Metodo XOR by cLaRoScUrO

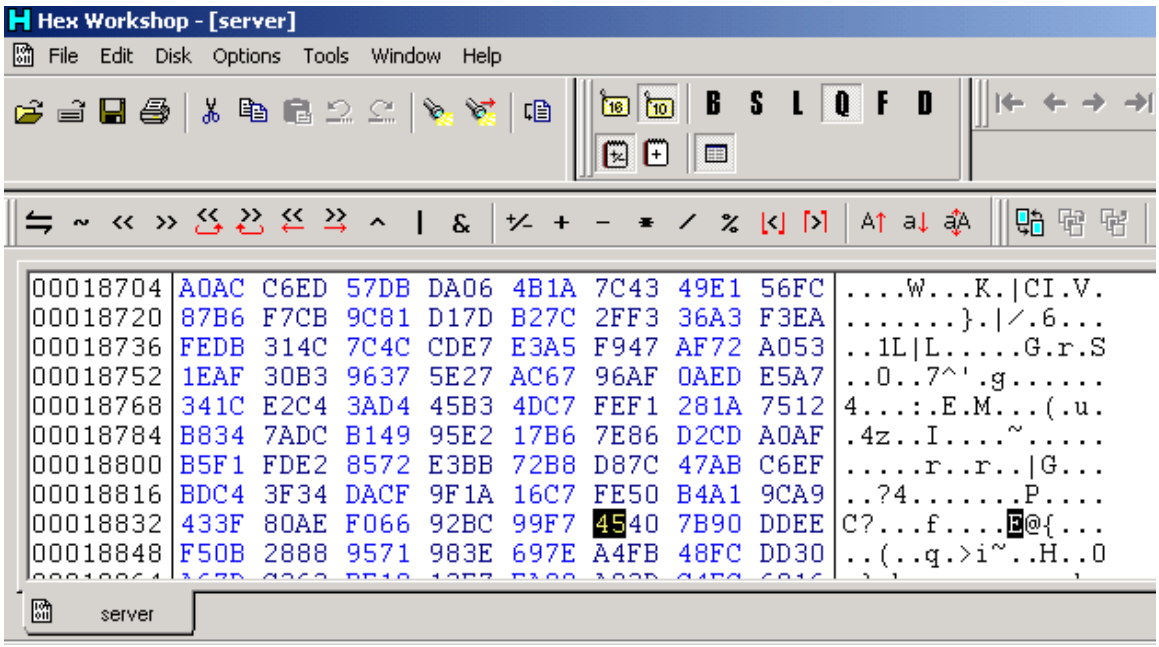
Bueno aqui les enseñare a hacer indetectable su Troyano o Crypter mediante el Metodo XOR, este metodo va muy bien para modificar las firmas pero no muy bien para la Heuristica.
Bueno empezemos, vamos a necesitar estos programas:

***Olly Dbg**

***Hex WorckShop o cualquier editor Hexadecimal**

***Topo**

Bueno les cuento en que consiste este metodo, si abrimos algun server o stub de algun crypter con algun editor Hexadecimal, veremos algo asi:



Ahora suponiendo y aclaro es una supocicion ya que tome una firma al azar y ustedes lo aharan con una que detecte su antivirus o los antivirus, esta claro, bueno suponiendo que la firma detectada sea 45 como muestra la imagen esto es lo que haremos, vamos a INICIO>EJECUTAR: y escribimos "calc" sin las comillas o simplemente abrimos la calculadora de windows :P y la ponemos en Hex y hacemos esta operacion:

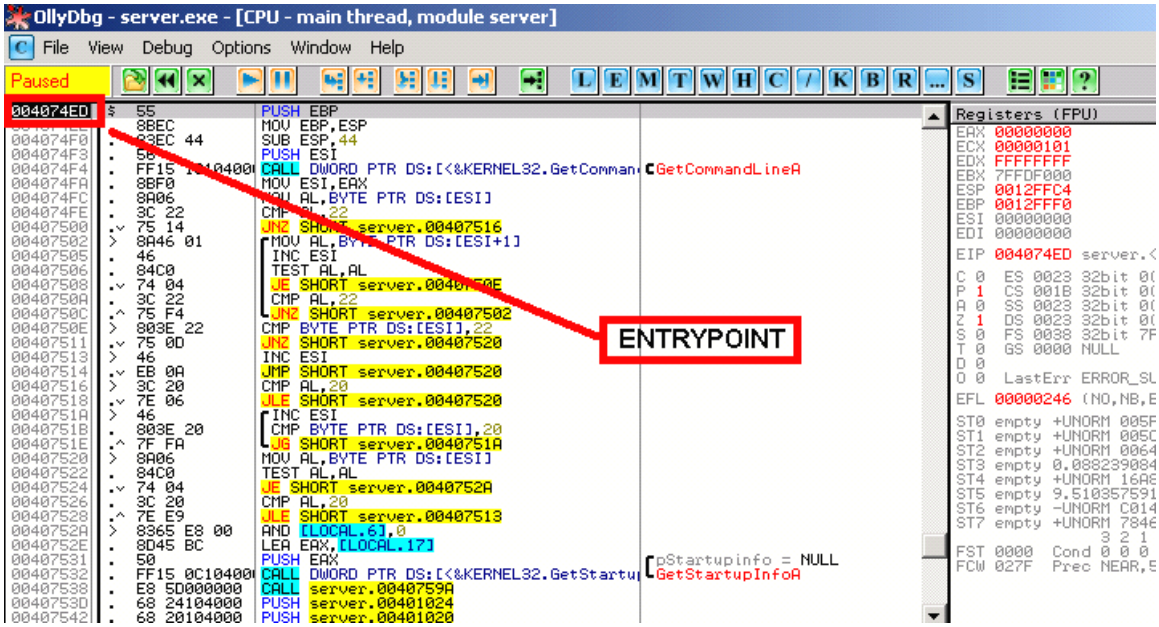
45 XOR 0E = 4B
4B XOR 0E = 45

Se dan cuentan? el XOR es reversible y lo que hara en cambiar la firma detectada asi no lo detectara su antivirus, pero si solo hacemos esto el server o crypter quedara inutilizable, por lo que tendremos que

agregar un pequeño codigo que lo que hara es que al ejecutarse nuestro server en memoria cambia la firma cambiada por la original, espero se me entienda...

Bueno continuamos ya que esto es solo teoria hasta el momento.

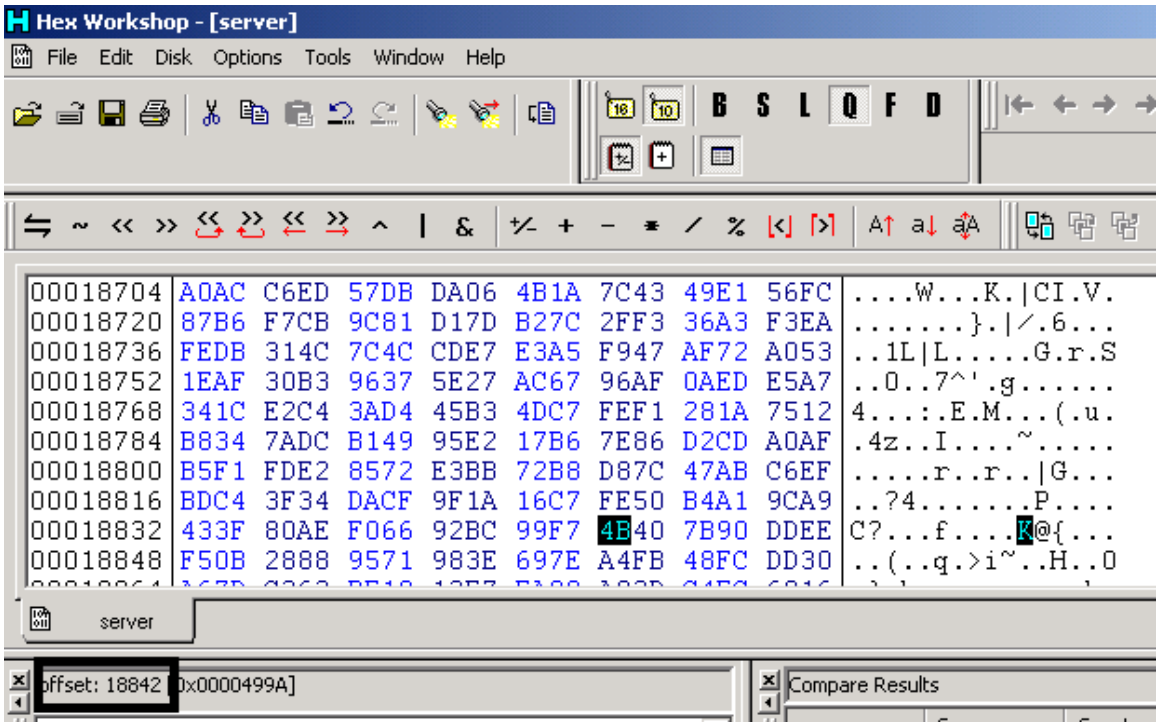
Vamos a nuestro Olly y abrimos nuestro server o stub (para este ejemplo use el server del Bifrost) y anotamos la direccion del entrypoint que la primera que aperece en el Olly tal cual se ve en la imagen, esta la usaremos mas adelante.



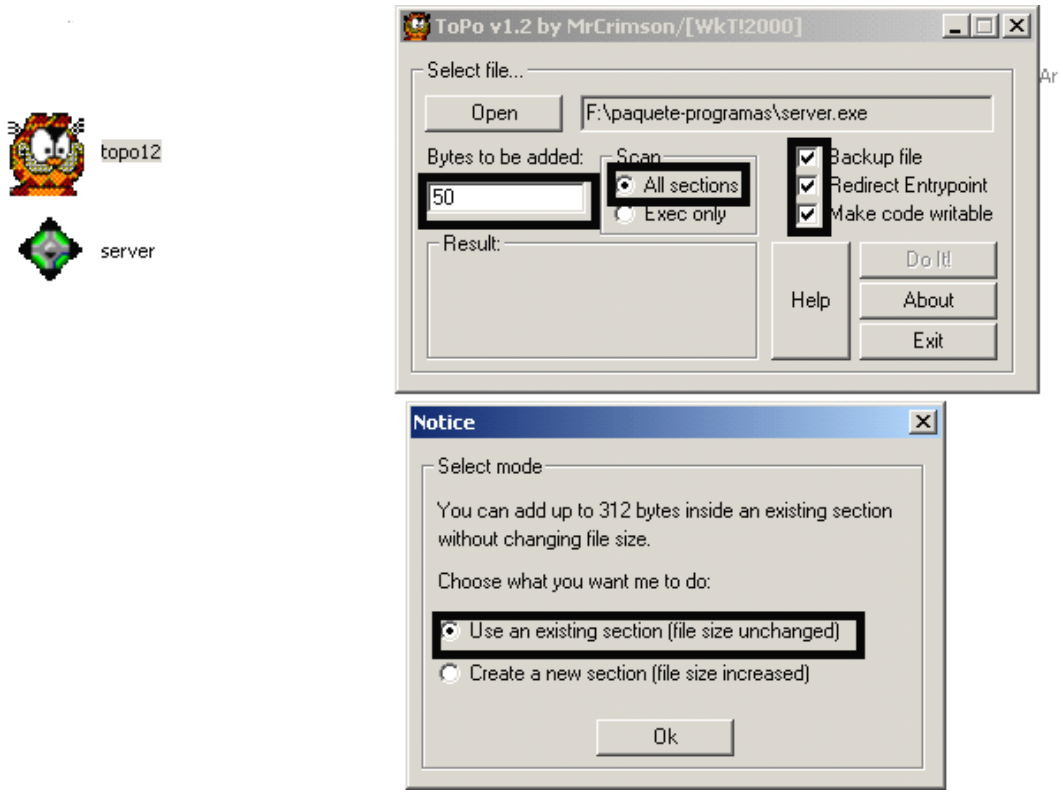
Bien este paso solo era para anotar el Entrypoint ahora continuamos...

Teniendo nuestra firma cercada y como dije suponiendo en mi caso que sea "45" como la imagen y habiendo hecho la operacion en la calculadora la cambiamos por el resultado del XOR.

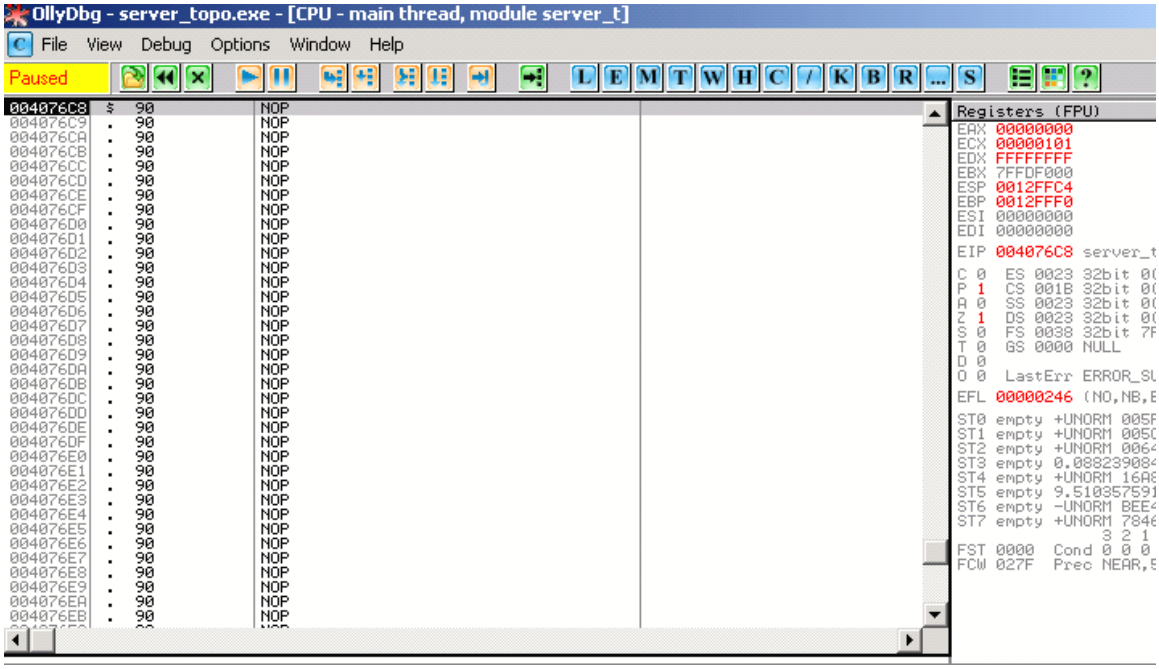
IMPORTANTE: No te olvides anotar el offset donde modificaste la firma ya que lo vamos a necesitar mas adelante.



y guardamos nuestro server o stub sea el caso... bien esto estara inservible asi que tendremos que agregar ese pequeño codigo que les decia anteriormente pero antes debemos hacer un lugar para meter este codigo y que apunte al Entrepoint o inicio de nuestro ejecutable, para ello utilizaremos el Topo, lo abrimos marcamos las opciones como la imagen y le damos a **Do It!**

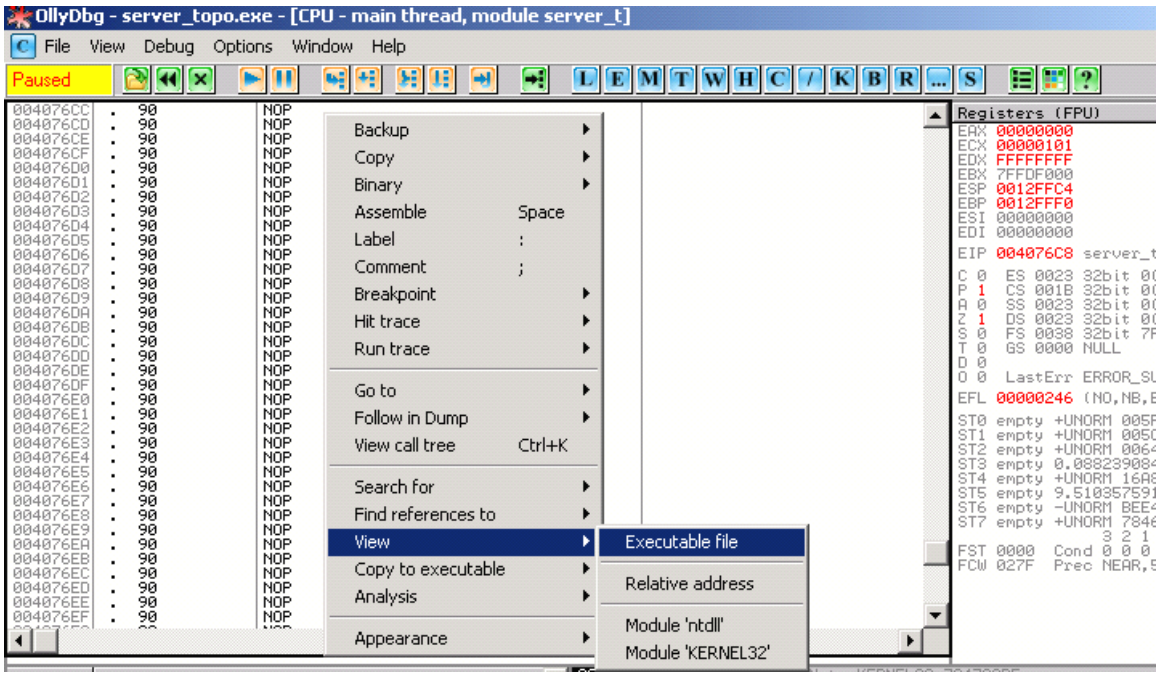


Bueno continuamos ahora vamos a nuestro Olly y abrimos nuestro server ya pasado por el topo y se vera algo asi:

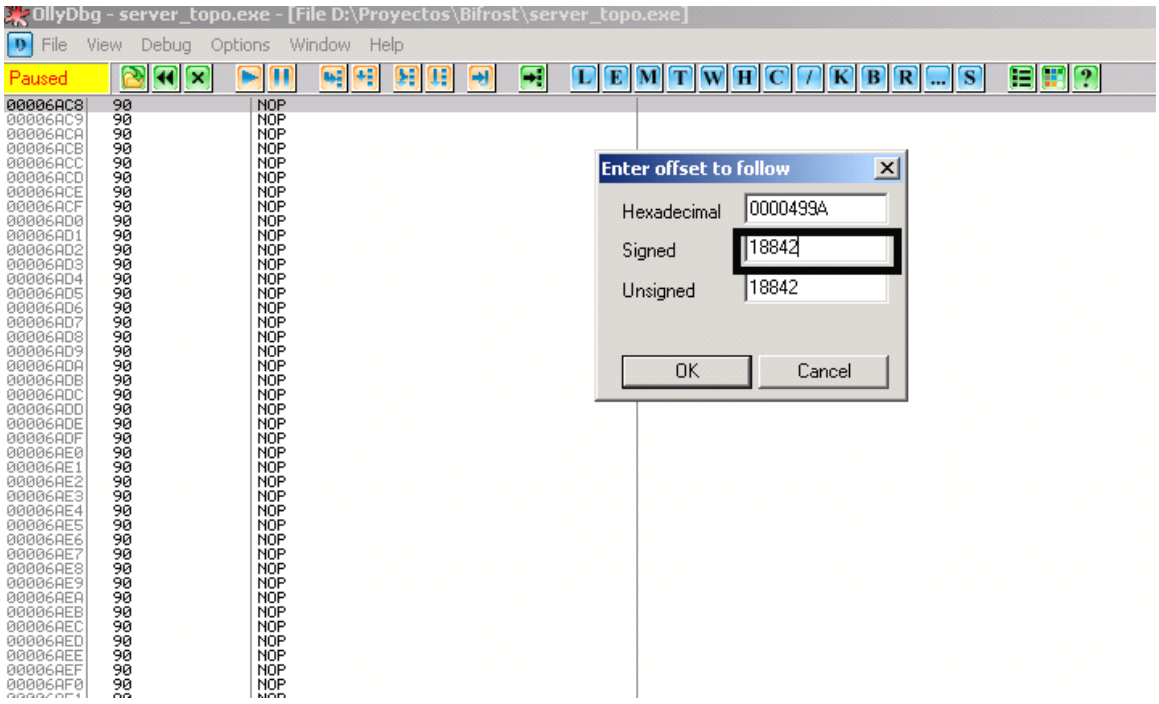


Bien ahora estando aqui hacemos click derecho con el mouse y vamos a **View... Executable file**...

como en la imagen:

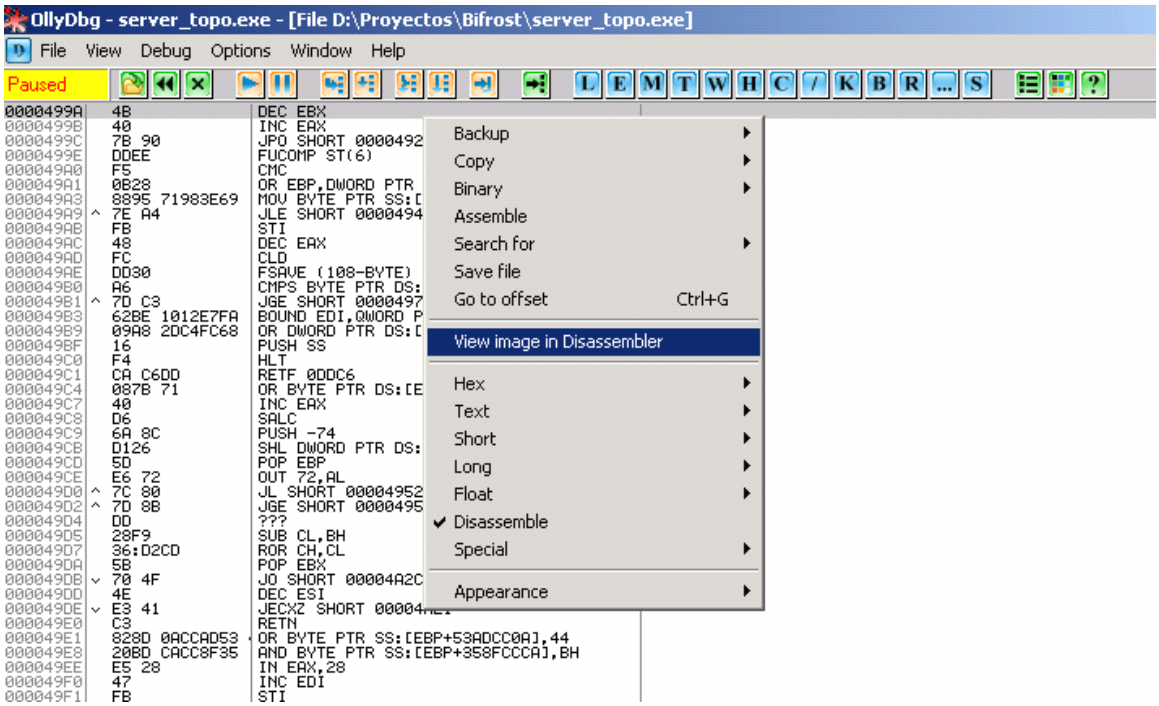


Nos encontramos con otra pantalla, donde apretaremos **Control + G** y en cuadro que nos sale metemos el offset donde modificamos la firma (que le dije antes que anotaran) y le damos OK

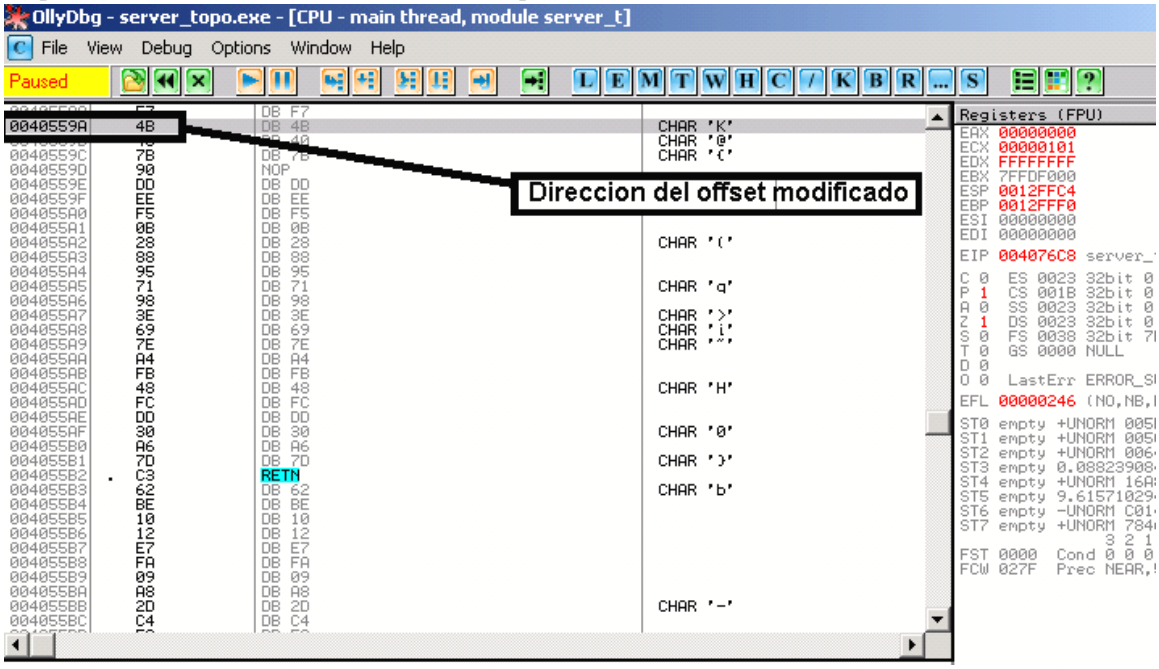


Ahora ya nos encontramos en el offset que habiamos modificado como podran ver... y ahora lo

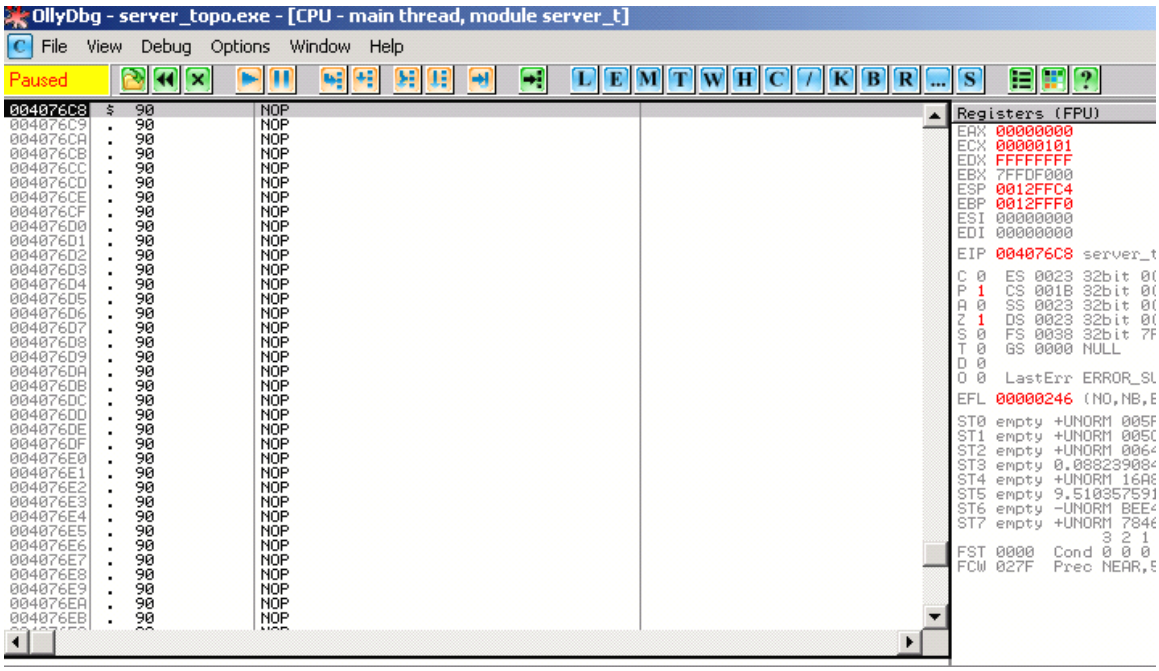
hacemos es teniendo seleccionado el offset al que nos trasladamos es click derecho del mouse y vamos a **View image in Disassembler.**



Nos lleva otra vez a la primer pantalla del Olly en la direccion donde modificamos nuestro offset, aqui lo que hacemos es anotar la direccion de este que en mi caso es **0040559A.**



Vamos que ya casi terminamos!!! XD ahora cerramos y volvemos a abrir nuestro server (el que pasamos por el topo claro) o le damos en el Olly al botoncito verde con dos flechitas << o de retroceder y volvemos a la primer pantalla...



Bien ya solo nos queda meter nuestro pedazito que es este

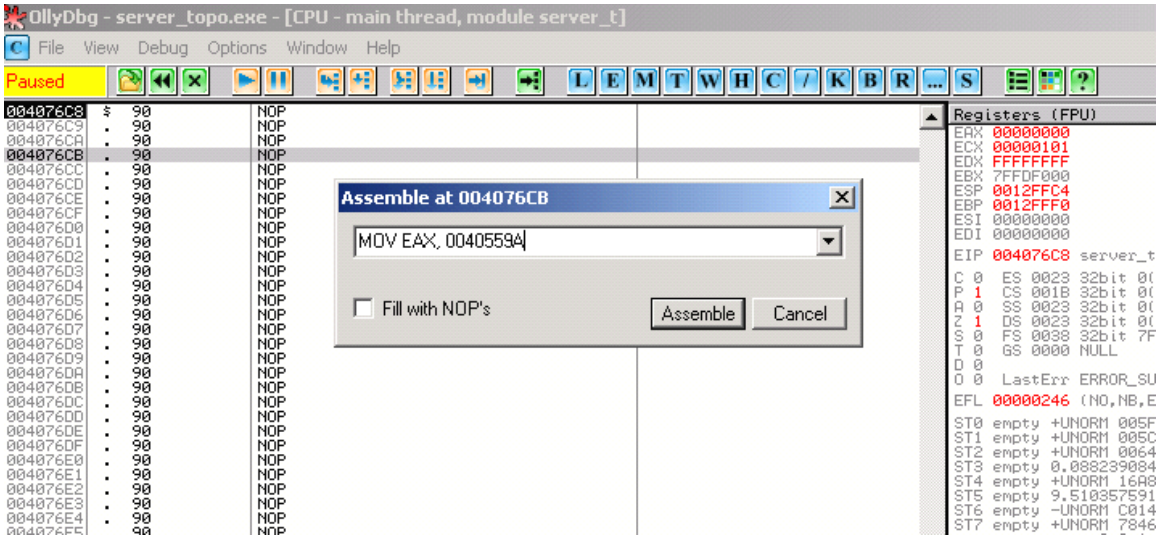
MOV EAX,0040559A

XOR BYTE PTR DS:[EAX],0E

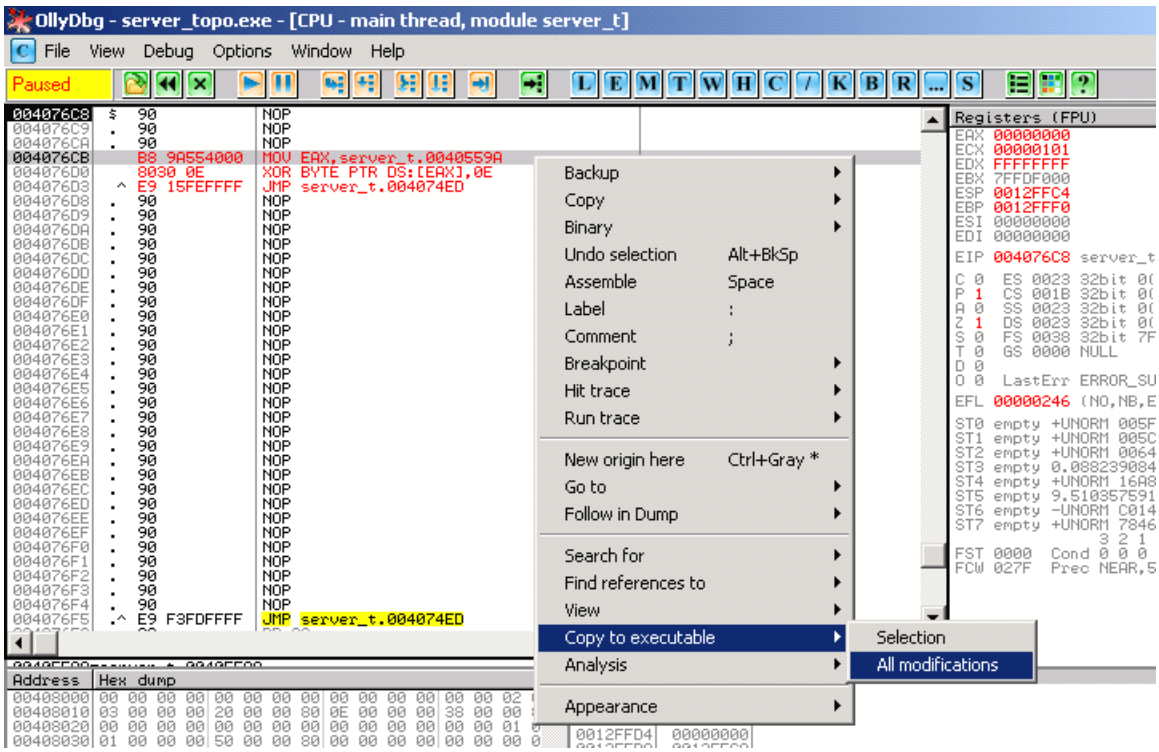
JMP 004074ED

Bien este codigo lo que hara es, la primer linea guardara la posicion de la firma que modificamos en el registro, la segunda linea aplicara el XOR como lo habiamoes hecho en la calculadora y la ultima linea hace un salto a donde comienza nuestro ejecutable o sea el Entrypoint.

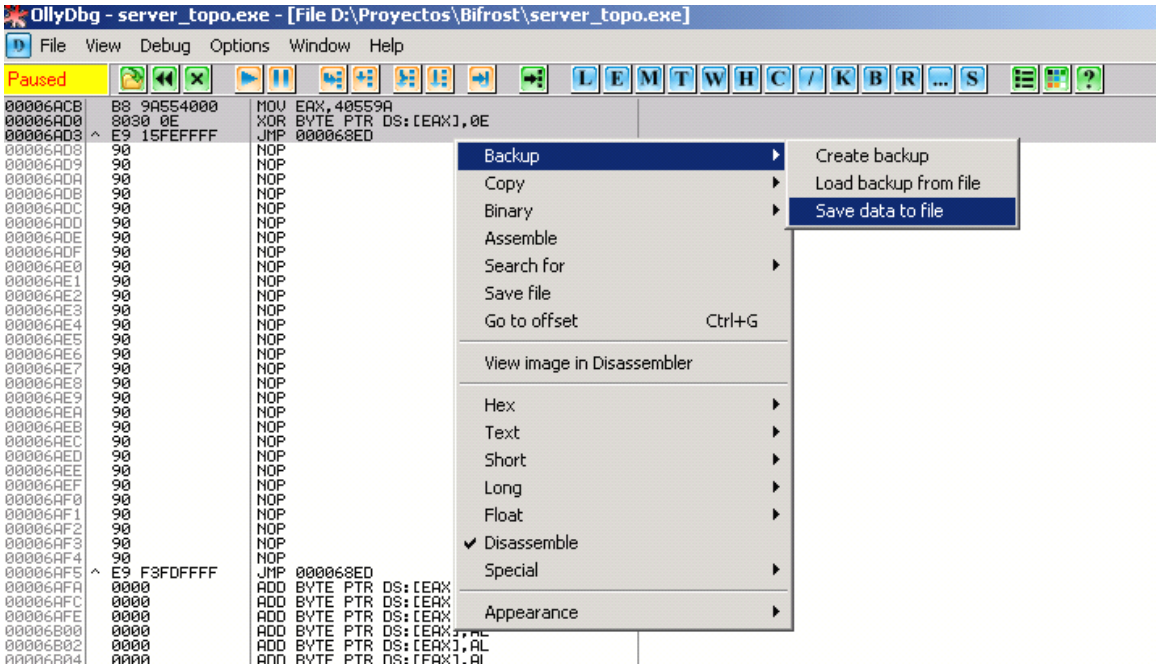
Bien para insertar nuestro codigo hacemos click derecho sobre alguno de los NOP que tenemos y vamos donde dice **Assemble** y escribimos la primer linea y le damos en el boton **Assemble** y hacemos lo mismo con las otras dos lineas.



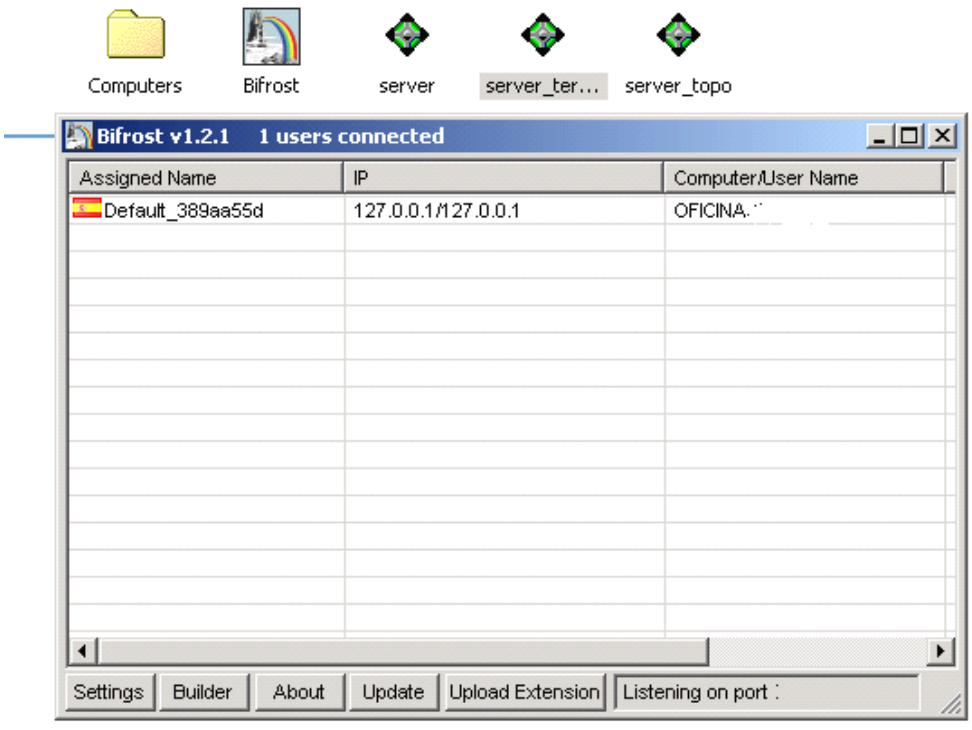
Una vez que hallamos inseratado todo el codigo ya solo nos queda guardar nuestra aplicacion, para ello nos posicionamos sobre alguna de las modificaciones que hicimos y hacemos click derecho del mouse, vamos **Copy to executable, All modifications** y en la ventanita que nos sale **Copy all...**



Y en la siguiente pantalla otra vez click derecho del mouse, **Backup, Save to data to file..** y lo guardamos con el nombre que queramos...



Y ya terminamos... no fue tan dificil no? ahora probar que funciona...



Bueno como ven funciona, no sera indetectable a algun antivirus porq recuerden que tome una firma al azar, no una que detectara algun antivirus.

Bueno espero les sea util y sepan disculpar errores si los hay, este tutorial lo hice basandome en el tuto de leos_79 Hacer indetectable troyano (metodo XOR) posteado en Foro.ElHacker.net

saludos y hasta la proxima.

Hecho pura y exclusivamente para PortalHacker.net si queres copiar este tutorial respeta las fuentes y autores.

by cLaRoScUrO