BY ANTRAX

Indetectabilizacion de Troyanos. [TODOS LOS METODOS] By ANTRAX

Hola. Soy Antrax. Llevo días preparando la guía de oro de los troyanos.

Esta guía contiene todos los métodos posibles de la red para hacer troyanos indetectables. En otras palabras es la recopilación más grande de internet.

CONCEPTOS

Primero que nada, tendremos en cuenta algunos conceptos:

Offset: Firma, los offsets son firmas que los Antivirus eligen para detectarlo

Stub: Son los moldes que usan los troyanos para armar sus servers

Servers: Es lo que enviamos a nuestro objetivo

Cliente: Es lo que usamos para manipular la PC a la que atacamos

FUD: Full UnDetected (Indetectable al 100%)

Método Antrax “Tapando Offsets” [Edición Hexadecimal]

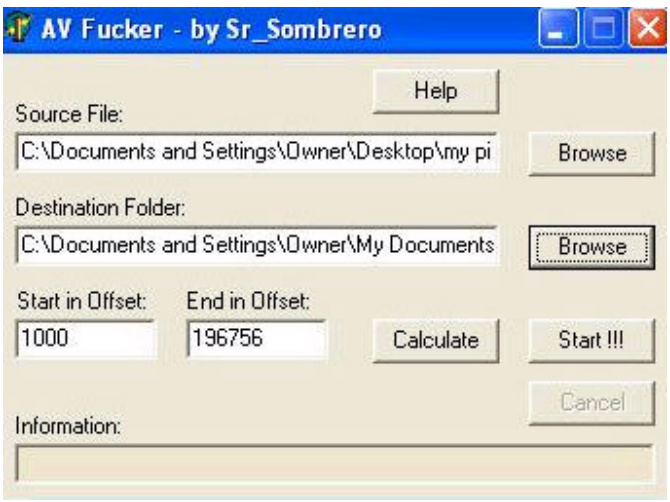
Este método consiste en editar las firmas detectables de un Stub para que quede indetectable. Es un método bastante largo y costoso, pero el más efectivo.

El método Antrax consiste en dos partes:

Parte 1:

Creamos una carpeta que se llame **fake2fuker en mis documentos**

Abrimos el AV Fucker



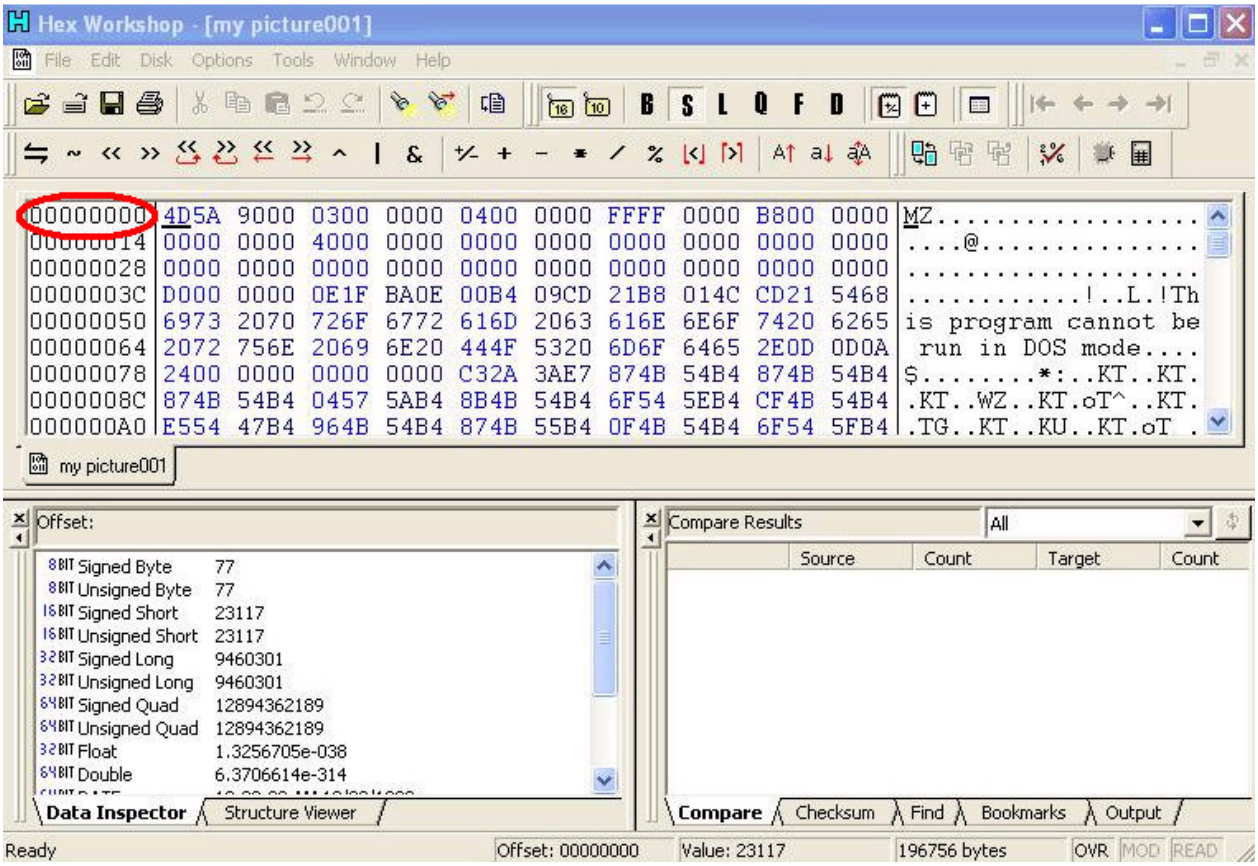
En Source File seleccionamos el Stub o Servidor que queramos hacer indetectable.

En Destination Folder, ponen la carpeta en donde descompondrán los offsets.

En Start in Offsets ponemos en donde queremos que comience a descomponer

Y en End in Offset ponemos en donde queremos que termine.

Para saber los valores de Start y los de End, es necesario abrir el Editor Hexadecimal, en este caso el Hex WorkShop. Una vez abierto ponemos: **OPTIONS → FILE OFFSET → DECIMAL.** Después de eso abrimos nuestro cliente o server y saldrá algo así:

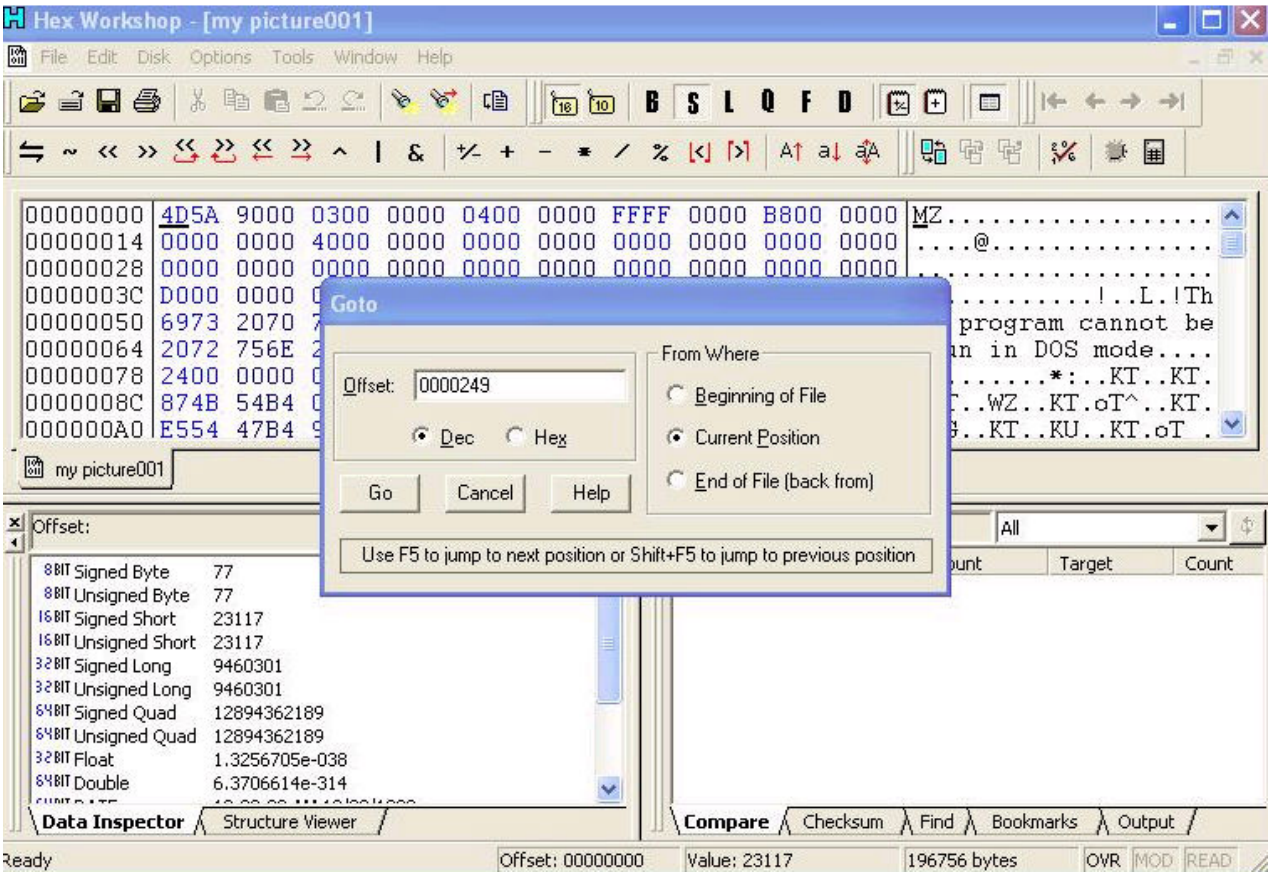


Como podrán ver, en la imagen comienza con ocho ceros “00000000” eso quiere decir que ese valor va en Start in Offset. Y luego bajamos al todo y buscamos el ultimo numero de todos y lo ponemos en End in Offset.

Una vez hecho eso, pulsamos en Start!!! Y comenzara a fraccionar el Stub o Server por Offset.

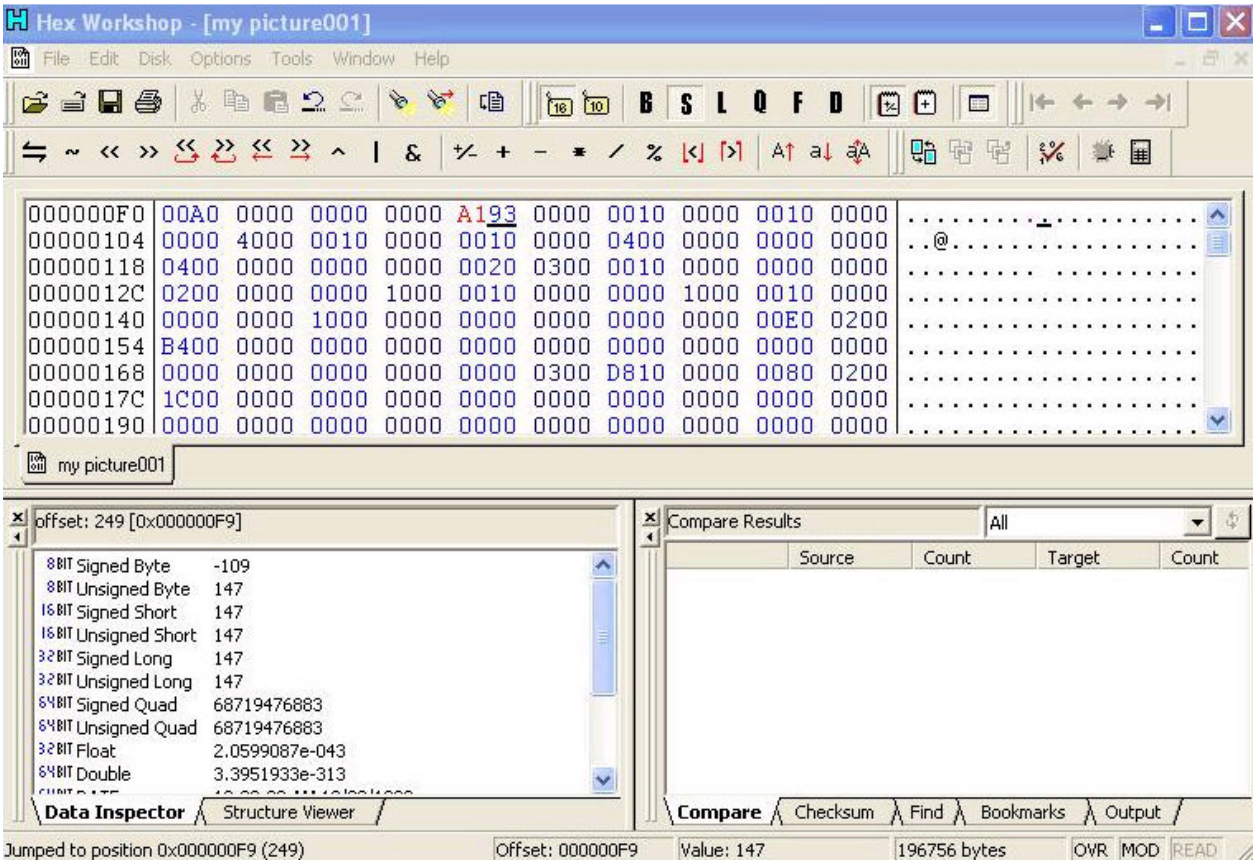
NOTA: Si el disco duro se les llena y no alcanzaron a descomponerlo al todo, intenten descomponer por partes. Ej: si el End Offset es 00020000, busquen la mitad, y les quedara 00010000. Y si no les resulta, busquen la mitad de la mitad hasta que les entre.

Una vez que termine de analizar, le pasamos el Antivirus a la carpeta **fake2fuker**, y a los offsets que nos detecte como virus, debemos modificarlos. Si el server está muy quemado, detectara a unos 2000 offsets. El AV va a detectar a uno o varios archivos, por ejemplo: “0000249”. Esto quiere decir el numero de offset que el AV eligió para hacerlo malicioso. Entonces debemos abrir el editor hexadecimal y presionamos “Ctrl + G” que es un buscador:



En Offset ponemos el numero del Offset que detecto el AV. Las opciones tildadas deben quedar como están en la imagen, Y presionamos “Go”.

Esto nos llevara directo al offset malicioso:

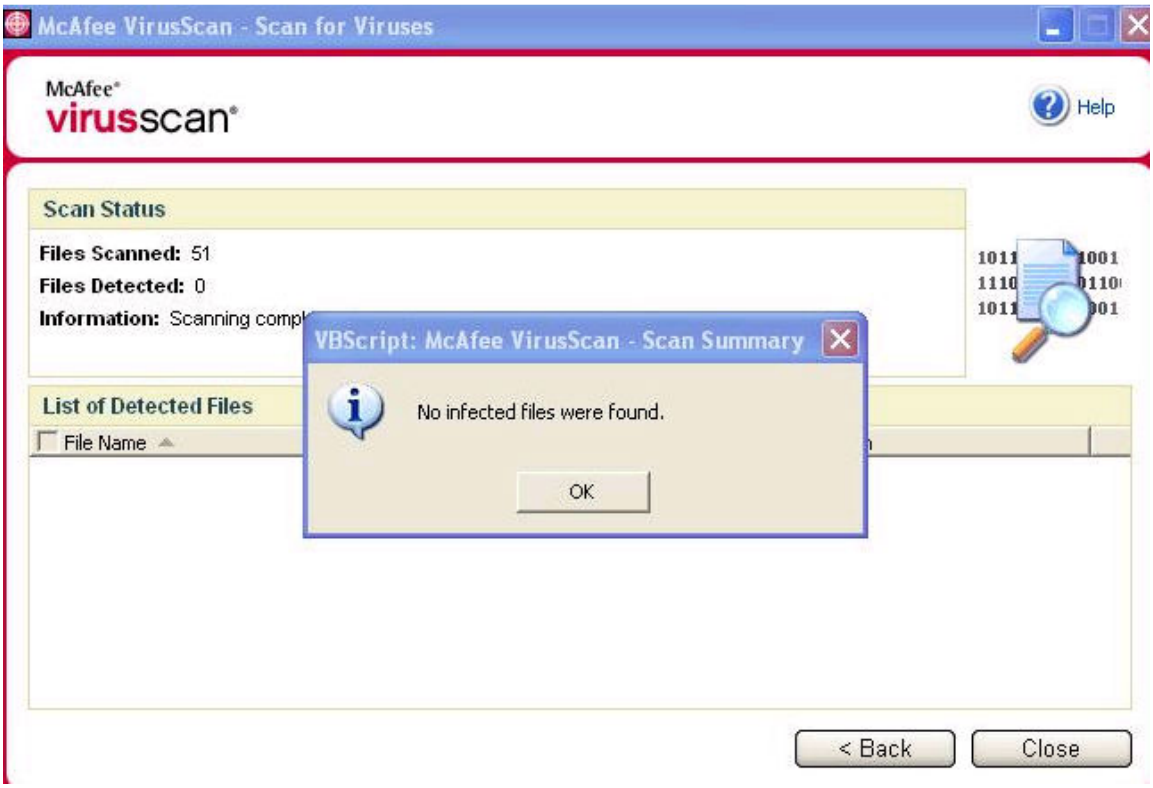


Nos va a tirar directo al offset A093 acá esta lo importante, el método consiste en sumar +1 o bien +2 o restar -1 o bien -2 hay que probar con varios porque muchas veces al modificar el offset se arruina el server o cliente. En este ejemplo le vamos a cambiar el

A093 POR A193
y así cambiamos todos los offsets maliciosos que nos haya detectado el AV (Anti Virus).

Después de haber modificado todo, guardamos el proyecto del editor hexadecimal CON EXTENSION .EXE esto es importantísimo!!!

Finalmente abrimos el AV y se lo pasamos a nuestro Server o Stub:



Y listo!! Ya esta indetectable…

Parte 2:

Debido a que este método es muy complicado ya que los Avs detectan muchos offsets, lo que debemos hacer es lo siguiente:

Opción 1: Buscamos un Server Editado de algún lado, si no encuentran, busquen en Club hacker que yo mismo los he subido (www.r00thack.webcindario.com). Una vez encontrado, podrán observar que lo detectan pocos AVs. Una vez analizado pueden proceder a la edición Hexadecimal anteriormente explicada, y será mucho más fácil ya que habrá menos offsets

Opción 2: Buscar un Crypter, lo más FUD posible, y una vez encriptado nuestro Server o Stub, podrán observar que muchos Offsets fueron tapados y podrán proseguir con la edición Hexadecimal anterior mente mencionada y les será mucho más fácil ya que tendrán una menor cantidad de Offsets.

Este método es muy Eficaz aunque costoso. Y una vez que el server fue modificado con este método, puede de que dure años sin ser detectado.

Programas necesarios: http://rapidshare.com/files/89079403/Tools_By_DiNnO.rar.html y el http://www.hexworkshop.com/

----------**By ANTRAX**----------

Método RIT [Mejorado por ANTRAX]

Este método también consiste en tapar Offsets. Pero este es solo con programas. Los programas necesarios son estos:

ResHack: http://rapidshare.com/files/115721345/ResHacker.zip.html

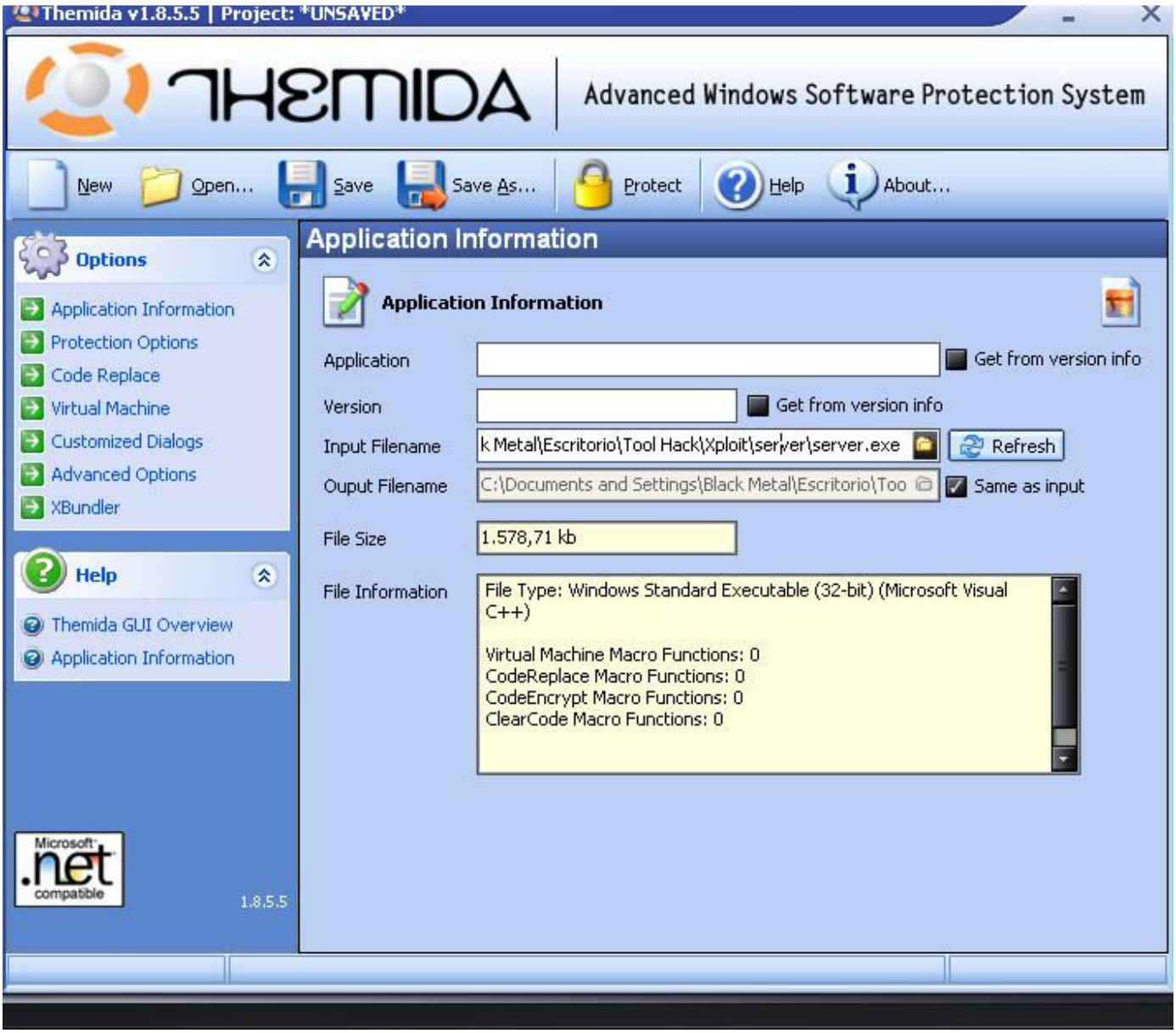
LordPe: http://rapidshare.com/files/115721522/LordPE.zip.html

Themida: http://www.megaupload.com/es/?d=AM4D2KT0

IExpress: ya viene con el PC

Lo primero que debemos hacer es abrir el Themida, y proteger nuestro server.

Para ello seguimos los siguientes pasos:



Lo único que debemos hacer en esta ventana es poner nuestro server en Input Filename.

Después de esto ponemos en el panel de la izquierda la opción "**Protection Options**"

Acá solamente se marcan las opciones **Aplication y Resources**, lo demás lo dejas todo desmarcado y con **Anti-Patching en None.**

Despues nos dirigimos a Virtual Machine

Dejamos todo como está menos esto:

Entry Point Virtualization: 15

Processor Type: Mutable Cisc Processor

Multiprocesor: 1 CPU

Opcode Type: Metamorph – Level 1

Dynamic Opcode: Disabled

Despues de esto nos vamos a Advanced Options

Se daja todo como está menos el Last Section Name que se pone rhkv

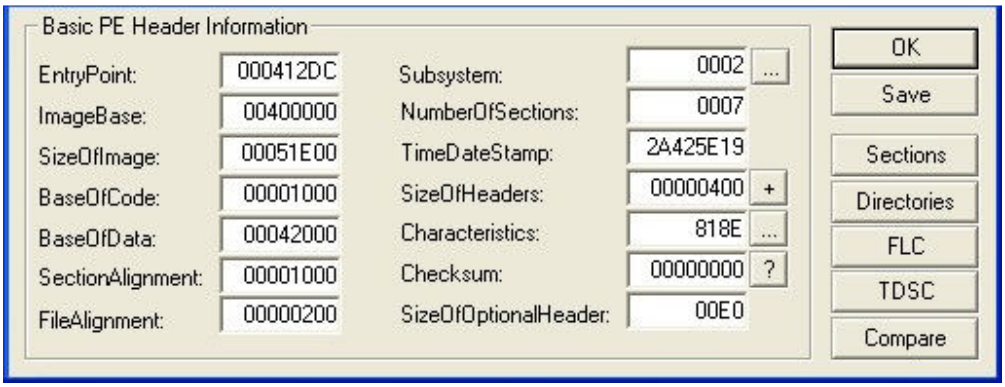
Una vez acabado todo esto se le da clic en **Project** y despues, cuando haya acabado en **Close**

Una vez terminado esto… Tendremos el server encriptado o protegido.

Despues de esto, abrimos el LordPE

Ahora hacemos click en donde dice **Rebuild PE** y escogemos el server del troyano. Ahora hacemos click en **PE Editor** y se escoge otra vez el server del troyano.

Bien, ahora nos saldrá esto:



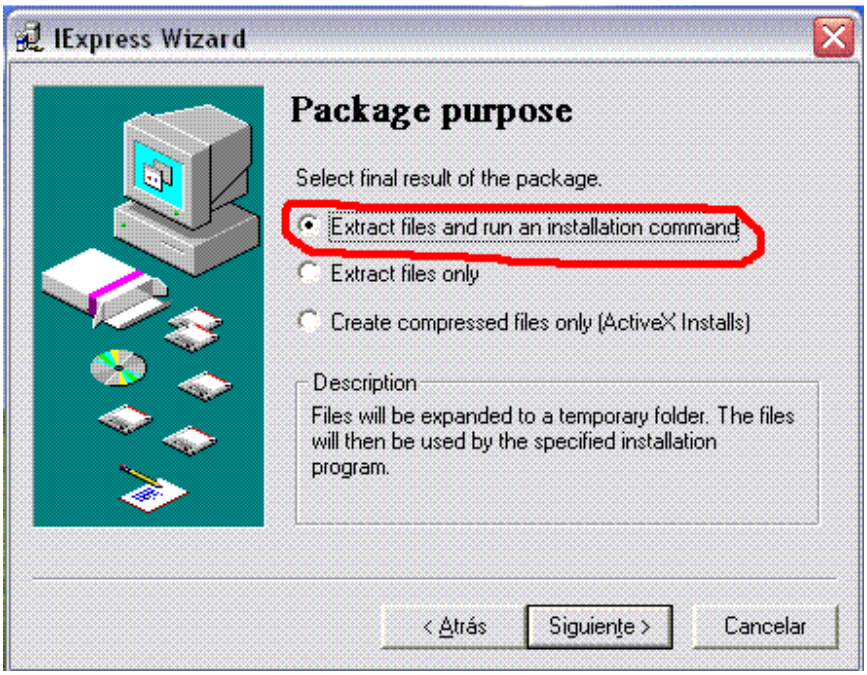
Lo único que hay que hacer es sumarle uno a **BaseOfCode, BaseOfDate, TimeDateStamp** y **Checksum**. Ej: 00001000 quedaría 000010001 y así con los mencionados anteriormente

Para finalizar clicamos en **Save** y despues en **Ok** y se sale.

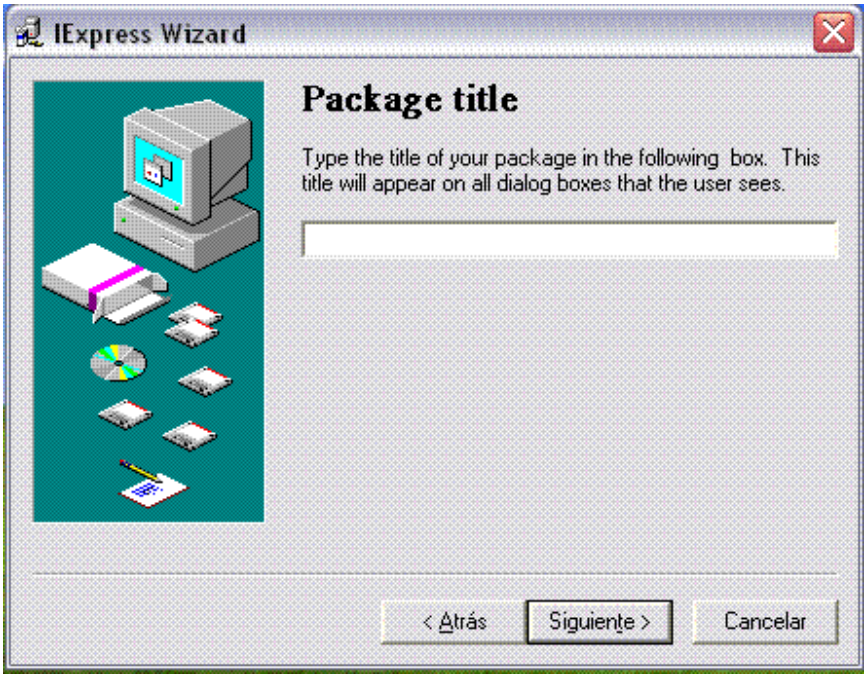
Una vez finalizado esto, es el turno del Iexpress.

1.- para que salga damos en inicio/ejecutar y escribimos iexpress
2.- nos sale algo como esto

3.- Damos en Siguiente

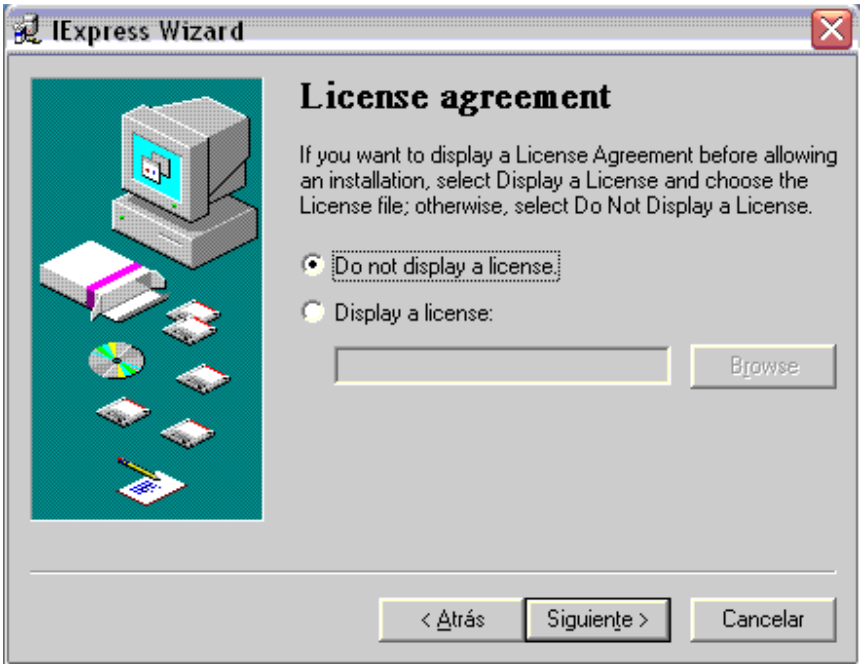


4.-Nos aseguramos de que este marcada la primera opción y damos en siguiente.

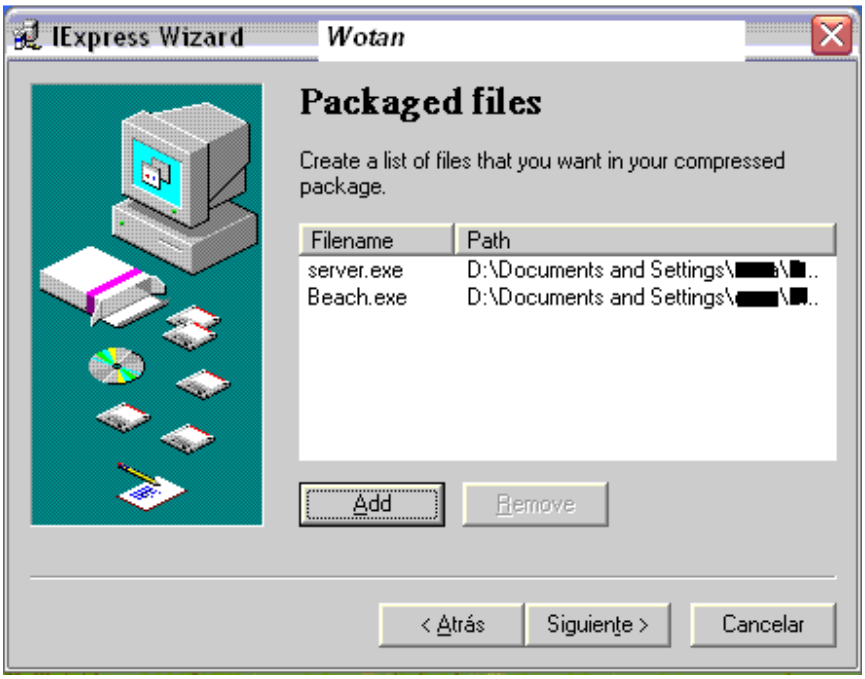


5.- Aquí ponemos el nombre del paquete y damos en siguiente

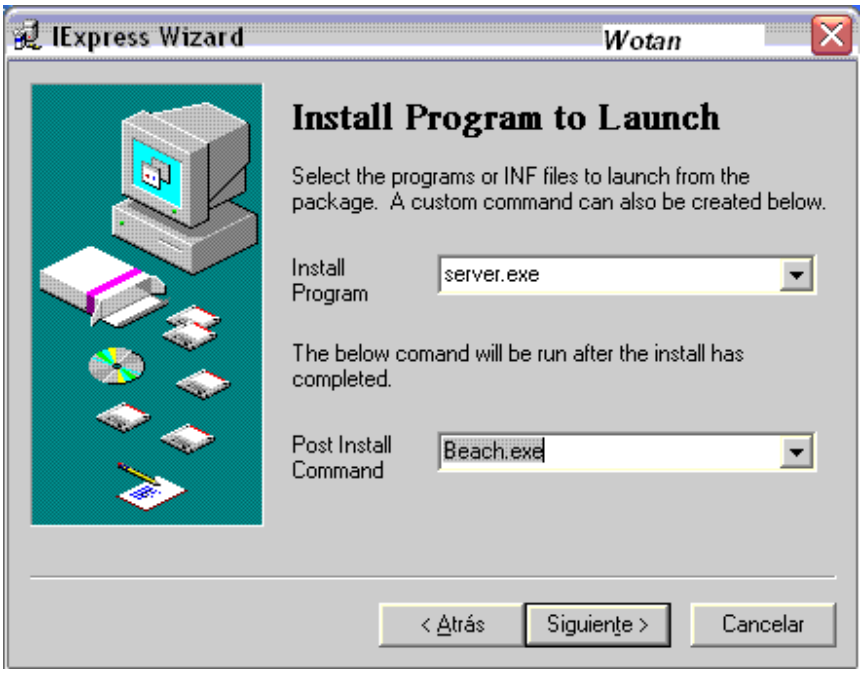
5.- Dejamos el No Prompt y damos en siguiente



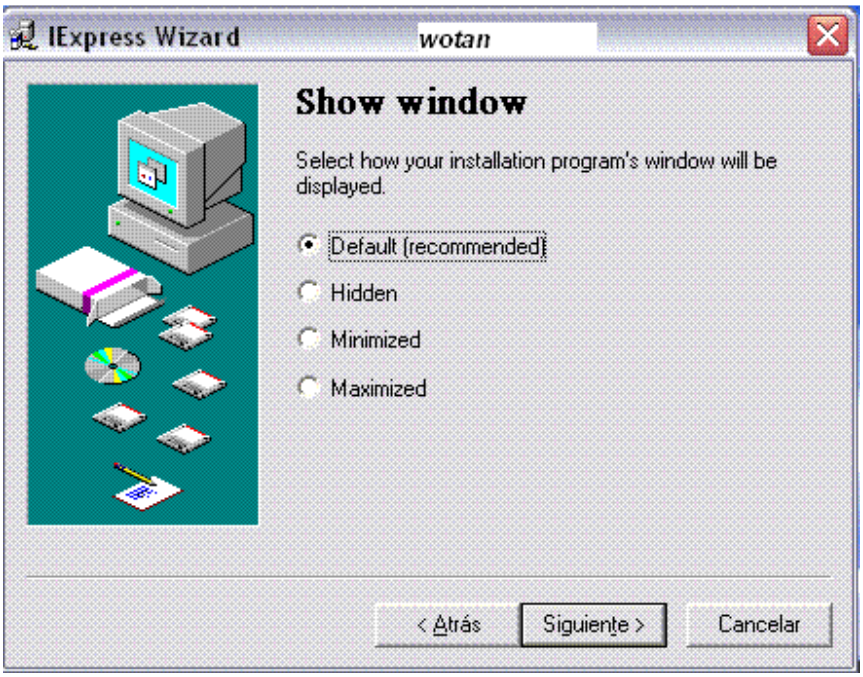
6.- Aca también dejamos seleccionado la primera opción y damos en siguiente



7.- Bien.. Ahora hacemos click en Add y agregamos primero el archivo que quieras unir (server.exe) y luego un archivo ejecutable que quieras que se muestre al ejecutar el paquete, los dos archivos tienen que ser .exe y luego en siguiente. en este caso vamos a utilizar un flash.

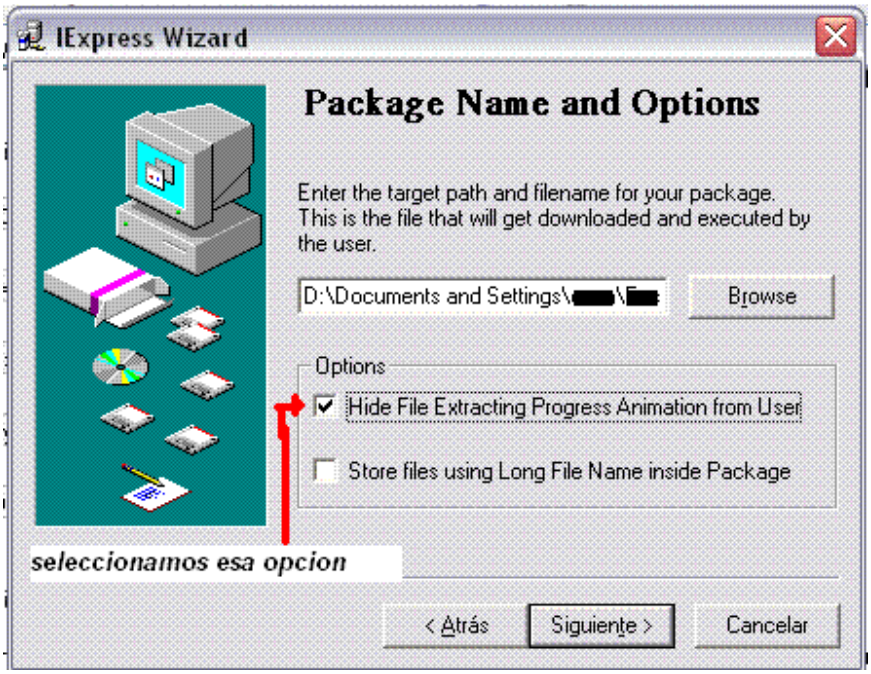


8.- donde dice: install the program pones el server o lo que quieras que se instale y en el otro el archivo a mostrar y siguiente.

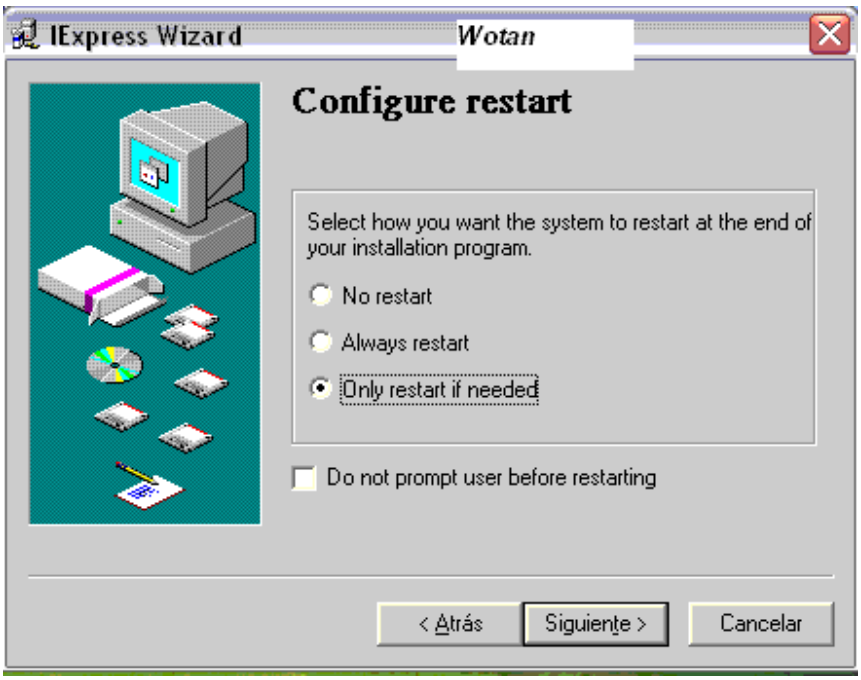


9.- Aca nos aseguramos de que este seleccionado el primero y le damos en siguiente

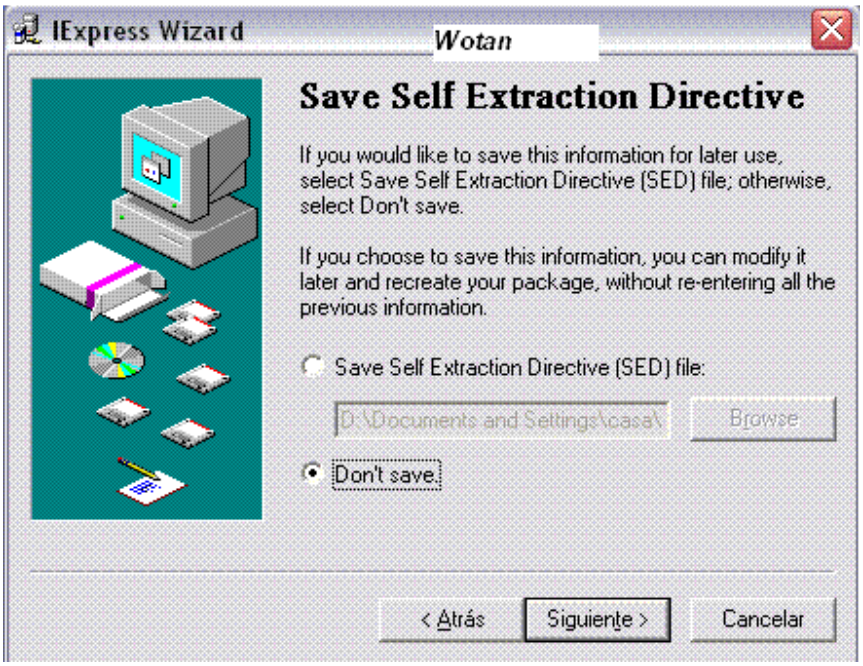
10.- En esta otra tienen la opción para que muestre o no un mensaje al ejecutar.



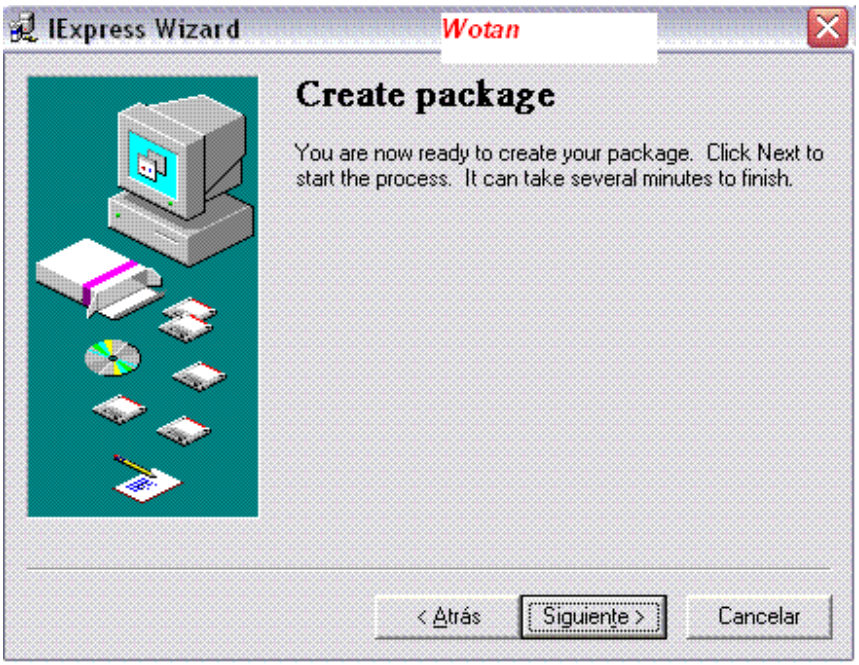
11.- escojemos el archivo que van a unirse los dos archivos, este sera el archivo ejecutado por el usuario, en este caso beach.



12.- nos da la opcion de reiniciar, reiniciar todo o solo reiniciar si es necesario, seleccionen la opcion NO RESTART. ahi me equivoque en la imagen.



13.- le damos en no, es para guardar informacion del paquete o no guardar la info

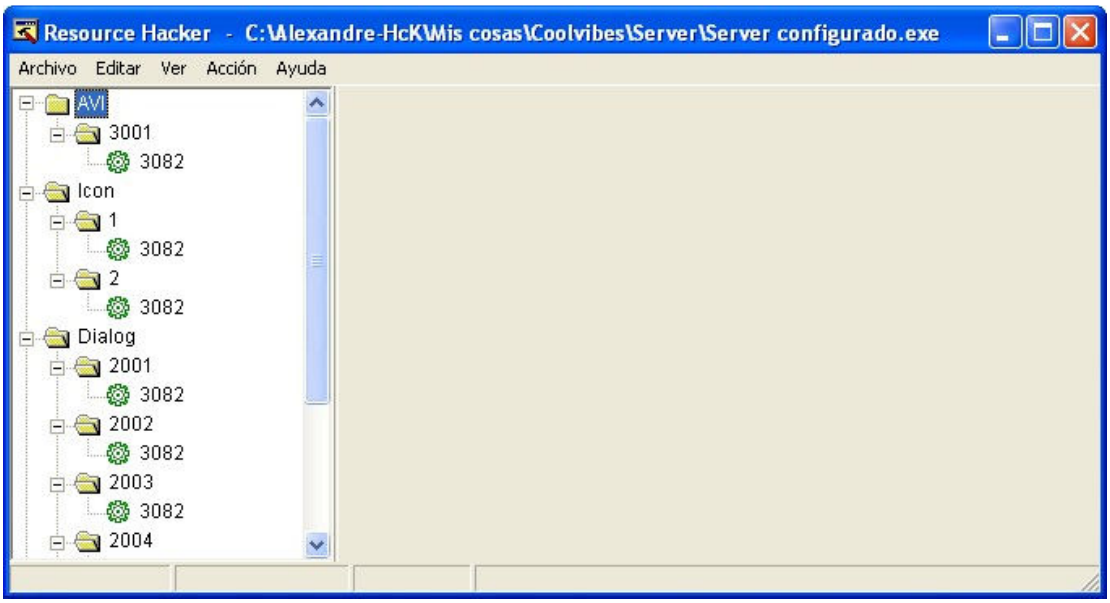


14.- listo ahora solo dale en siguiente para crear el paquete y ya.

Solo queda cambiarle el icono para que pase desapercibido.

Ahora es el turno del ResHacker.

abrís el ResHacker y despues abrís todas las carpetas, como aparece en la foto:



Como veis aparecen todo carpetas (AV, Icon, Dialog etc.) y subcarpetas, (3001 y todas esas) bueno, pues los archivos que hay dentro de las subcarpetas le das con el botón secundario y **Borrar**

Hay que borrar todos los archivo que hay en el server excepto lo que hay en **RCData**.

Si has hecho todo bien quedará al final solo la carpeta RCData, bien, ahora le das click en **Archivo** y clic en **Guardar como**… y sobrescribís el server.

Ahora ya tenemos el server casi indetectable. Solo hay que pasar otra vez el LordPe con la configuración que di al princpio de este tutorial.

Imágenes: Alexandre y Wotan Metodo RIT: Editado By ANTRAX

METODO MEEPA By MAZARD

Introduccion

El mejor modo de hacer indetectable un troyano es modificando la firma de modo que el código siga haciendo lo mismo de forma un poco distinta, esto sin saber ensamblador puede resultar algo complicado, con otros métodos como el método rit y el método que voy a explicar no necesitan de apenas conocimientos sobre ensamblador y son pura mécanica. La ventaja que aporta este método respecto al rit de hackxcrack es que no representa ningún problema que la firma esté en una parte encriptada del código, o en alguna parte en la que introducir código directamente represente un problema para el funcionamiento del programa. Además a diferencia del rit al no tener que interpretar la instrucción correspondiente a cierto punto de la firma se puede automatizar fácilmente.

El Método MEEPA

La mayoría de antivirus, como el kaspersky cuando se le pide que analice la memoria no está realmente buscando firmas en ella sino que mira los programas en ejecución y analiza en disco sus ejecutables y librerias cargadas.
Entonces que pasaría si en disco no existe la firma pero en memoria si?
Que el virus no seria detectado y funcionaria perfectamente.
Por lo tanto lo que haremos será:
1-Modificaremos un byte de la firma en disco para que el antivirus no detecte el troyano.
2-Crearemos espacio en el exe para introducir nuestro código.

3-Cambiaremos el punto de entrada del exe para que inicialmente se ejecute nuestro código.
4-Desde nuestro código cambiaremos EN MEMORIA el byte que habíamos modificado por su valor original.
5-Saltaremos desde nuestro código al punto de entrada real del programa.

Herramientas Necesarias

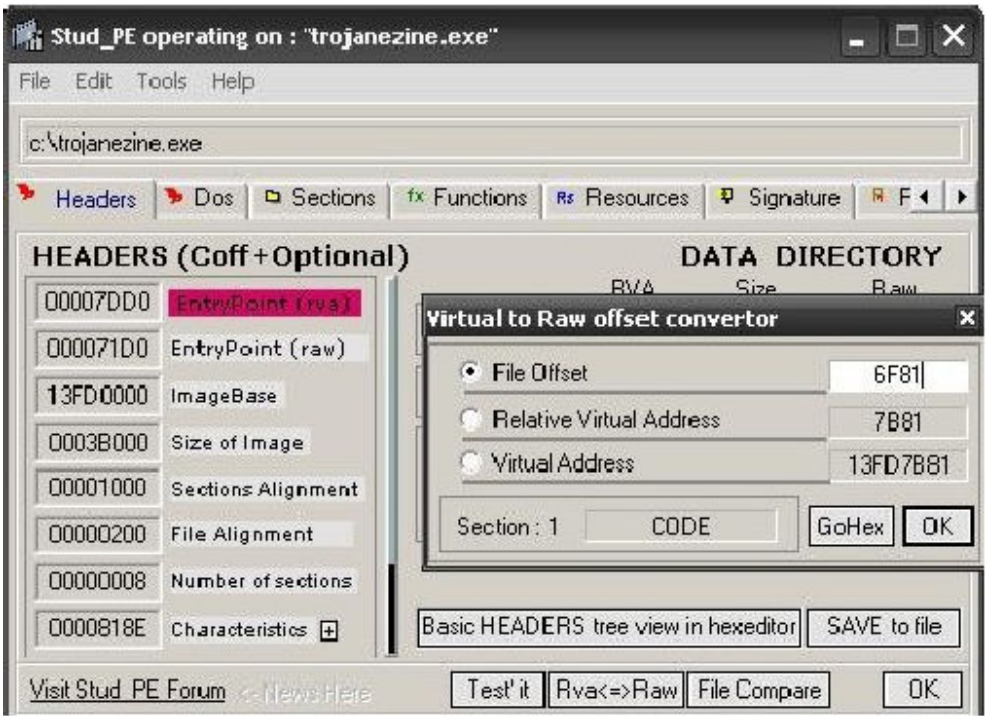
-El troyano que vamos a modificar.
Será el server del nuclearrat 1.0 configurado para que conecte a 127.0.0.1 y se instale en c:\windows\trojanezine.
-El studpe para modificar la cabecera pe32 del exe.
-Un editor hexadecimal.
-Partimos de la base que la firma de kaspersky para este troyano es desde 6f81 hasta aproximadamente 7147.

Junto con la ezine tienes el troyano para testear y el studpe, están los dos encriptados con contraseña ya que el nuclearrat lo detectarán todos los antivirus y el stud_pe puede que algunos lo detecten como hack tool. La contraseña para descomprimir el paquete es "método meepa"
Editores hexadecimales hay miles por internet, yo aconsejo hdd hex editor, no está nada mal y tiene una versión gratuita.

Recolectando Informacion

PE32 significa portable executable y fue diseñado por Microsoft para tener el mismo formato de archivos ejecutables para todos los windows. Nosotros no necesitamos conocer mucho sobre él, lo que nos interesa es modificarlo para poder añadir código al ejecutable y cambiar el punto de entrada de este.

Con el troyano cargado en el studpe vemos toda la información de la cabecera pe32 de nuestro troyano. Cogemos el imagebase(13fd0000) y lo sumamos al entrypoint rva(7dd0) nos dará la dirección absoluta una vez cargado en memoria del punto de entrada del programa (13fd7dd0)
Ahora le damos a rva<=>raw e introducimos en file offset el inicio de la firma (6f81), debajo nos devolverá la dirección virtual de ese punto de la firma (13fd7b81)

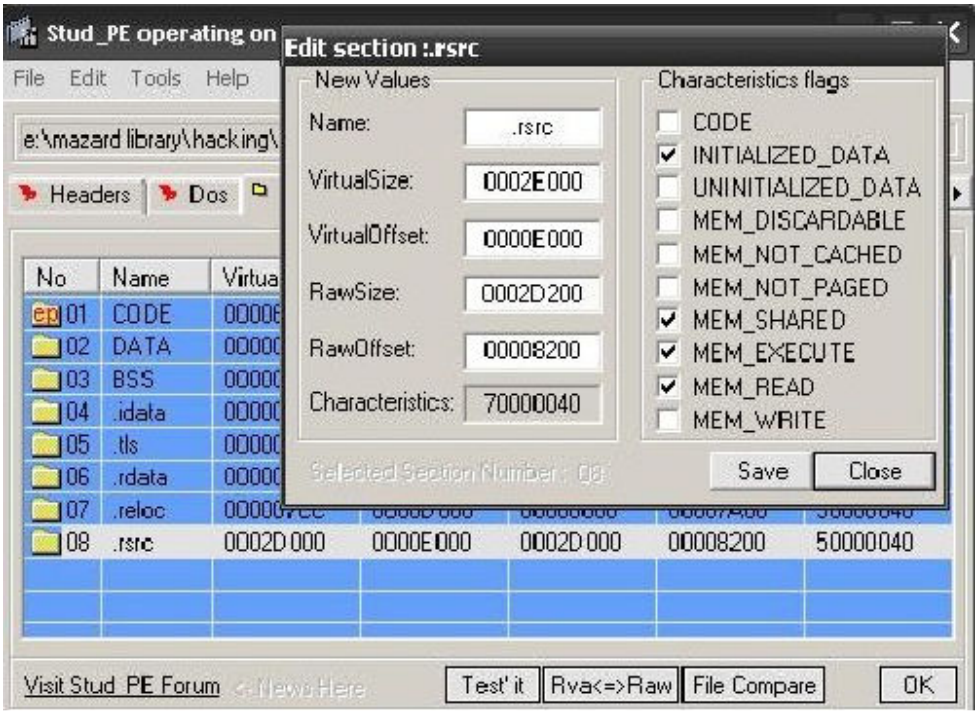


Mas adelante veremos para que queremos esta información.

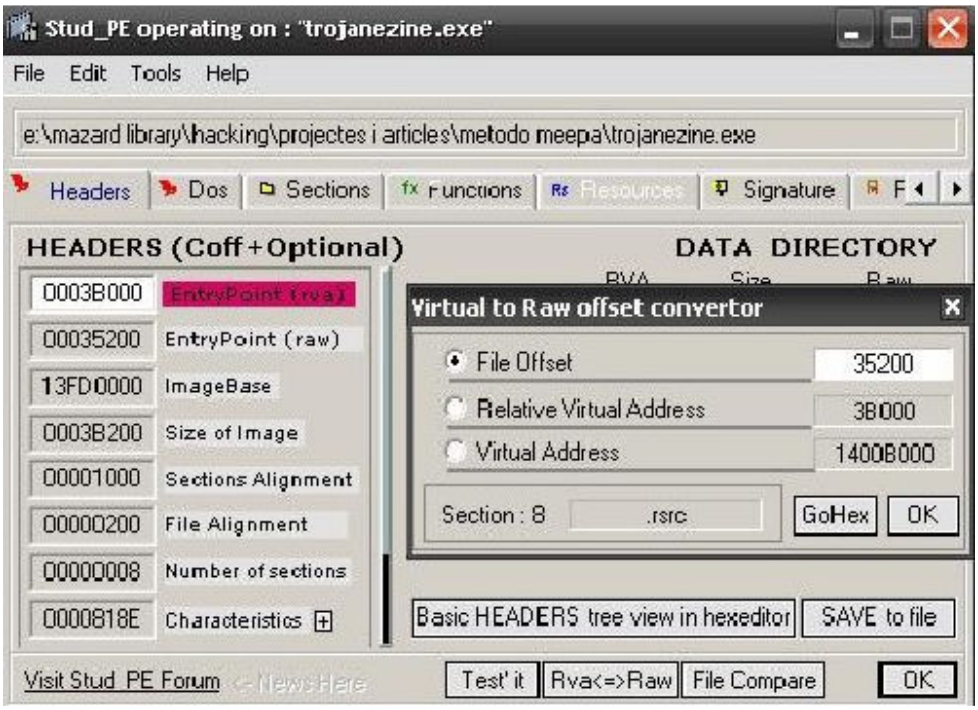
Modificando el PE32

Crear espacio en el exe para nuestro código no es absolutamente necesario, podriamos utilizar espacios vacíos por la alineación del ejecutable. Para los que conozcan un poco el formato PE sería a partir del pointertorawdata+virtualsize y tendríamos un espacio libre de virtualsize-sizeofrawdata, pero es posible que no exista este espacio y el proposito del artículo es que el método sea genérico. Otra posibilidad sería crear una nueva sección para nuestro código pero en algunos casos podría darnos problemas y nos obligaría a reajustar casi todo el archivo, así que vamos a lo mas fácil, ampliaremos el espacio de la ultima sección del ejecutable, emplazando nuestro código justo al final del exe.
Vamos a sections y vemos que en nuestro caso concreto la última sección es ".rsrc" le damos clic derecho "edit header" sumamos el raw offset y el raw size y nos dará 35200, esto es el punto en el que empezará nuestro código, si cargamos el programa con un editor hexadecimal veremos que es justo en el final, si no fuera así significaría que el troyano añade los datos de configuración en el mismo archivo pero fuera del exe, por lo que deberíamos insertar el código que veremos mas adelante justo en este punto dejando lo que ya había en el final.

En raw size le sumaremos 200 (512 bytes en hexadecimal) y en el caso de que el raw size sea mas grande que el virtual size le sumaremos a este ultimo 1000. Decir que el raw size y el virtual size no pueden ser cualquier cosa, tienen que ser multiplos de la alineación del archivo y la sección. Pero nosotros sea cual sea el troyano objetivo con ampliar 512bytes tal y como lo montamos tendremos mas que suficiente. También le damos permisos de ejecución a la sección para que se pueda lanzar nuestro código. Quedaría así:



Ahora hacemos click en Rva<=>raw y en file offset ponemos el inicio de nuestro código 35200 nos dará la dirección virtual relativa (a image base) y lo introducimos en el entrypoint(rva) de este modo conseguimos que lo primero que se ejecute al lanzar el exe sea el trozo que hemos ampliado de la sección (nuestro código). Dado que hemos aumentado el tamaño de una sección en 512 bytes (200) tenemos que añadirlo al tamaño total del exe por lo que size of image quedará en 3B200.
Pulsamos "save to file" para guardar los cambios, quedaría así:



Por último le vamos a dar permisos de escritura en la sección de codigo, vamos de nuevo a sections, clic derecho a la sección “code”, “edit headers” y seleccionamos “mem_write”:
Esto lo hacemos para que se nos permita cuando este el programa cargado en memoria escribir en el punto modificado de la firma su valor real.

Escribiendo nuestras 3 lineas de código

Que hemos hecho hasta ahora?
1-Hemos añadido espacio en la última sección del pe (espacio al final del exe)
2-Hemos cambiado el punto de entrada del programa para que lo primero que se ejecute sea lo que haya en el espacio que hemos añadido
3-Hemos recolectado información necesaria:
  Offset en disco del byte de la firma: 6f81
  Direccion virtual del byte de la firma: 13FD7B81
  Antigua Direccion virtual de entrada al programa: 13fd7dd0

Ya tenemos el exe preparado y la información necesaria. Ahora vamos al tajo, abre el archivo con tu editor hexadecimal.
Nos vamos a la dirección 6f81 que es el punto de la firma a modificar, nos apuntamos el valor que hay ahí (53) y lo sobrescribimos con cualquier cosa (11 mismo). En este punto el programa ya no es detectado, pero petará por dos motivos:
1-Hemos modificado el byte de la firma aleatoriamente y por lo tanto nos hemos cargado el programa.
2-El punto de entrada al programa va a un sitio donde no hay código.

Solucionemos los problemas creando el código que reestablecerá el byte modificado:

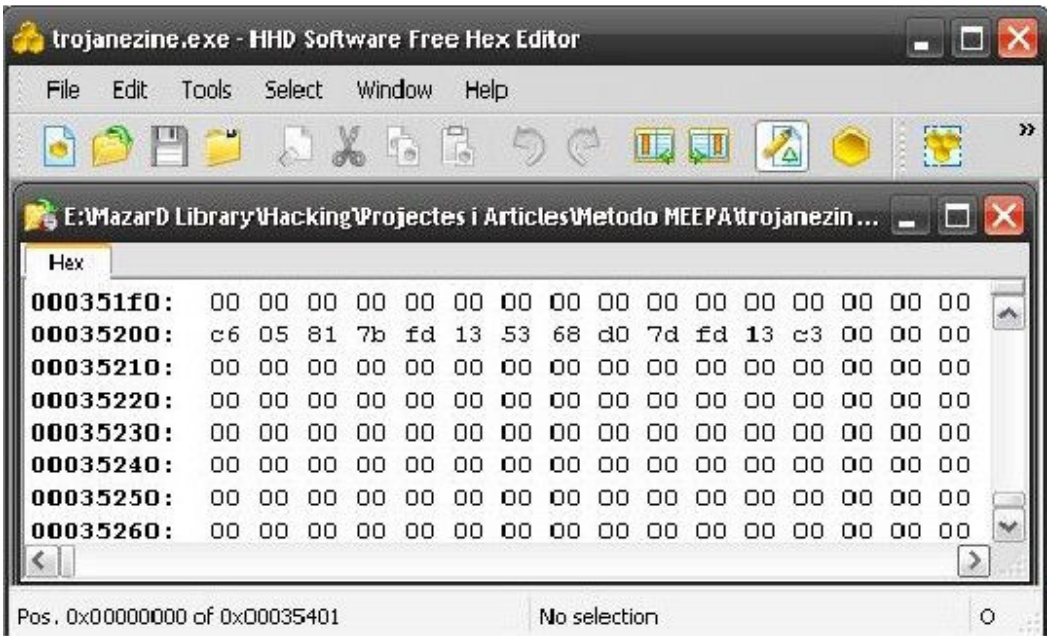
mov byte ptr [13fd7b81],53
Con esto se copiará el byte 53 a la posición de memoria que en el archivo habiamos puesto 11.
push 13fd7dd0
ret
Con estas dos instrucciones saltaremos al punto de entrada real del programa (una envía la dirección a la pila y la siguiente coge el último valor puesto en la pila y "salta" a él. No utilizamos el jmp porque podría darnos problemas con la dirección del salto.

La representación hexadecimal de las instrucciones anteriores sería:
c605 817bfd13 53 -->c605 representa "mov byte ptr" el siguiente es la dirección y el siguiente el valor que introducimos

68 d07dfd13-->68 representa "push" y el siguiente es el valor que introducimos
c3-->c3 representa ret

Si te fijas las direcciones están al revés cogidas de dos en dos, esto es debido al endian, tampoco entraremos en esto, con que sepas que las direcciones se representan así es suficiente:
13 fd 7b 81 => 81 7b fd 13
13 fd 7d d0 => d0 7d fd 13
3 aa 42 12 => 12 42 aa 03

Ahora vamos a introducir este código con el editor hexadecimal, nos vamos al final del ejecutable (35200) e insertamos el código anterior. También tenemos que recordar que habíamos añadido 512bytes (200) y aunque solo rellenemos unos cuantos estos deben existir fisicamente en el archivo, así que hasta 35400 insertamos nulos.



Guardamos y listo. Troyano indetectable y 100% funcional.
Autor: **MazarD**

Manual Indetectar servers

Herramientas:
http://foro.portalhacker.net/index.php/board,80.0.html

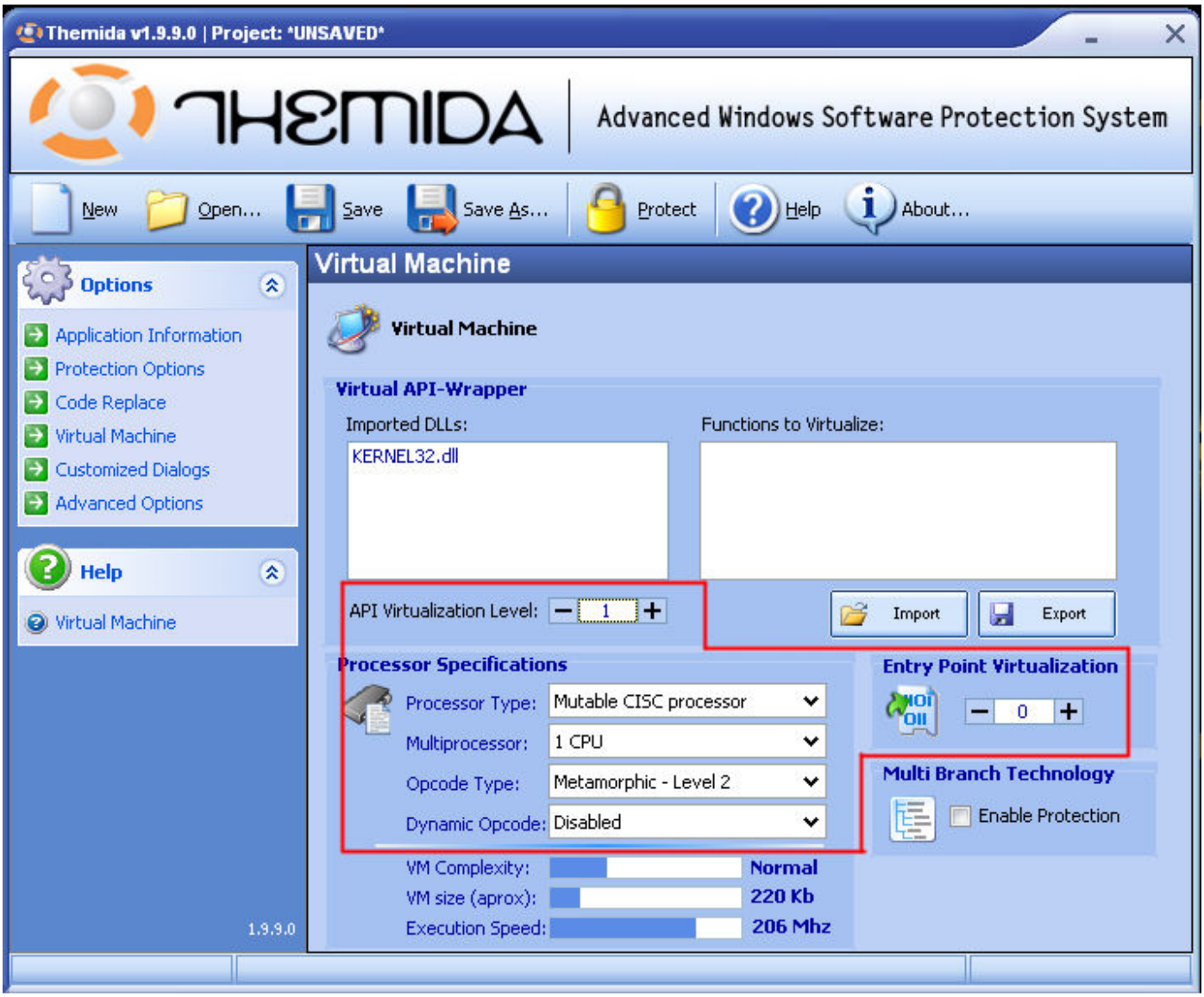
Open Crypter(solo para el posion):
http://rapidshare.com/files/134133101/Open_Crypter__diciembreII_.rar.html

Está probado con los servers del Bifrost 1.2.1 y el poison 2.3.0 en el poison antes que pasarle el themida tienen que pasarle un crypter al server por ejemplo el Open crypter,
despues siguen el proceso..

Advanced Options

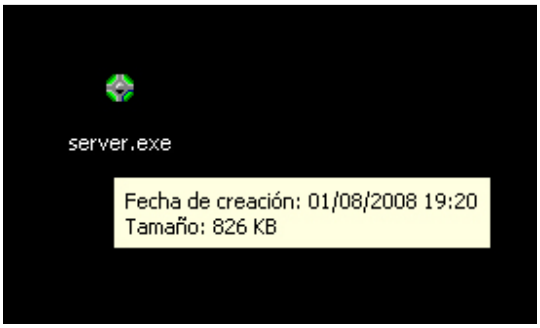
en **Last Section Name**: ponen lo que quieran.

Virtual Machine lo dejamos como en la imagen



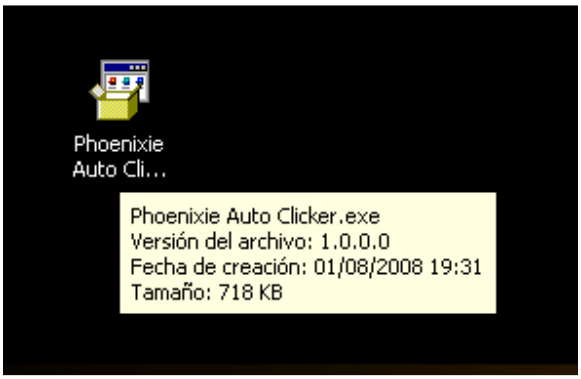
Protection Options lo dejamos así

y le damos a **Protect** para terminar

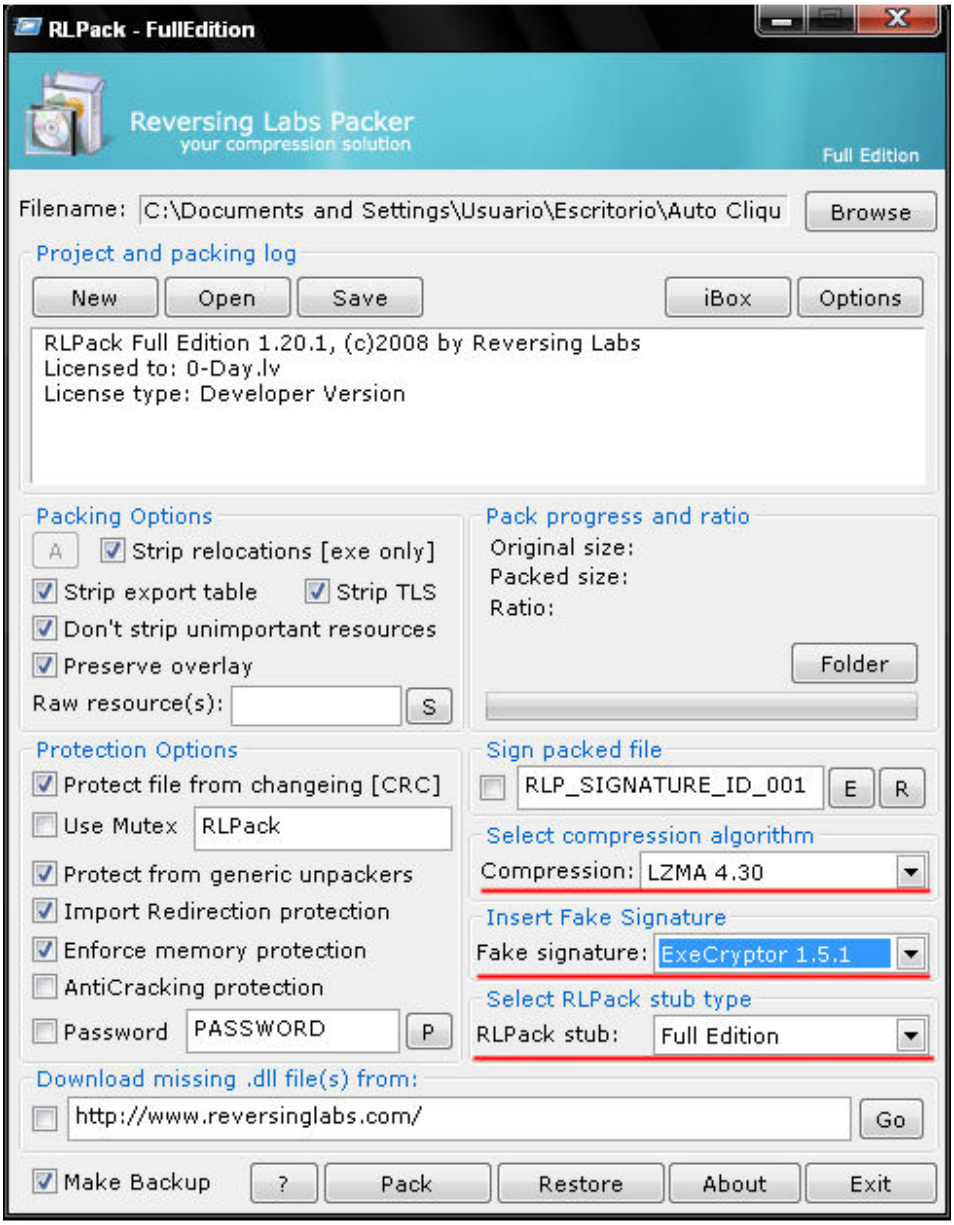


Ahora le pasan el Iexpress, que mas arriba esta explicado.

Ahora lo tienen que unir con algun binder o con el mismo iexpress para despues poder pasarle el rlpacker sino no podran pasarlo y les tirará eorres.En mi caso lo voy a unir a un Autoclicker
este será el resultado

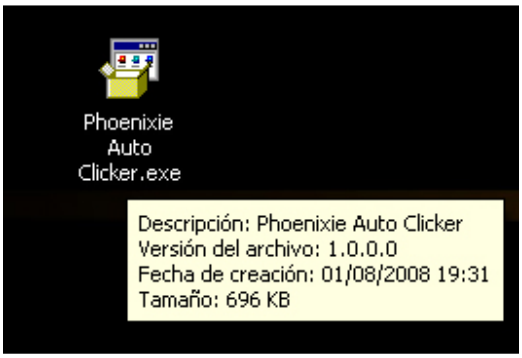


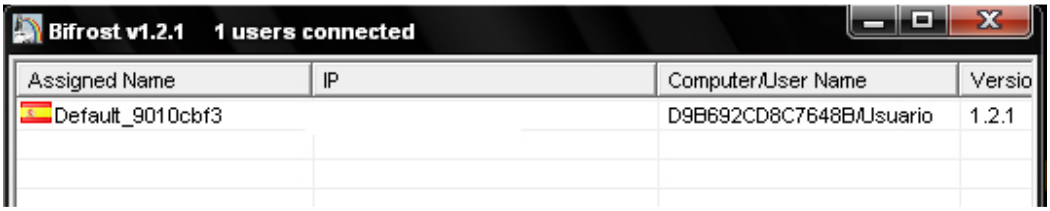
despues ejecutamos el RLPacker y vamos a ***Browse*** y buscan el archivo

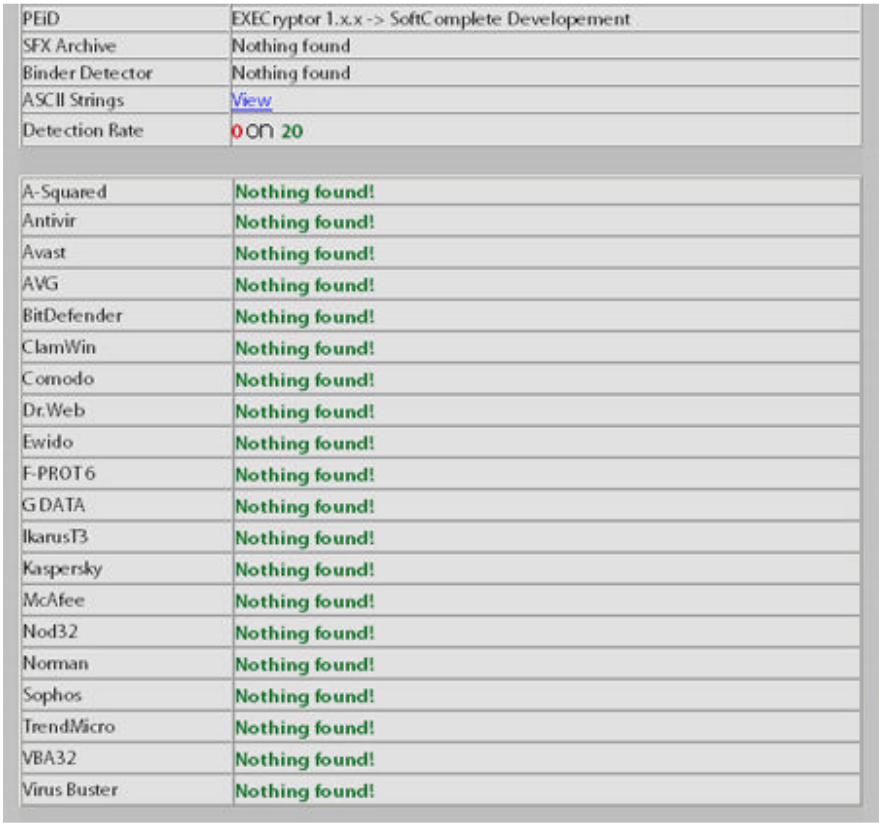


marcan las casillas como en la imágen y lo que esta marcado en rojo.

NOTA: Les dirá algo del "Strip TLS" le dicen que NO.
NOTA2: Cuando termine el programa le dicen que NO sino se ejecutará y se infectarán ustedes mismos.







PEiD	EXECryptor 1.x.x -> SoftComplete Developement
SFX Archive	Nothing found
Binder Detector	Nothing found
ASCII Strings	View
Detection Rate	0 on 20

A-Squared	Nothing found!
Antivir	Nothing found!
Avast	Nothing found!
AVG	Nothing found!
BitDefender	Nothing found!
ClamWin	Nothing found!
Comodo	Nothing found!
Dr.Web	Nothing found!
Ewido	Nothing found!
F-PROT6	Nothing found!
G DATA	Nothing found!
IkarusT3	Nothing found!
Kaspersky	Nothing found!
McAfee	Nothing found!
Nod32	Nothing found!
Norman	Nothing found!
Sophos	Nothing found!
TrendMicro	Nothing found!
VBA32	Nothing found!
Virus Buster	Nothing found!

by .Huêx ***si quieren copiar el manual respeten la fuente. Para portalhacker***

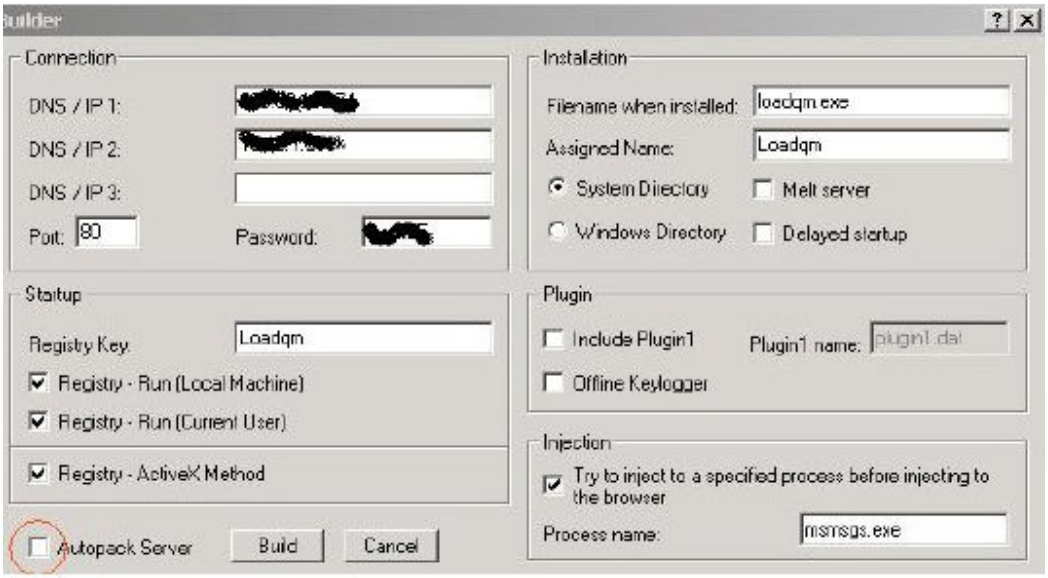
METODO ANTRAX II

Este método lo hice hace bastante tiempo con la primera versión del bifrost, y aun funciona.

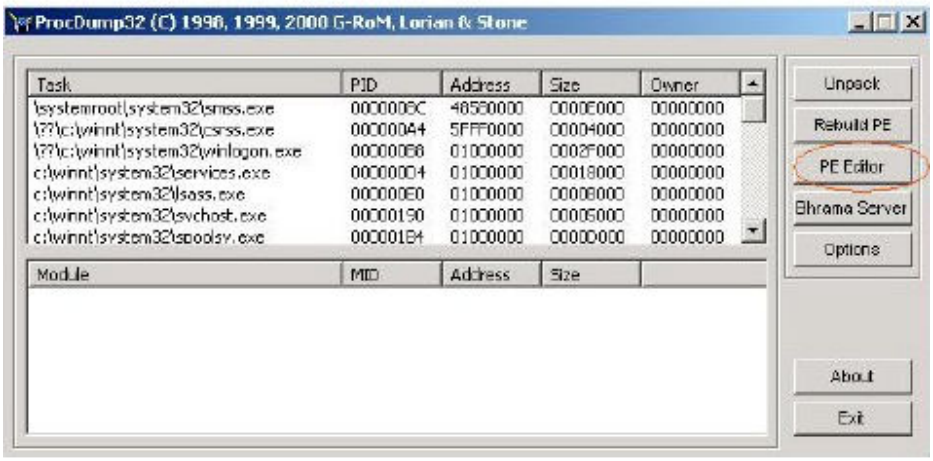
Herramientas:

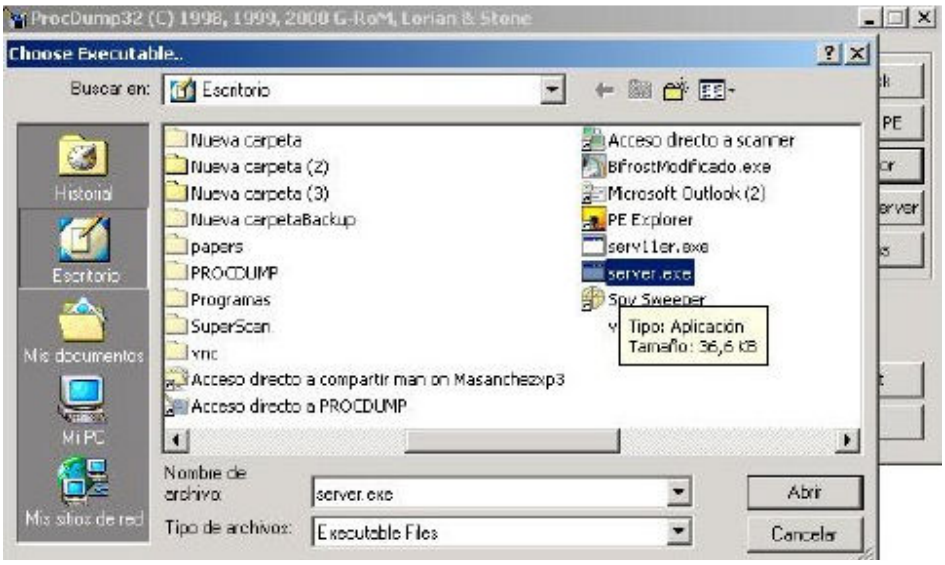
- **PROCDUMP**
- **UPX**

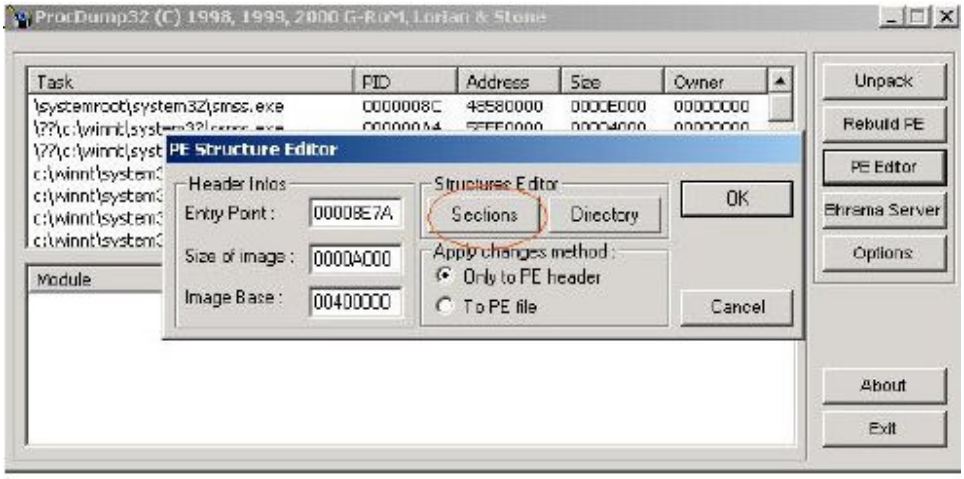
1.- Crear el Server:



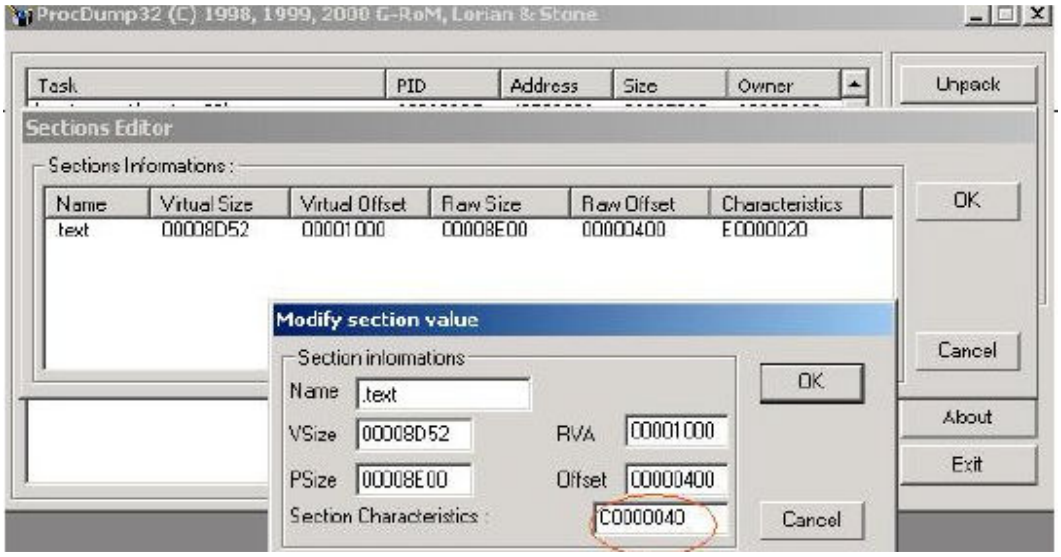
En este caso la compresion no esta activada (Autopack Server), por que despues lo vamos a comprimir con el upx, , mas adelante voy a explicar esa parte.



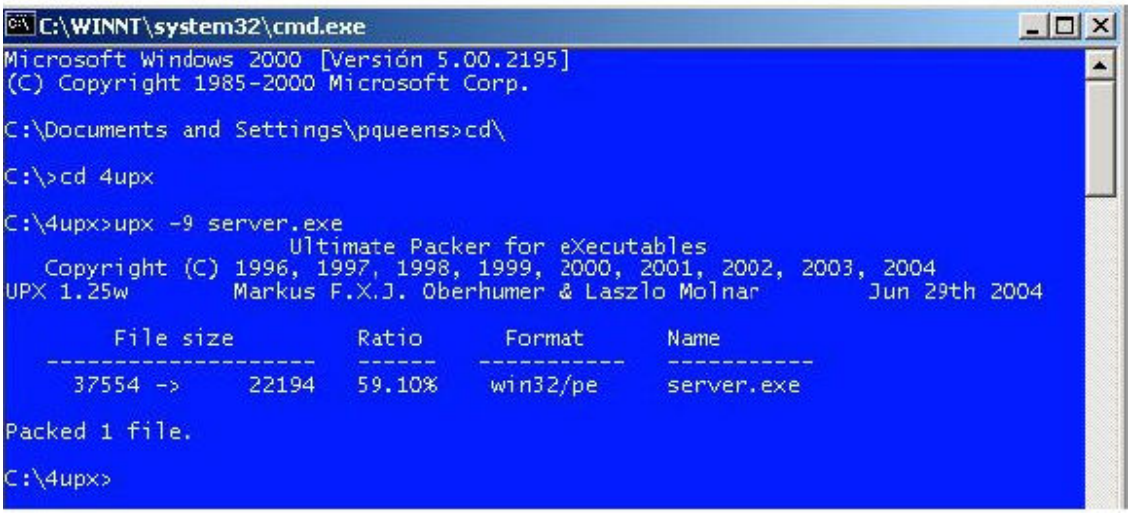




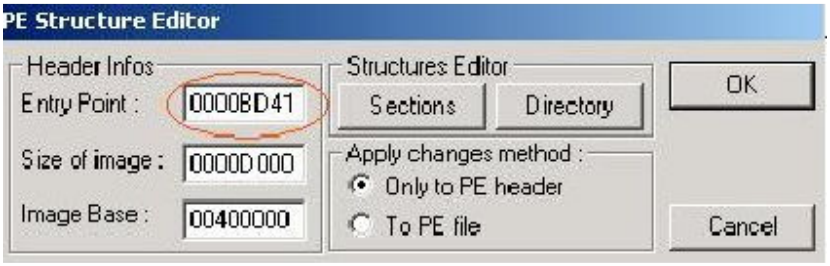
Ahora si entramos a la parte bonita , al momento de darle a Sections nos va a arrojar el Section editor, el cual en la cabecera hay un peculiar numero E0000020, eso nos dice que es ejecutable y que no esta comprimido, toncessss, se lo cambiamos a C0000040, eje, que paso ahí, pues lo estamos poniendo como si estuviera empaquetado



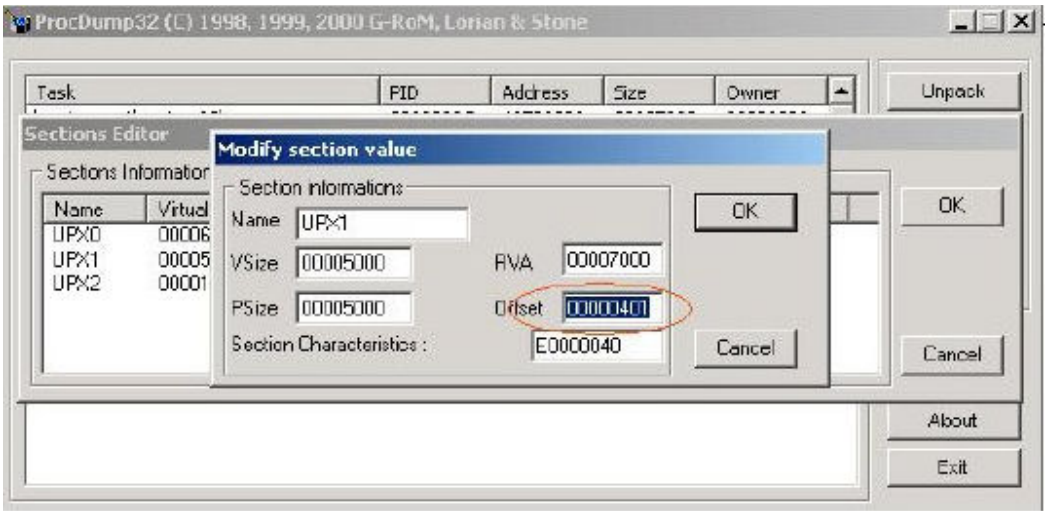
Bueno, le damos ok, ok, ok ,ok a todo, pssss , la huevadita esta a media caña, nos vamos a nuestra carpeta del upx y copiamos el server ya modificado y lo comprimimos con la sentencia c:\upx –9 server.exe y esto nos bota:



Bueno ya lo tenemos apretado de nuevo, entonces , volvemos con nuestro programita especial PROCDUMP y volvemos hacer los pasos anteriores pero, antes que todo modificamos ahora si El Entry Point 0000BD40 en mas 1 , osea 0000BD41



Igual entramos Section como la ves anterior y modificamos el UPX1 click derecho , edit section y modificamos el offset en + 1 , 00000400 en 00000401, le damos ok ok ok ok . etc



Y listo! Tendremos nuestro server indetectable!

Espero que les haya gustado a todos!

Dudas: an7r4x @hotmail.com

Todos los troyanos y cosas de este tuto lo podes encontrar en: www.r00thack.webcindario.com