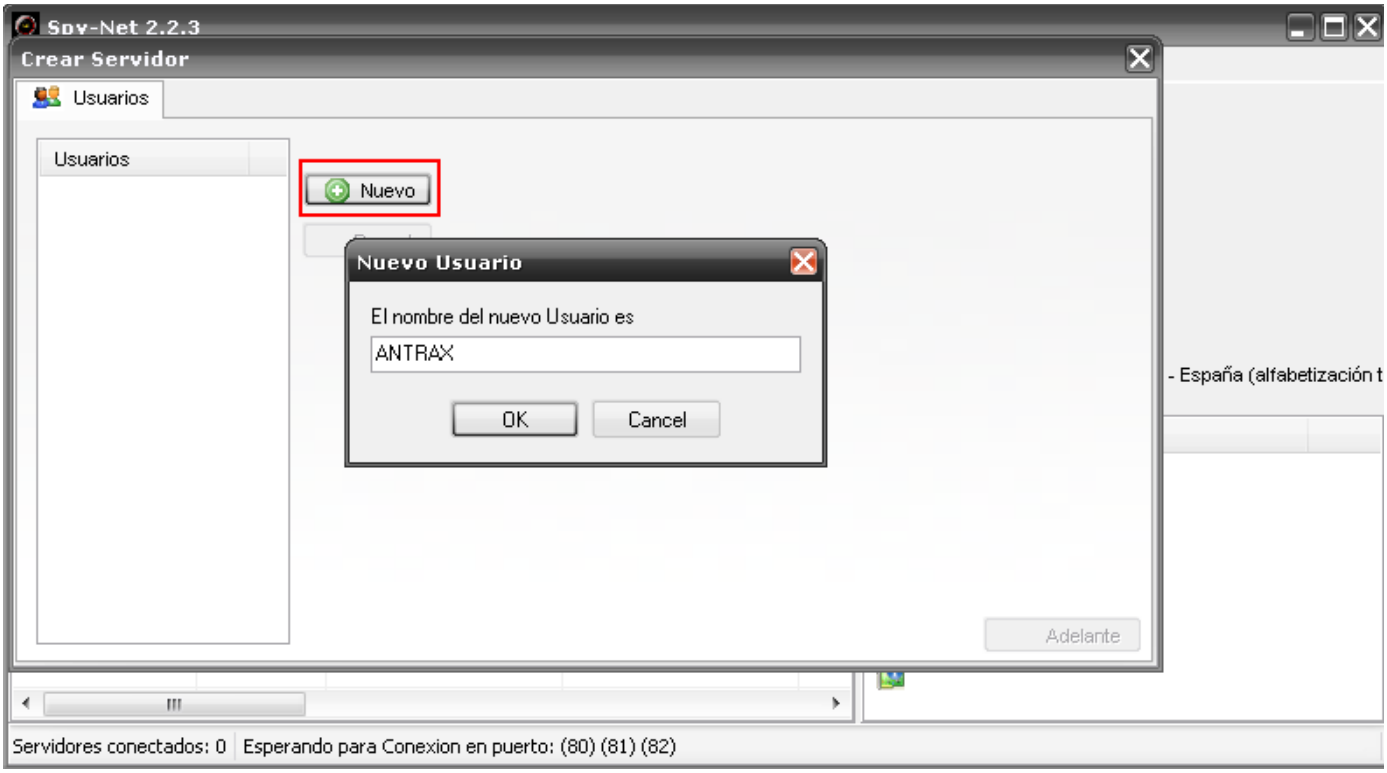
Tendremos a continuación una ventana nueva, en donde paso a paso iremos añadiendo opciones para configurar nuestro server.

Lo primero que nos aparecerá, será para crear un nuevo perfil de usuario.

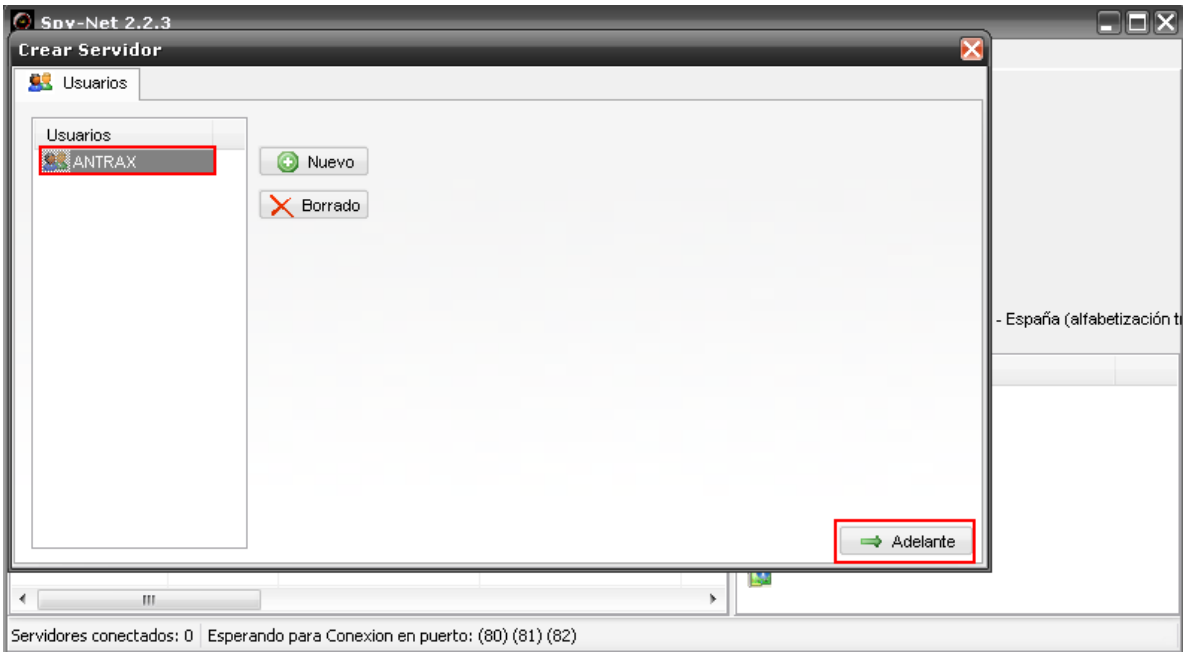
Esto se usa para poder tener varios tipos de configuraciones, y almacenarlas.

En caso de querer crear un servidor en un futuro, simplemente seleccionamos el usuario y la configuración se pondrá sola.

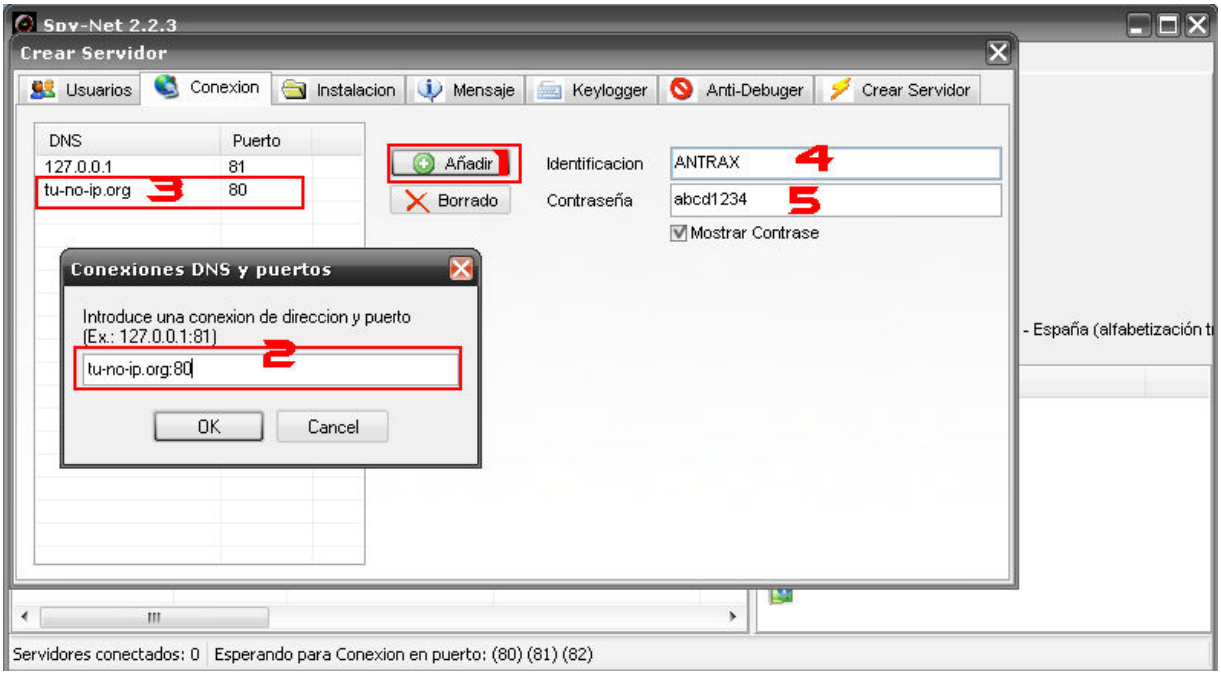
Damos Click en nuevo, y ponemos el nombre que deseamos. En mi caso pondre mi nick, ANTRAX.



Le damos a OK, y nuestro perfil creado quedara en la lista de usuarios.



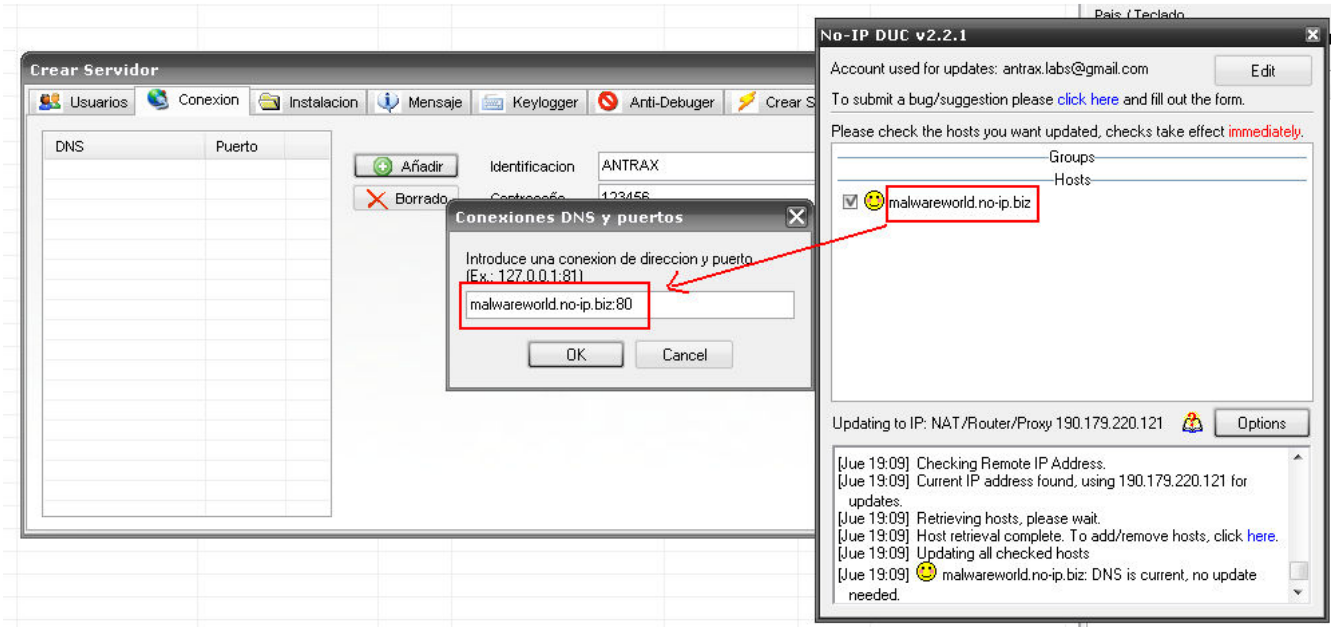
Seleccionamos nuestro perfil y damos click en Adelante para continuar.



1) Click en Añadir, para poner nuestra DNS (NO-IP).
2) Escribimos nuestra NO-IP y a continuación el puerto, les debe quedar de la siguiente manera:

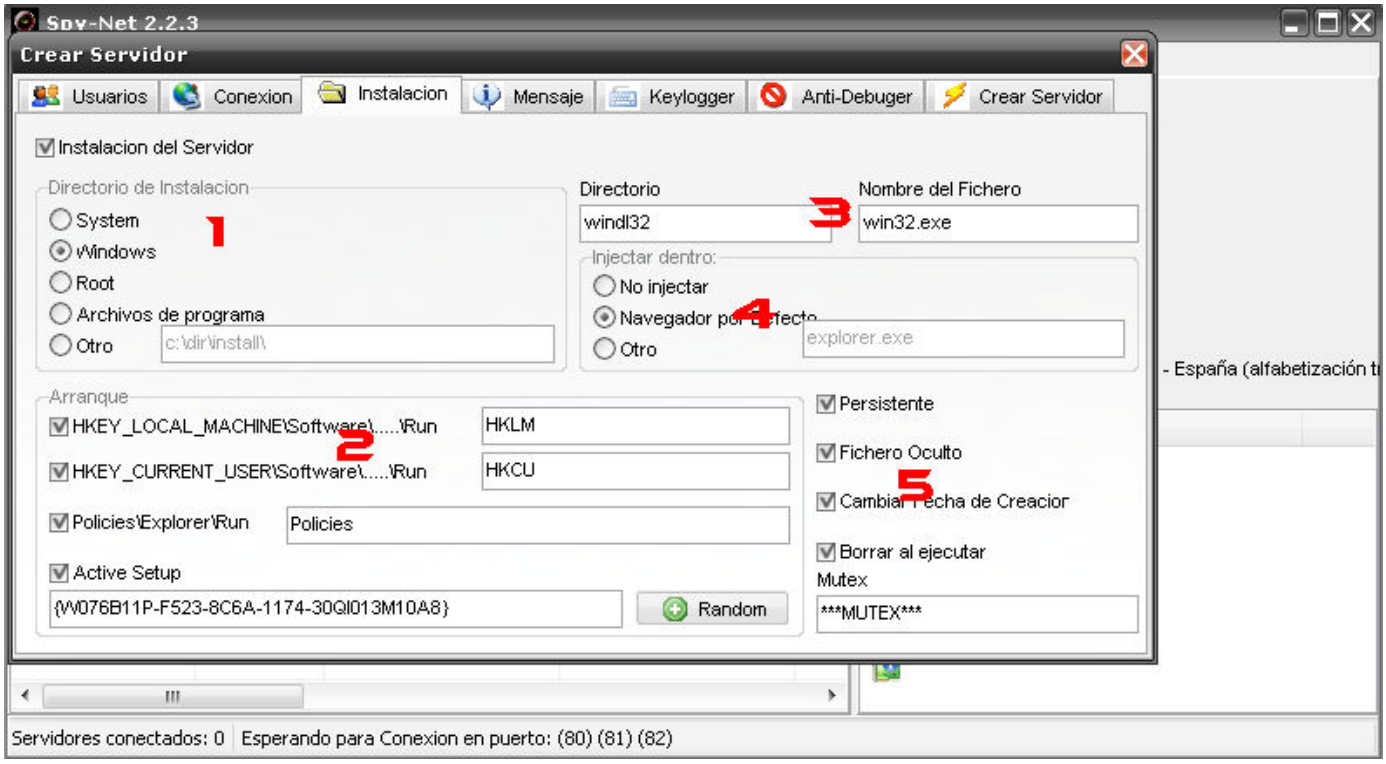
Malwareworld.no-ip.biz:80

Por supuesto que ese es un ejemplo, y que cada uno debe colocar la no-ip que creo y el puerto que decidió abrir.



3) Les debe quedar su DNS y Puerto en la lista.
4) Escriben el nombre de la persona a la que van a infectar en caso de que lo deseen, si quieren infectar de manera masiva les conviene dejar un mismo nombre para no tener que estar creando server por server.
5) Deben asegurarse de tener la misma contraseña que pusieron en el cliente

Una vez que tengamos esto, pasamos a la siguiente pestaña: Instalación

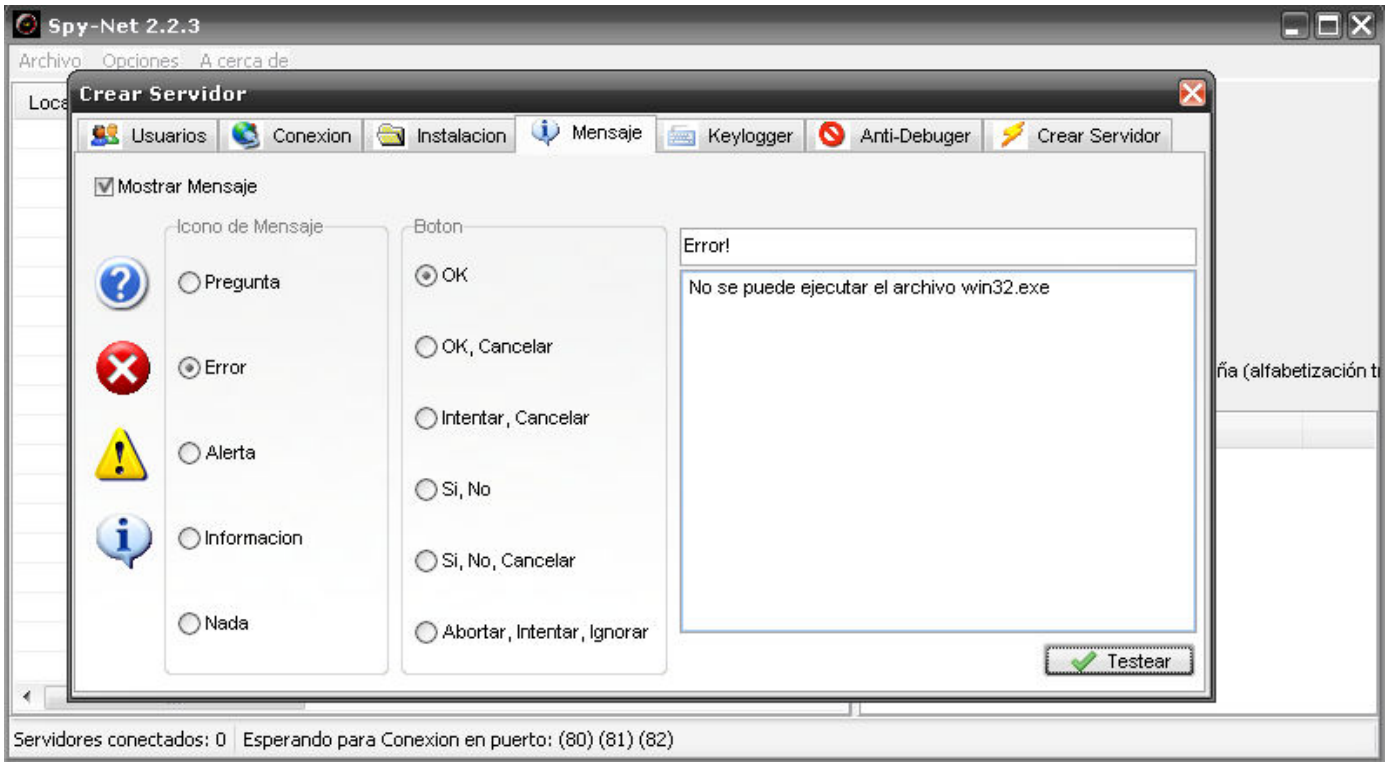


1) Seleccionamos el directorio en donde queramos que se instale, en este caso se instalara, en el directorio de Windows

2) Aquí configuraremos las opciones del arranque, esto es para que el servidor inicie cuando se enciende la maquina, ya que se añade al registro del sistema
3) Nombramos el directorio y el nombre del archivo por cual nosotros queramos, esto sirve para que nuestro remoto no se de cuenta en donde esta el troyano instalado.
4) Esta opción es para inyectar el proceso del troyano en uno que use nuestro remoto, o uno que nosotros escribamos, esto también sirve para evitar ser detectado
5) Por ultimo, seleccionamos las opciones para ocultar aun mas nuestro servidor y evitar ser descubiertos

Estas configuraciones se las conoce como rootkits ya que sirven para ocultar nuestro troyano en la pc que infectamos, y evitar ser borrado o identificado.

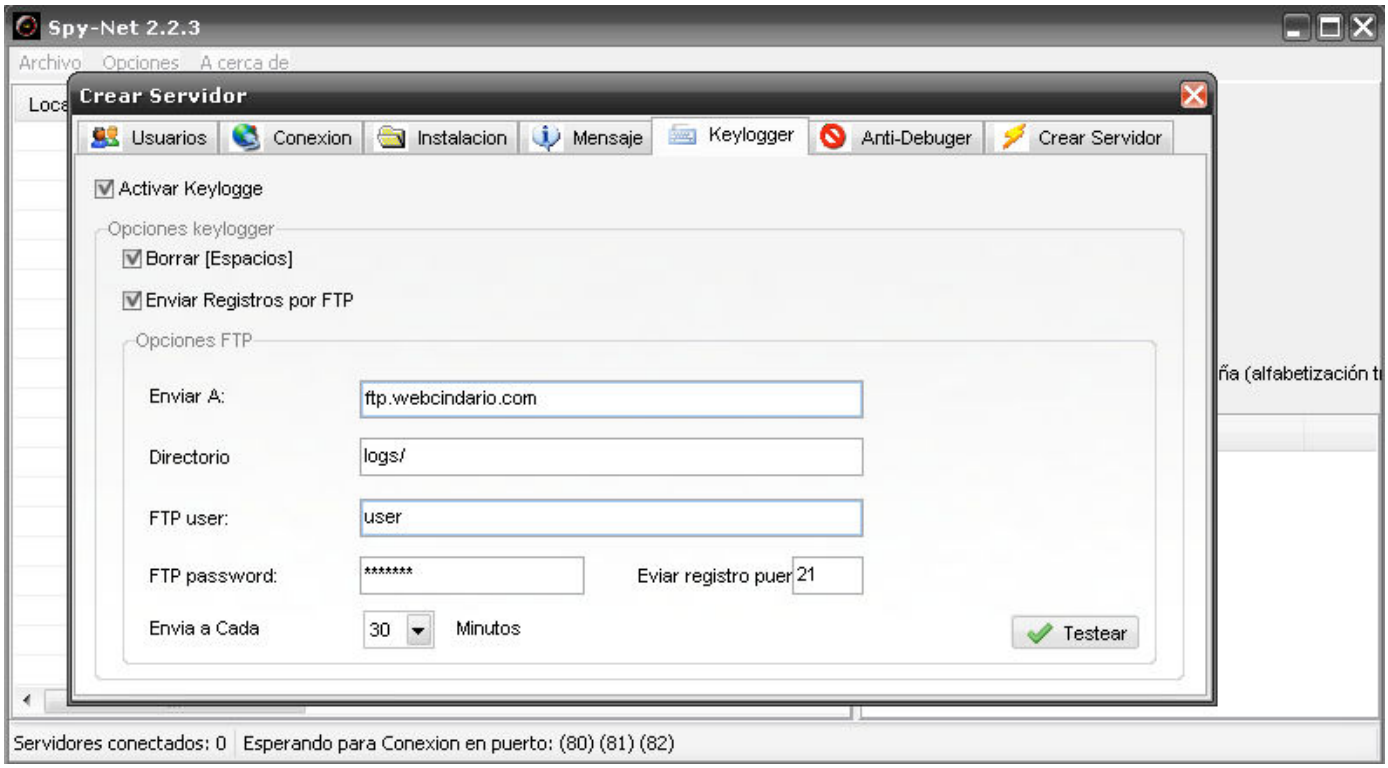
Pasamos a la siguiente pestaña: Mensaje



Esta opción no suelo usarla, pero acá les pongo un ejemplo para que vean como se utiliza.

Sirve para que cuando se ejecute el servidor, muestre un cartel o mensaje.

Pasamos a la siguiente pestaña: Keylogger



Como todos sabemos, el Keylogger sirve para capturar las pulsaciones de teclas que haga nuestro remoto.

La gran diferencia y ventaja de este troyano, es que nos da el gusto de enviarnos los logs de teclas por FTP (File Transfer Protocol) Protocolo de transferencia de Archivos.

Para los que no sepan, lo que es el FTP. Les recomiendo buscar en Google.

Pero explicándolo de manera poco formal, podemos decir que es un host (espacio virtual) en donde podemos almacenar cosas.

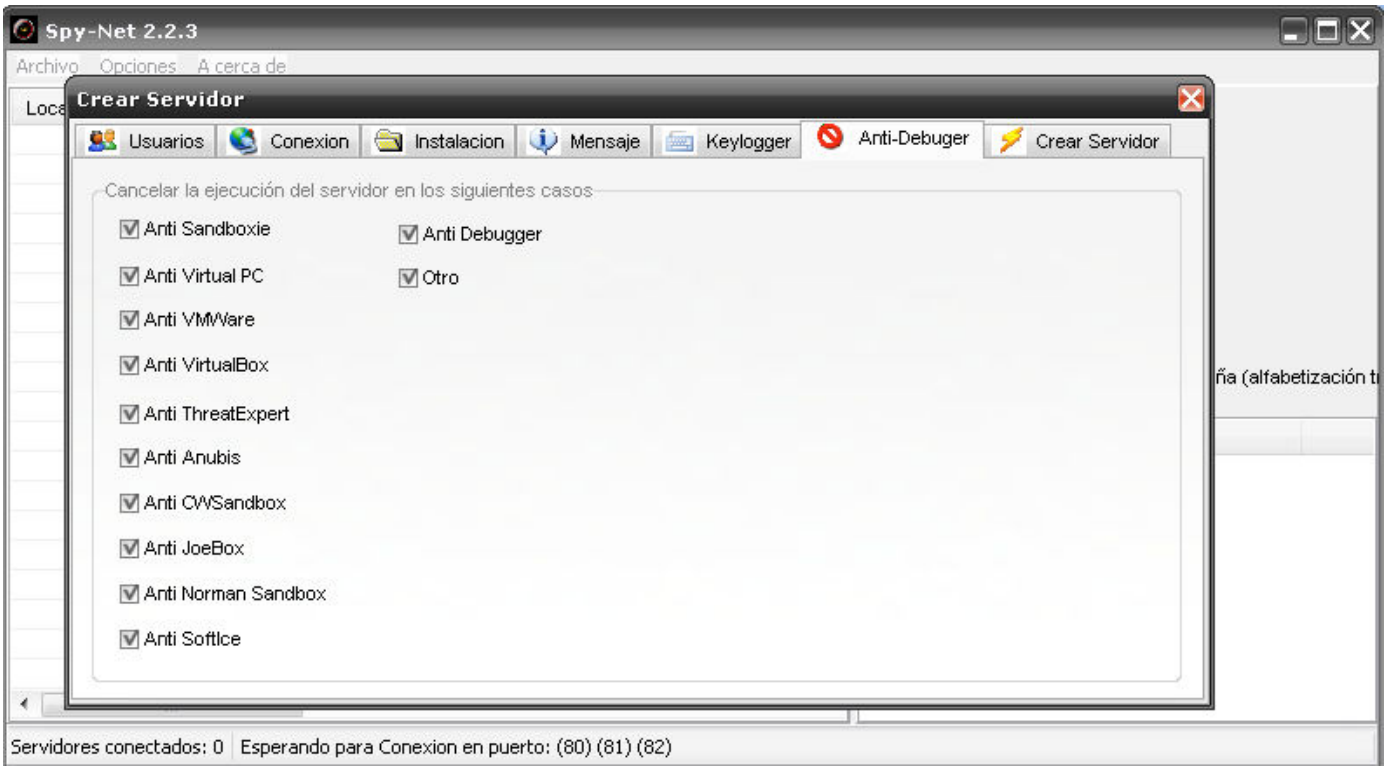
En este caso, almacenaremos los logs de nuestro remoto (las teclas pulsadas).

Lo veo super útil, ya que no es necesario estar las 24Hs vigilando a el infectado para ver en que momento pone alguna pass o dato importante,

ya que el mismo troyano se encargara de enviarnos todo por FTP a nuestro espacio.

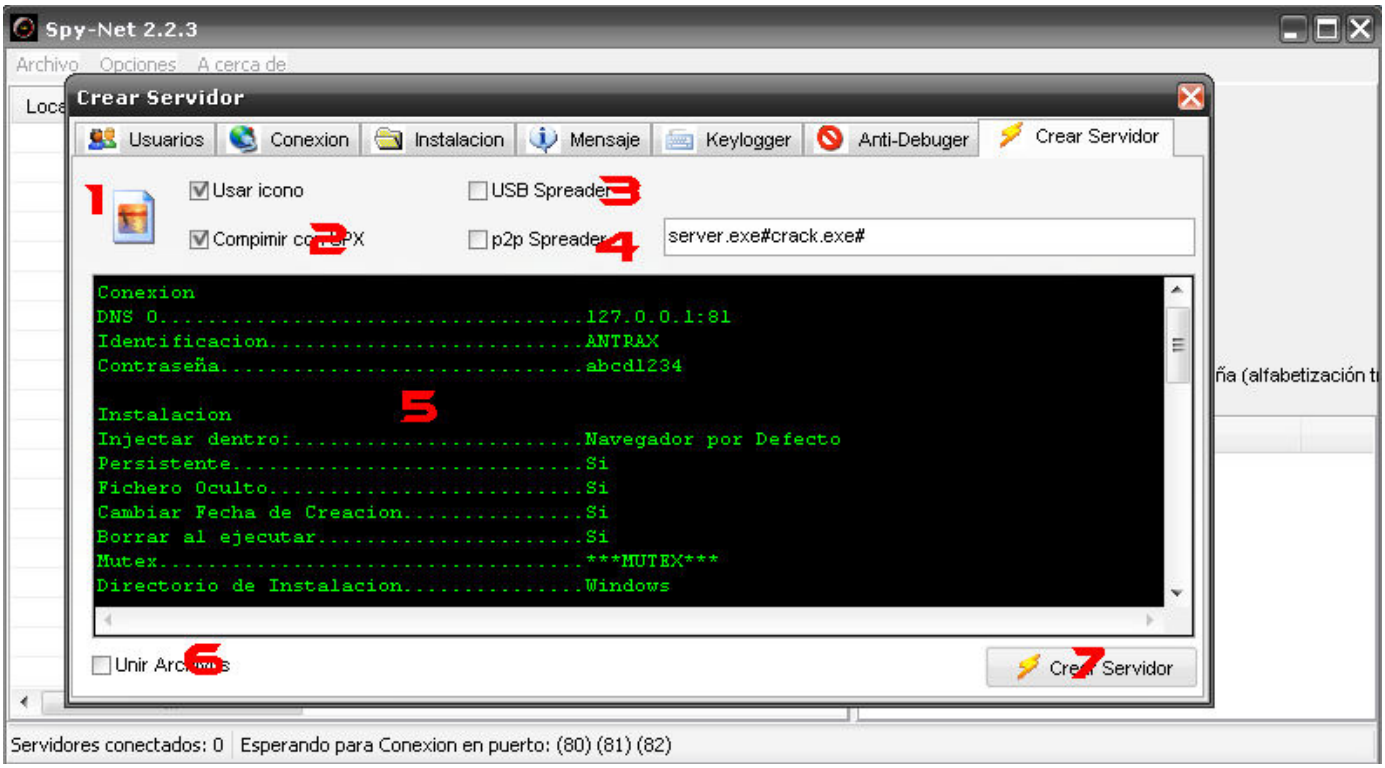
Para aquellos interesados en crear un FTP, les recomiendo webcindario, que jamás he tenido problemas.

Pasamos a la siguiente pestaña: Anti-Debuger



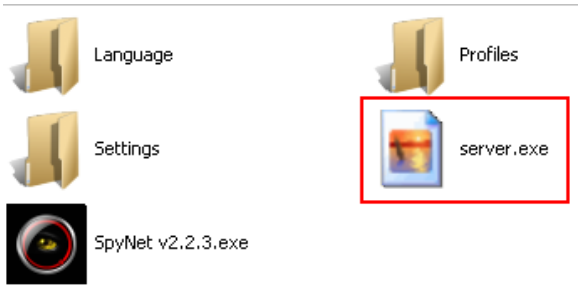
Esto sirve para que el servidor pase distintos tipos de testeos en caso de que nuestro objetivo sospeche del archivo.

Pasamos a la ultima pestaña: Crear Servidor



1) Haciendo click en la imagen, podemos cambiar de icono por que el deseemos.
2) La opción comprimir con UPX sirve para que nuestro servidor sea mas liviano
3) Propagación por USV
4) Propagación por P2P (Emule, Ares, LimeWire, Etc.)
5) Muestra toda la configuración e información que hemos puesto y seleccionado.
6) Esa opción sirve por si deseamos unir el servidor con algún archivo
7) CREAR SERVIDOR!

Una vez creado y guardado, lo podremos ver como finalizado en el directorio que fue guardado previamente seleccionado por nosotros.

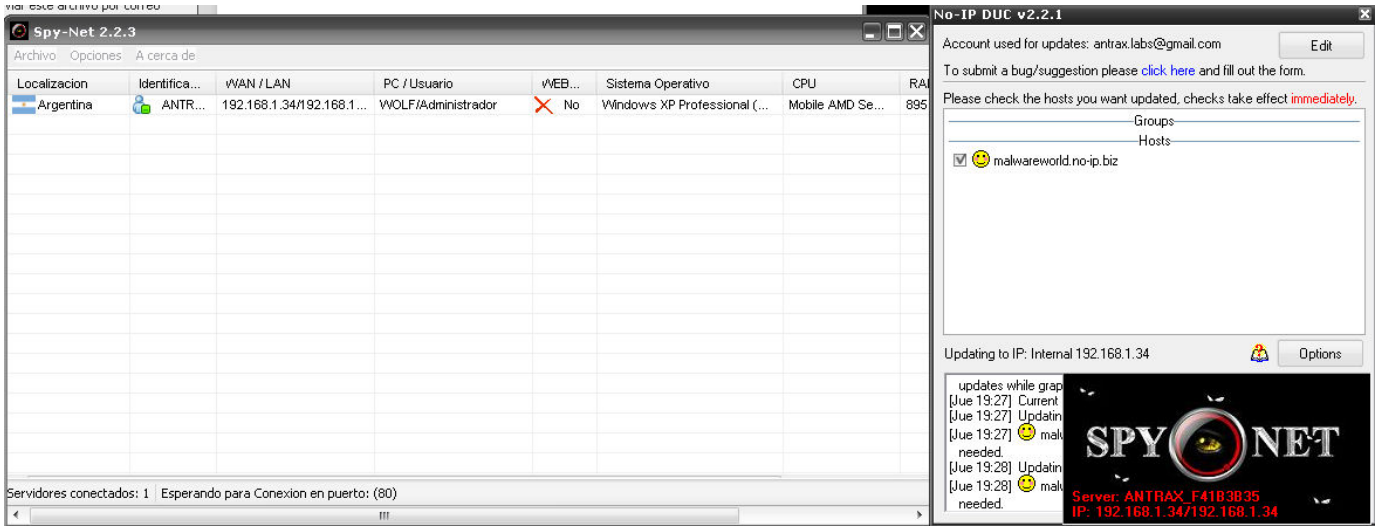


Comprobación:

Para comprobar que funciona, yo lo ejecutare en mi pc para que vean que si conecta.

Como verán, el servidor desaparece (ya que asi lo habíamos configurado) y salió el cartel de error que había hecho.

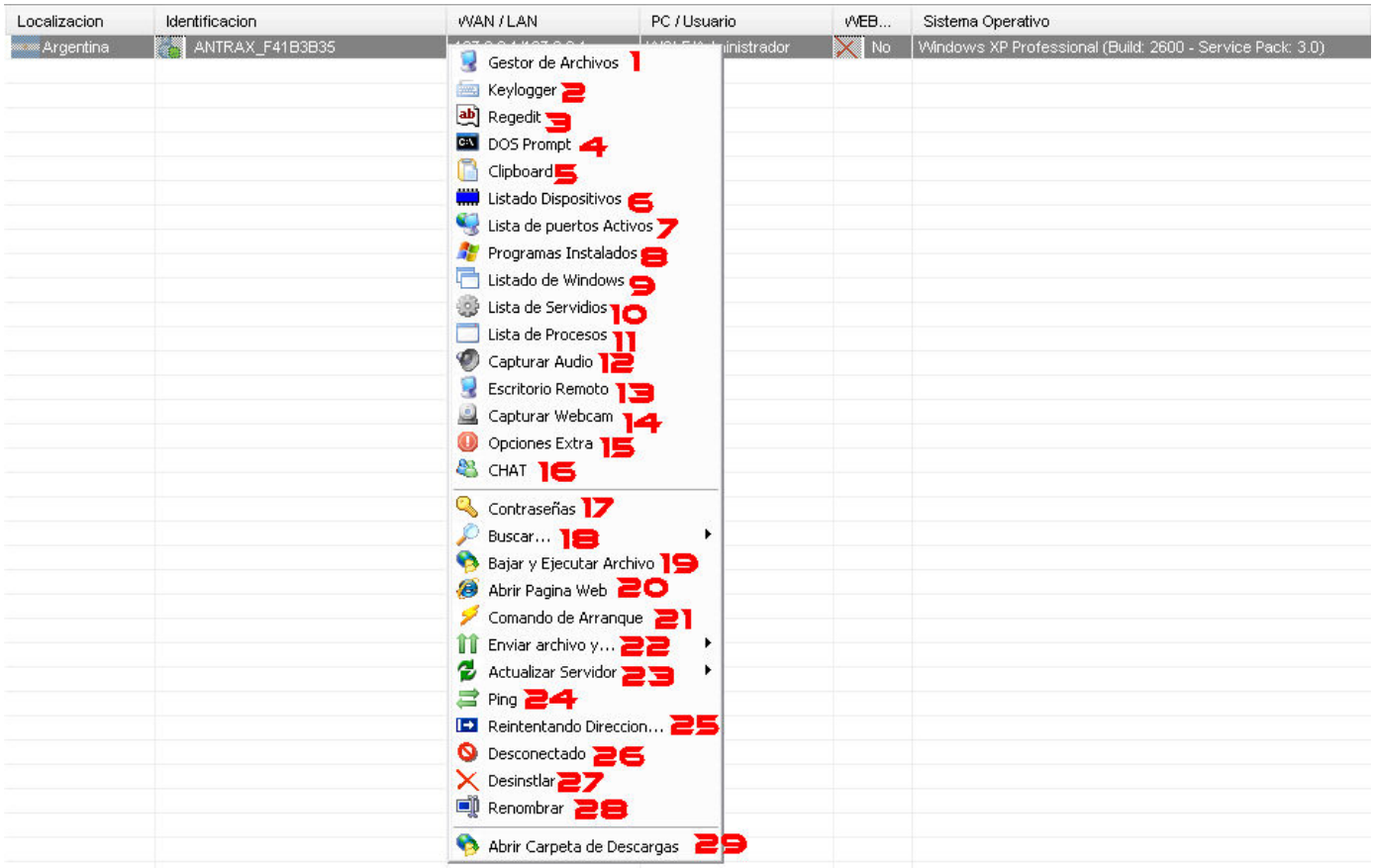
Seguido de esto, podremos apreciar un cartel de notificación estilo msn, que nos avisa que un remoto se ha conectado



Como verán, en el cliente muestra la bandera de mi país, Argentina, el nombre que le puse para identificar el remoto, ANTRAX, también aparece la IP, Sistema Operativo entre otras cosas…

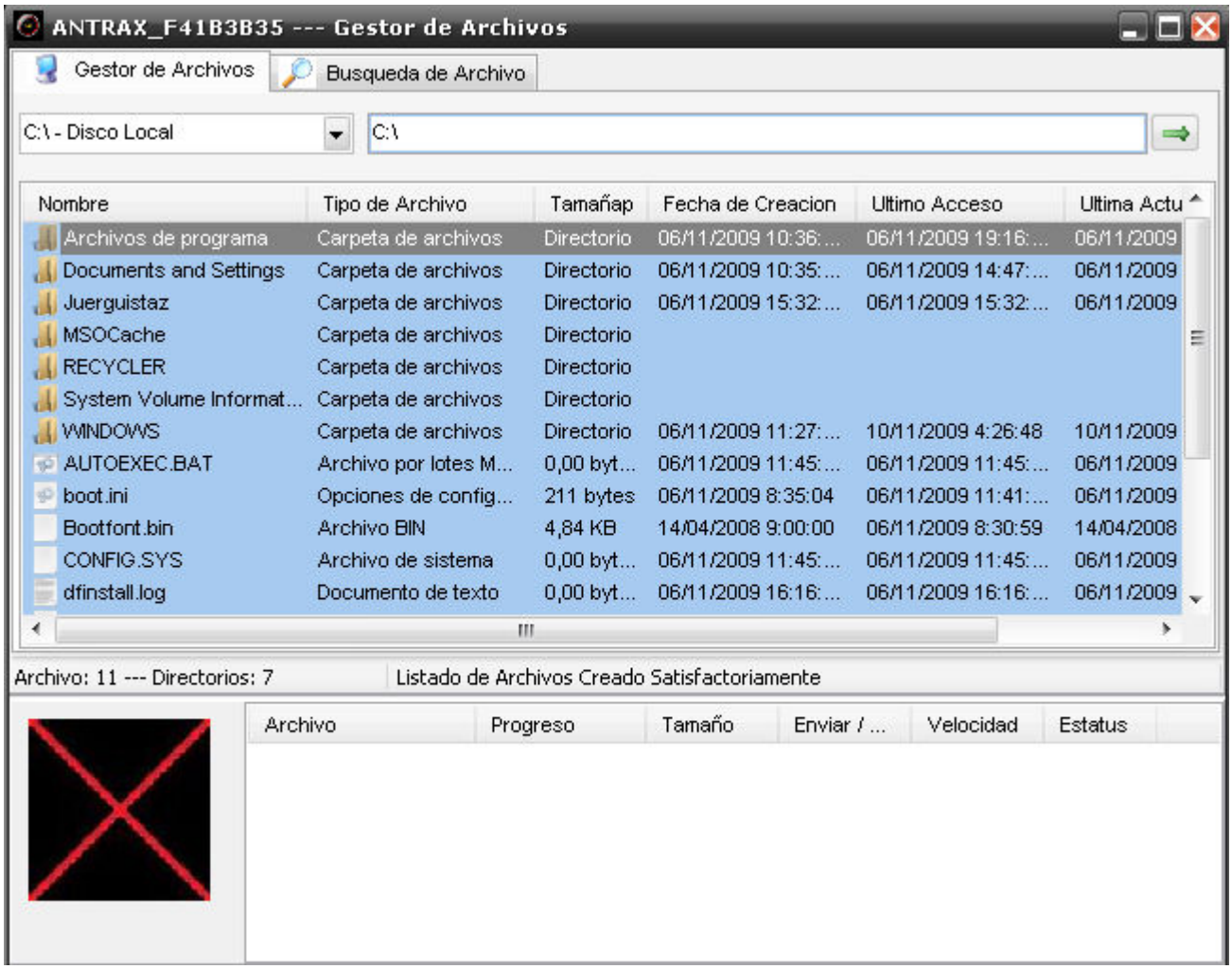
Opciones del Troyano:

Para acceder a las opciones, simplemente deberán hacerle click derecho a nuestro remoto para que se extienda un listado con las cosas que podemos hacer.

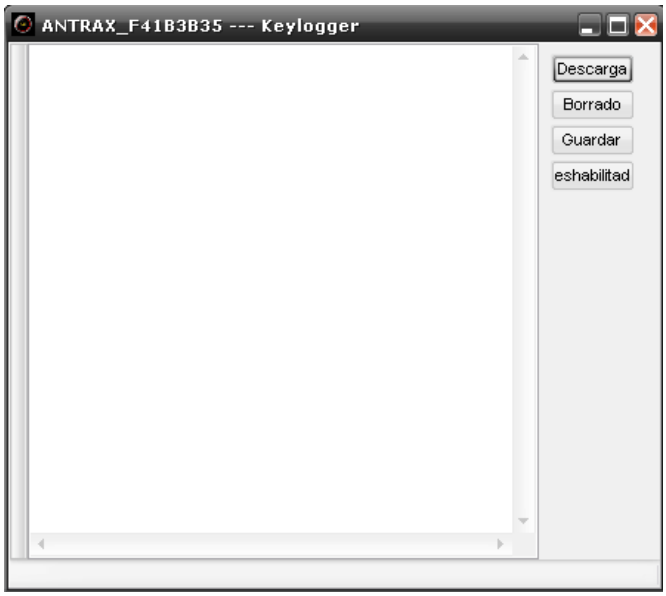


A continuación, explicare rápidamente para que sirve cada una de ellas:

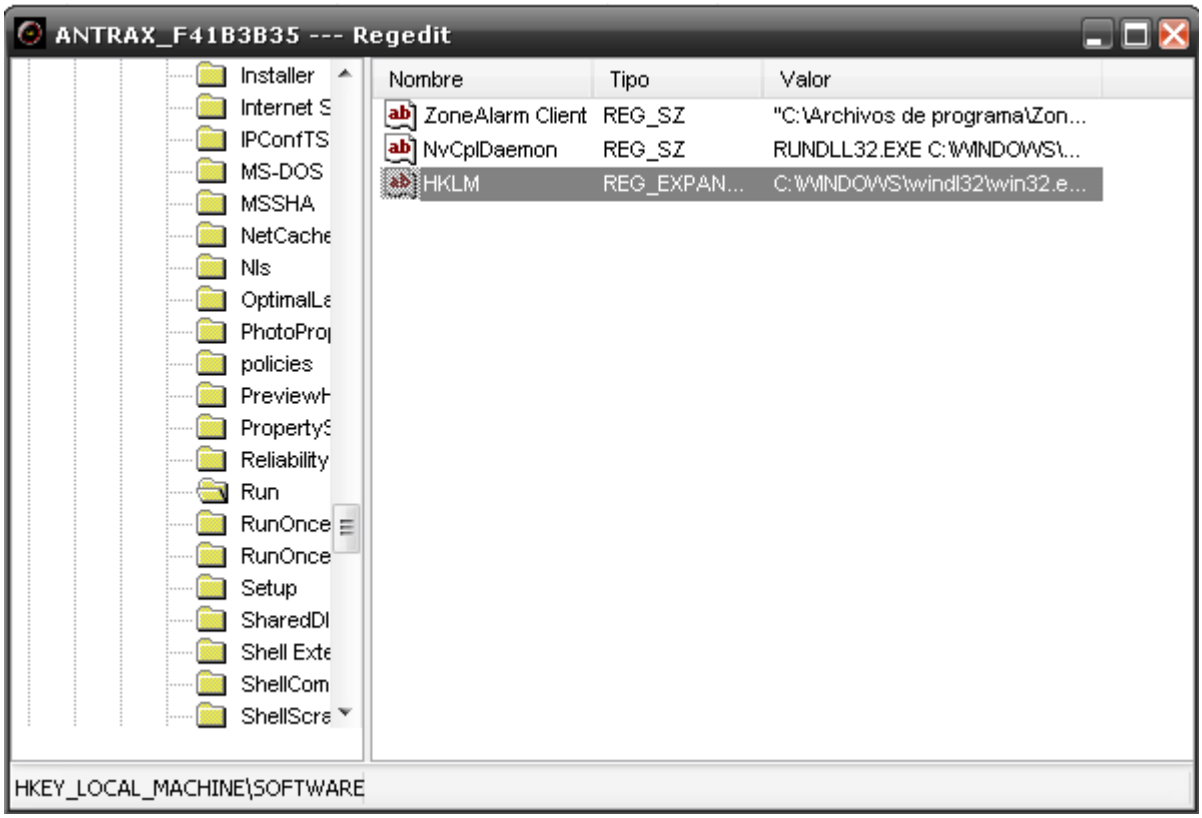
1) Gestor de Archivos: Podemos ver los archivos que nuestro remoto tiene en su PC.



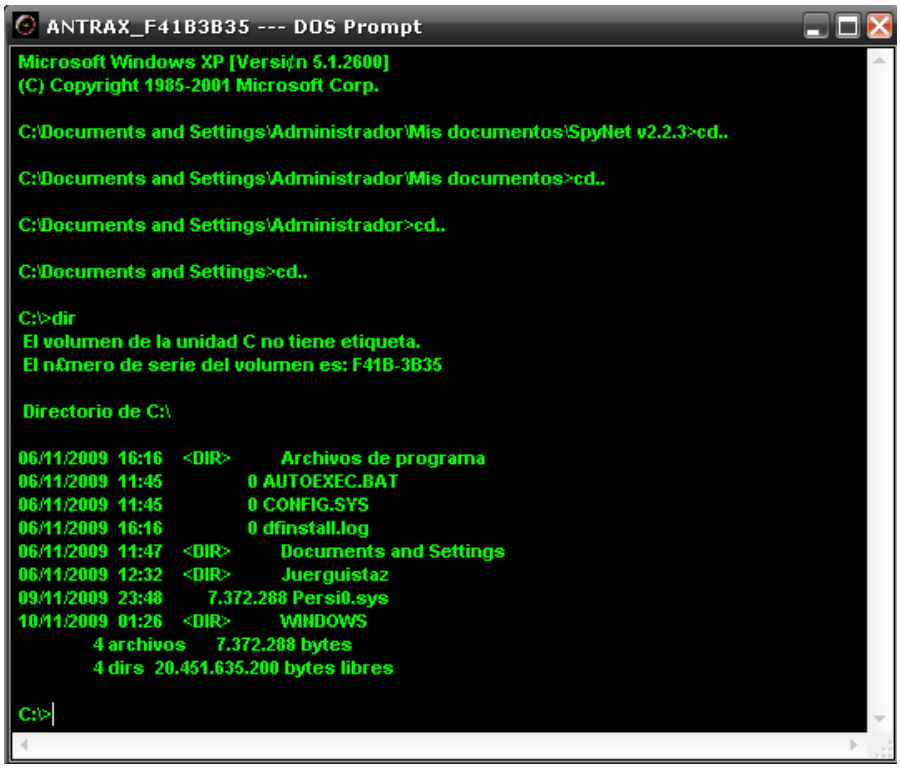
2) Keylogger: Podemos visualizar a tiempo real lo que esta escribiendo.



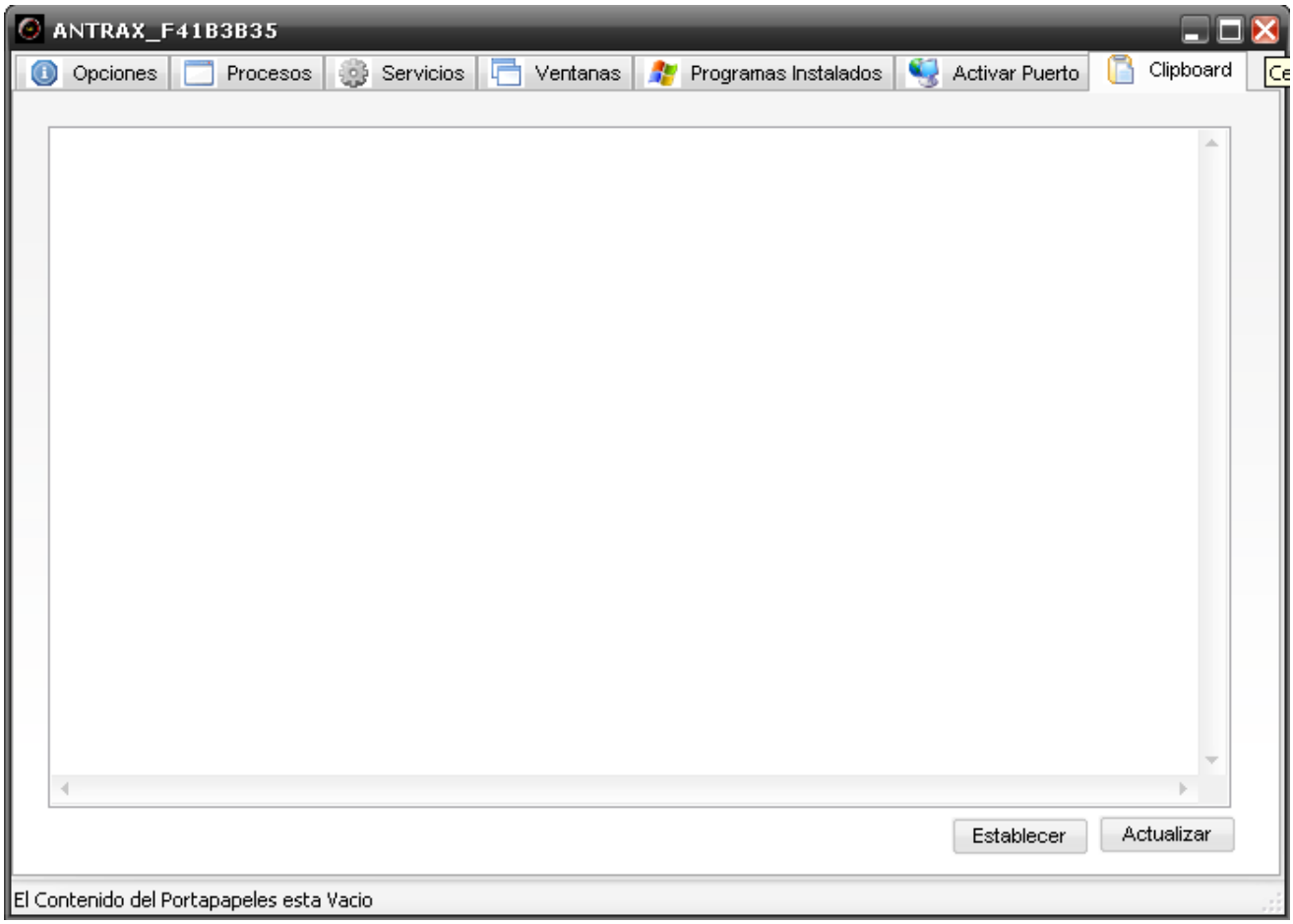
3) Regedit: Registro del sistema.



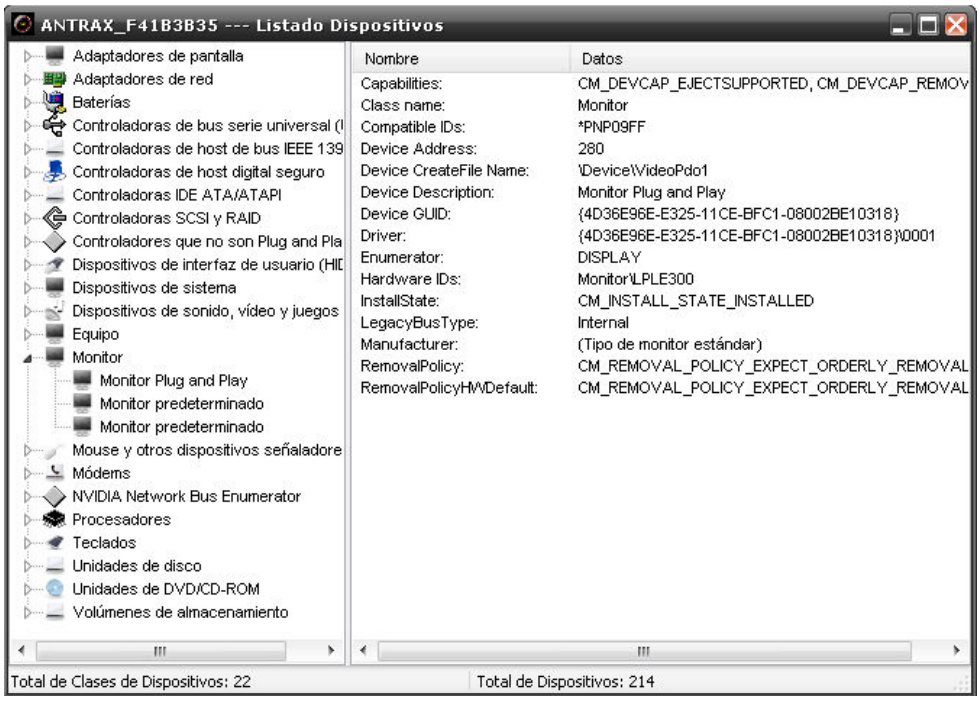
4) DOS Prompt: Esto nos sirve para podernos mover por la consola de Windows.



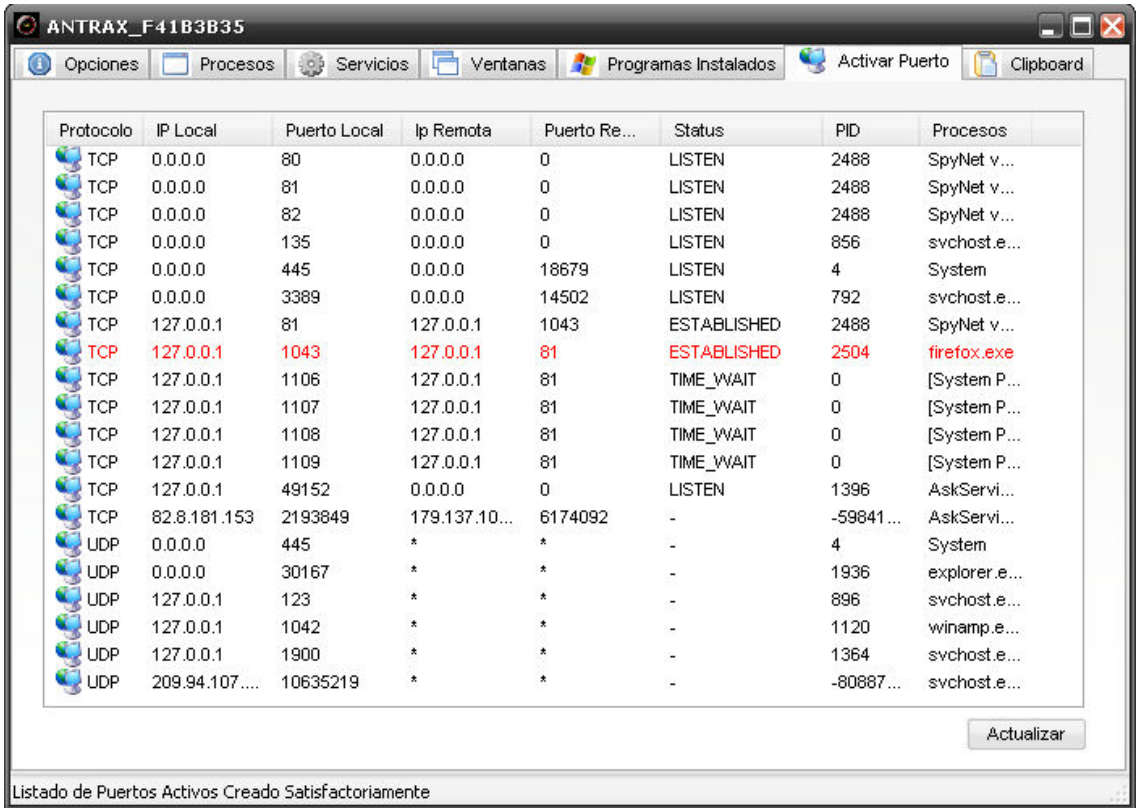
5) Clipboard: Portapapeles.



6)Listado de dispositivos: Drivers/Dispositivos instalados en la PC.

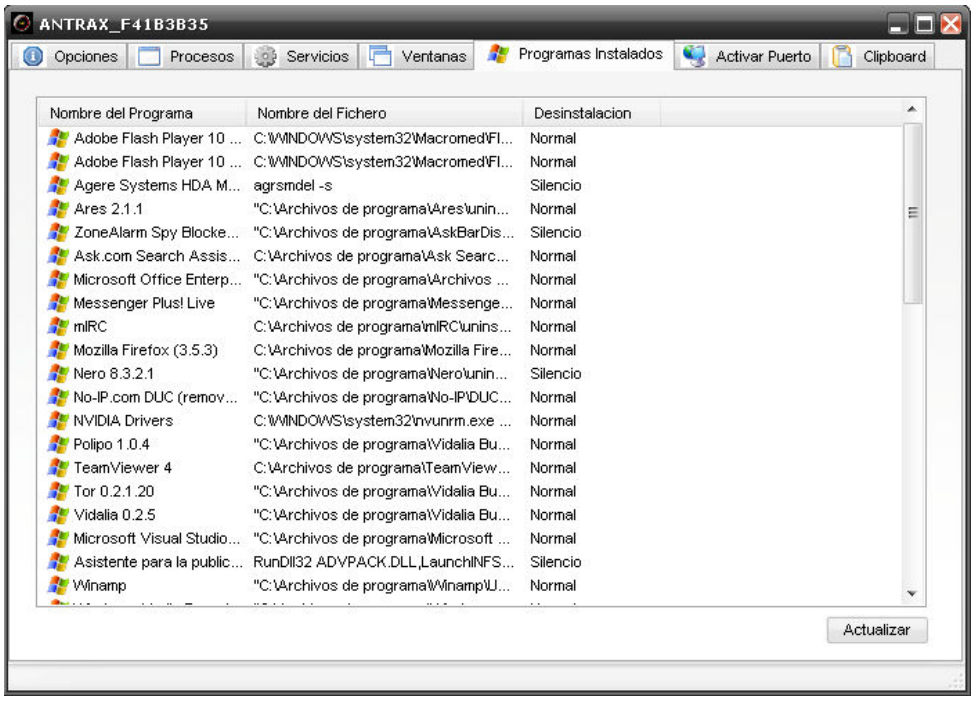


7) Puertos Activos: Muestra que puertos se están utilizando [El que esta en rojo, es el que esta usando nuestro Troyano].

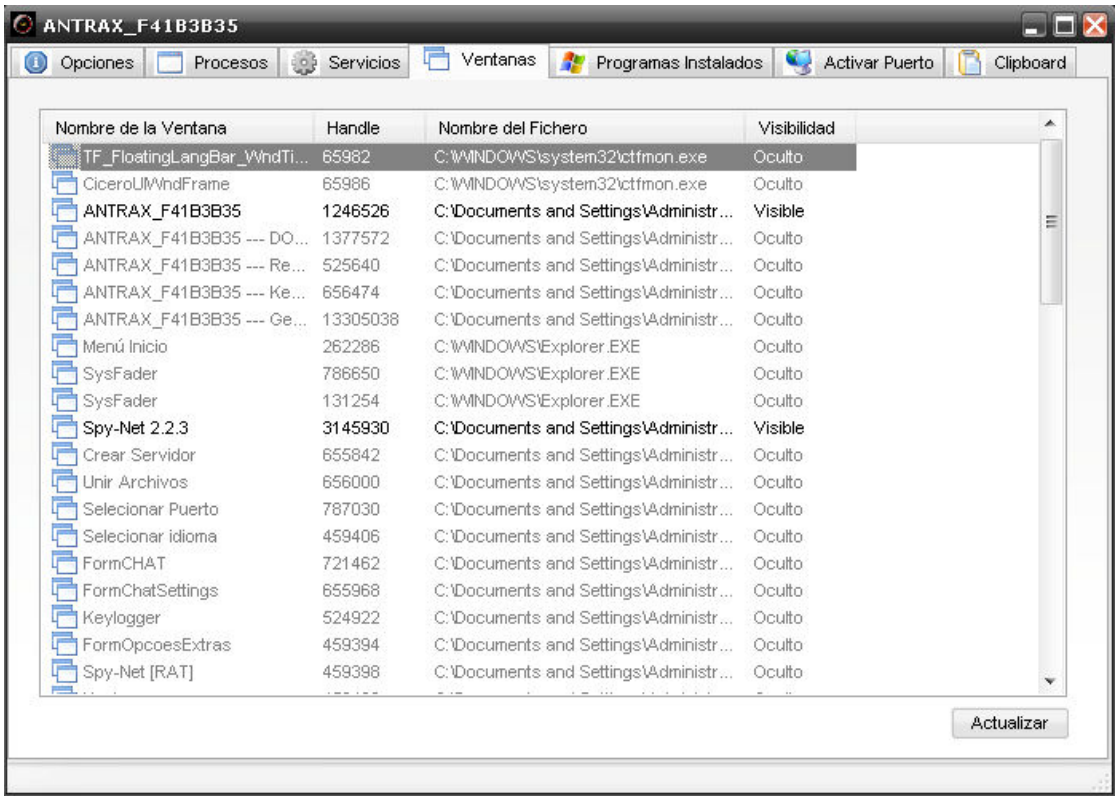


Protocolo	IP Local	Puerto Local	Ip Remota	Puerto Re...	Status	PID	Procesos
TCP	0.0.0.0	80	0.0.0.0	0	LISTEN	2488	SpyNet v...
TCP	0.0.0.0	81	0.0.0.0	0	LISTEN	2488	SpyNet v...
TCP	0.0.0.0	82	0.0.0.0	0	LISTEN	2488	SpyNet v...
TCP	0.0.0.0	135	0.0.0.0	0	LISTEN	856	svchost.e...
TCP	0.0.0.0	445	0.0.0.0	18679	LISTEN	4	System
TCP	0.0.0.0	3389	0.0.0.0	14502	LISTEN	792	svchost.e...
TCP	127.0.0.1	81	127.0.0.1	1043	ESTABLISHED	2488	SpyNet v...
TCP	127.0.0.1	1043	127.0.0.1	81	ESTABLISHED	2504	firefox.exe
TCP	127.0.0.1	1106	127.0.0.1	81	TIME_WAIT	0	[System P...
TCP	127.0.0.1	1107	127.0.0.1	81	TIME_WAIT	0	[System P...
TCP	127.0.0.1	1108	127.0.0.1	81	TIME_WAIT	0	[System P...
TCP	127.0.0.1	1109	127.0.0.1	81	TIME_WAIT	0	[System P...
TCP	127.0.0.1	49152	0.0.0.0	0	LISTEN	1396	AskServi...
TCP	82.8.181.153	2193849	179.137.10...	6174092	-	-59841...	AskServi...
UDP	0.0.0.0	445	*	*	-	4	System
UDP	0.0.0.0	30167	*	*	-	1936	explorer.e...
UDP	127.0.0.1	123	*	*	-	896	svchost.e...
UDP	127.0.0.1	1042	*	*	-	1120	winamp.e...
UDP	127.0.0.1	1900	*	*	-	1364	svchost.e...
UDP	209.94.107....	10635219	*	*	-	-80887...	svchost.e...

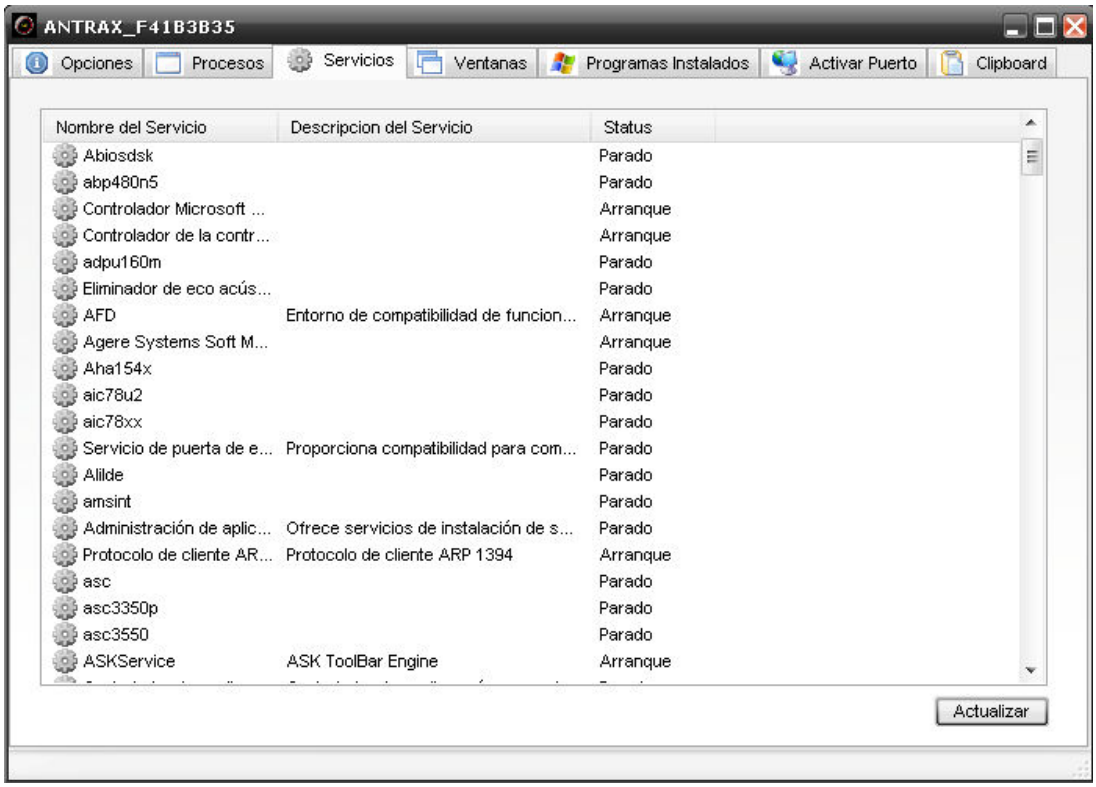
8) Programas Instalados: Los programas que están instalados en el PC de nuestro remoto, Clickeando con el otro botón se puede desinstalar el programa que deseen.



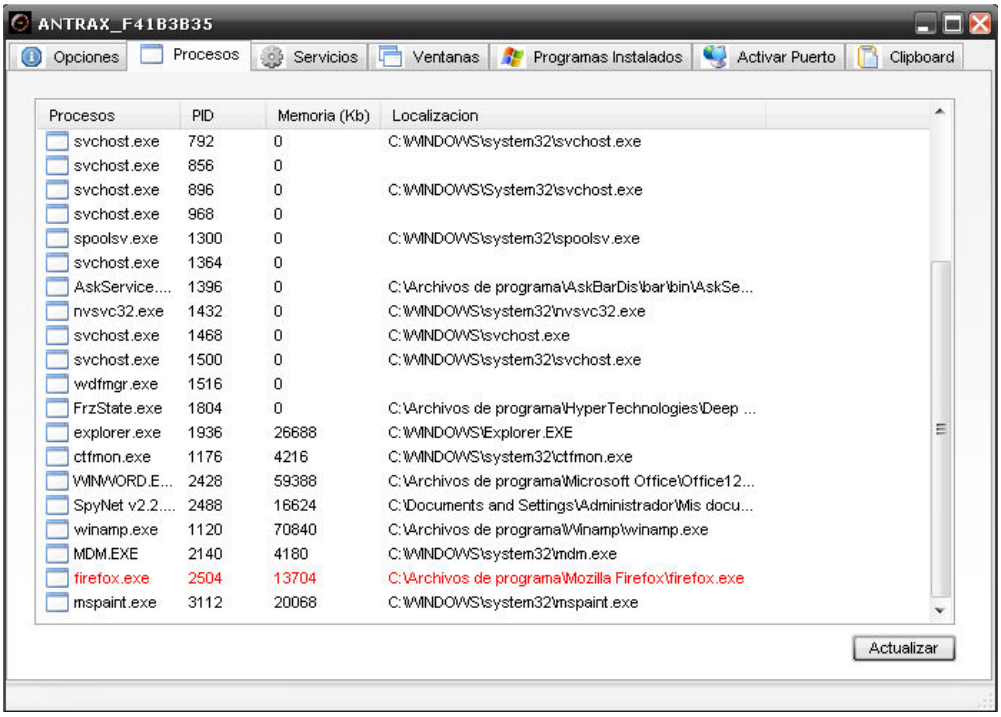
9) Ventanas: Muestra las ventanas activas en la PC, ya sean ocultas o visibles.



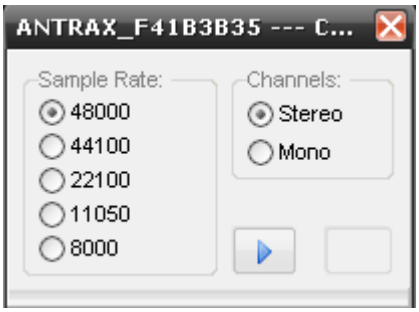
10)Servicios: Lista de servicios que hay en la PC.



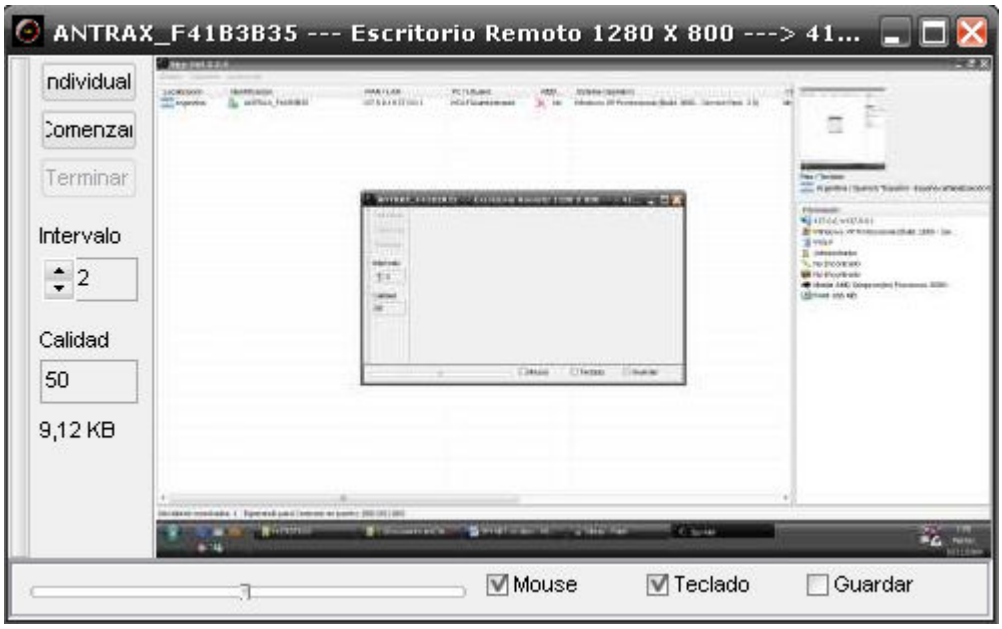
11)Listado de procesos: Muestra los procesos activos en la PC



12)Capturar Audio: Captura lo que se esta hablando por medio del micrófono de nuestro infectado.

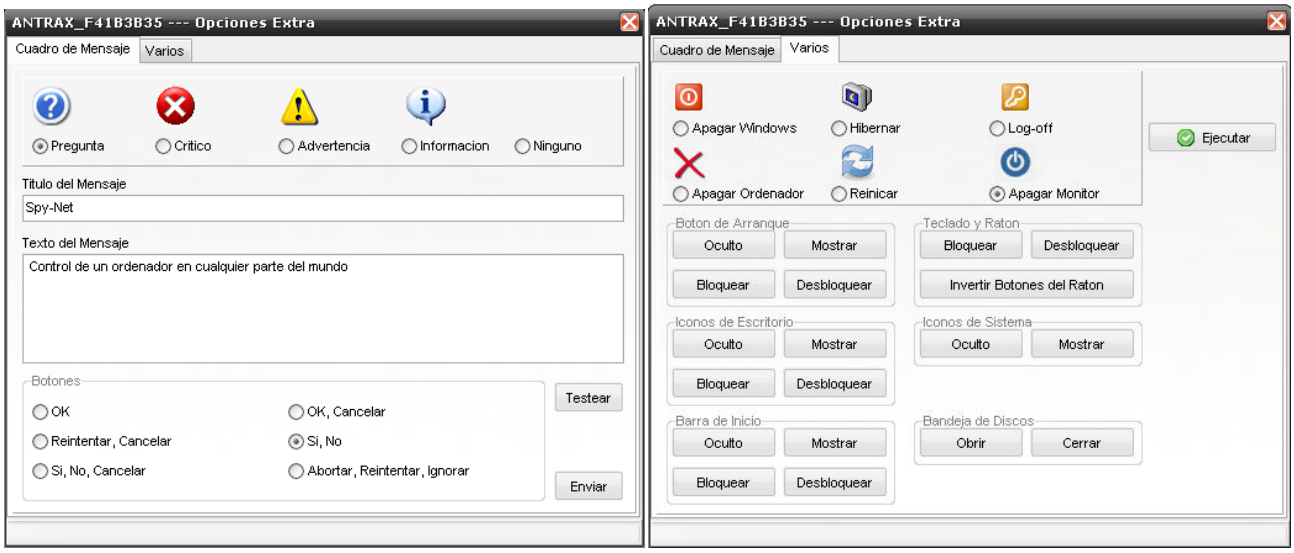


13) Escritorio Remoto: Permite controlar el teclado y el mouse de nuestro remoto.

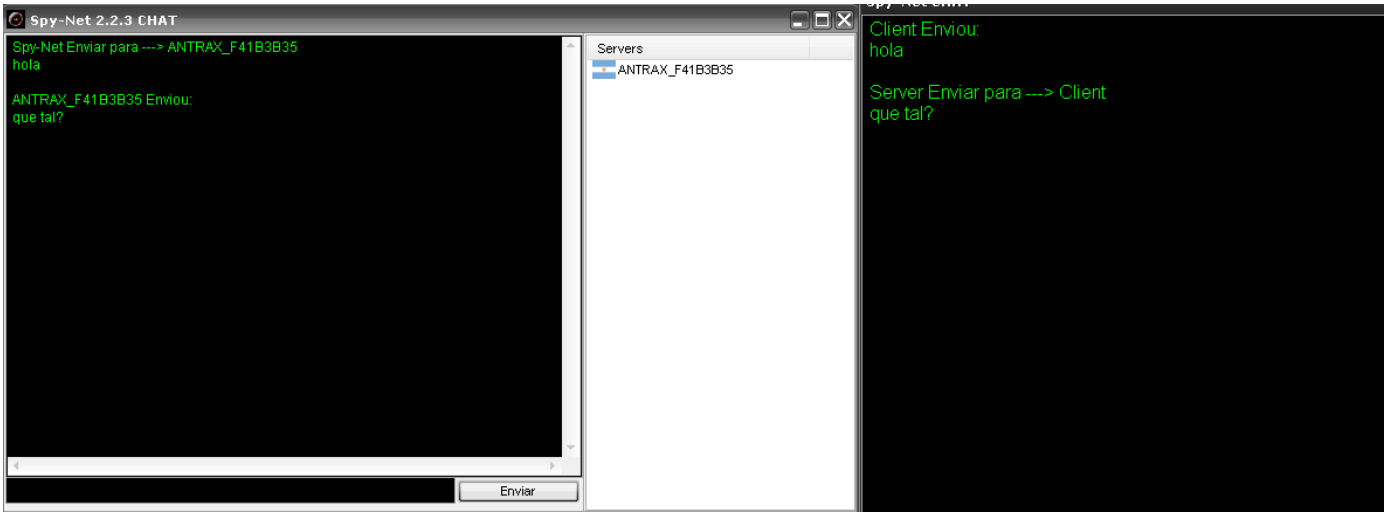


14) Capturar Webcam: Con esta opción podemos ver a nuestro remoto en caso de que tenga cámara. Lamentablemente yo no tengo, por eso no les podre mostrar una imagen de esta opción.

15) Opciones Extras: muestra carteles, y cambia de estado la PC.

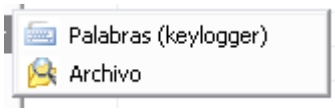


16) CHAT: Permite establecer una conversación con el remoto.



17) Contraseñas: Muestra las contraseñas almacenadas.

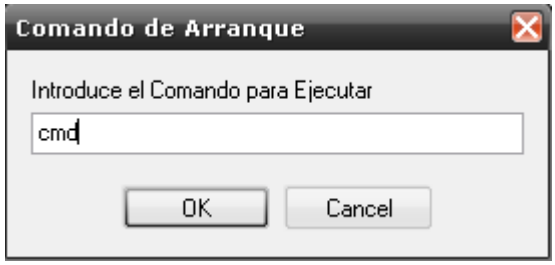
18) Buscar: Permite Buscar palabras en el Keylogger o Buscar Archivos en la PC del Remoto, solo debemos insertar una cadena de texto y lo buscara solo en caso de que exista.



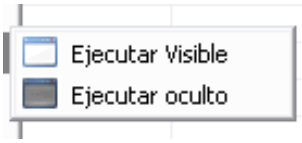
19) Bajar y Ejecutar Archivo: Permite descargar un Archivo desde una web y ejecutarlo en la PC de nuestro remoto.

20) Abrir Pagina Web: Permite abrirle a nuestro infectado la web que deseamos, en este caso mi Blog:

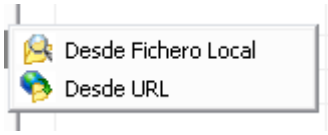
21) Comando de Arranque: Permite ejecutar el proceso que deseamos o comando que deseemos.



22) Enviar Archivo y Ejecutar: Permite subirle a nuestro remoto un archivo desde nuestra PC y ejecutárselo de manera visible o invisible.

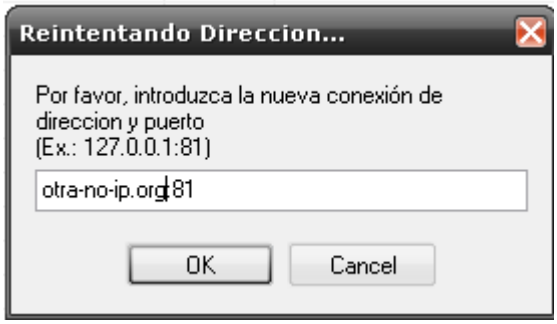


23) Actualizar Servidor: Permite subirle a nuestro infectado un nuevo servidor con algún tipo de actualización. Se puede hacer mediante un fichero de la misma PC o desde una URL.



24) Ping: Sirve para testear que la conexión este establecida correctamente.

25) Reintentando Dirección: sirve para Direccionar el remoto a otra DNS.



26) Desconectado: Sirve para desconectar el Remoto hasta que se vuelva a iniciar el Troyano.

27) Desinstalar: Sirve para remover el troyano de nuestro Remoto (Desinfectar)

28) Renombrar: Sirve para cambiarle el nombre a nuestro Remoto.

29) Abrir Carpeta de descargas: Sirve para ver los archivos extraídos de nuestro Remoto.

Esto es todo! Espero que les haya gustado y que les sirva. Nos vemos en la próxima edición.

Visiten Diariamente mi blog que es actualizado todos los días:

http://antrax-labs.blogspot.com

Para consultas, pueden enviar un mail a: antrax.labs@gmail.com

ANTRAX