&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&

& Tutorial de como modificar los crypters hecho por cLaRoScUrO. &
& 23 de Enero de 2009 &
& &

&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&

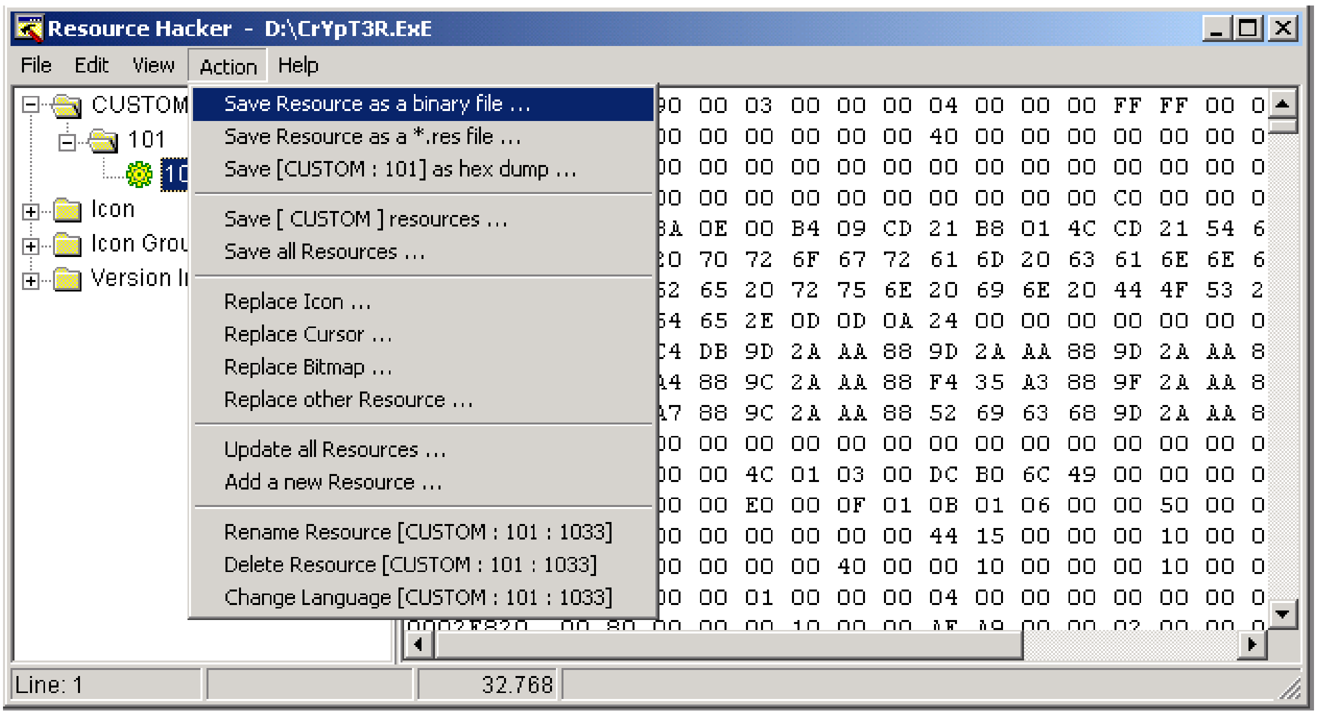
Bueno en vista de que todos quieren tener su troyano indetectable pero los crypters posteados en el foro duran dias y a veces horas les voy a enseñar o tratar al menos como modificar un crypter para que sea indetectable.. . Bueno manos a la obra...

Las herramientas que necesitaremos seran:

*Un Crypter para este tutorial vamos a usar este "CrYpT3R" (Crypter and Binder)
*HexWorkShop
*Olly DBG
*ResHack
*SignatureZero (o cualquier herramienta para buscar las firmas que detecta el antivirus)
*Ganas y Paciencia Tongue

Descargar: PACK_PROGRAMAS
Pass: remoteexecution.com

Bueno para empezar vamos al ResHack y abrimos nuestro crypter... y vamos a retirar nuestro stub tal como muestra la imagen para empezar a hacer las modificaciones ...vamos a Action/Save Resource as a binary file... y lo guardamos con el nombre que queramos.



Despues vamos a hacer un escaneo en NoVirusThanks. org (siempre marcando la opcion de no distribuir muestras) para ver cuantos Avs no los detectan y para ver que Avs necesitaremos. ..

Detection rate: 9 on 24

Detections

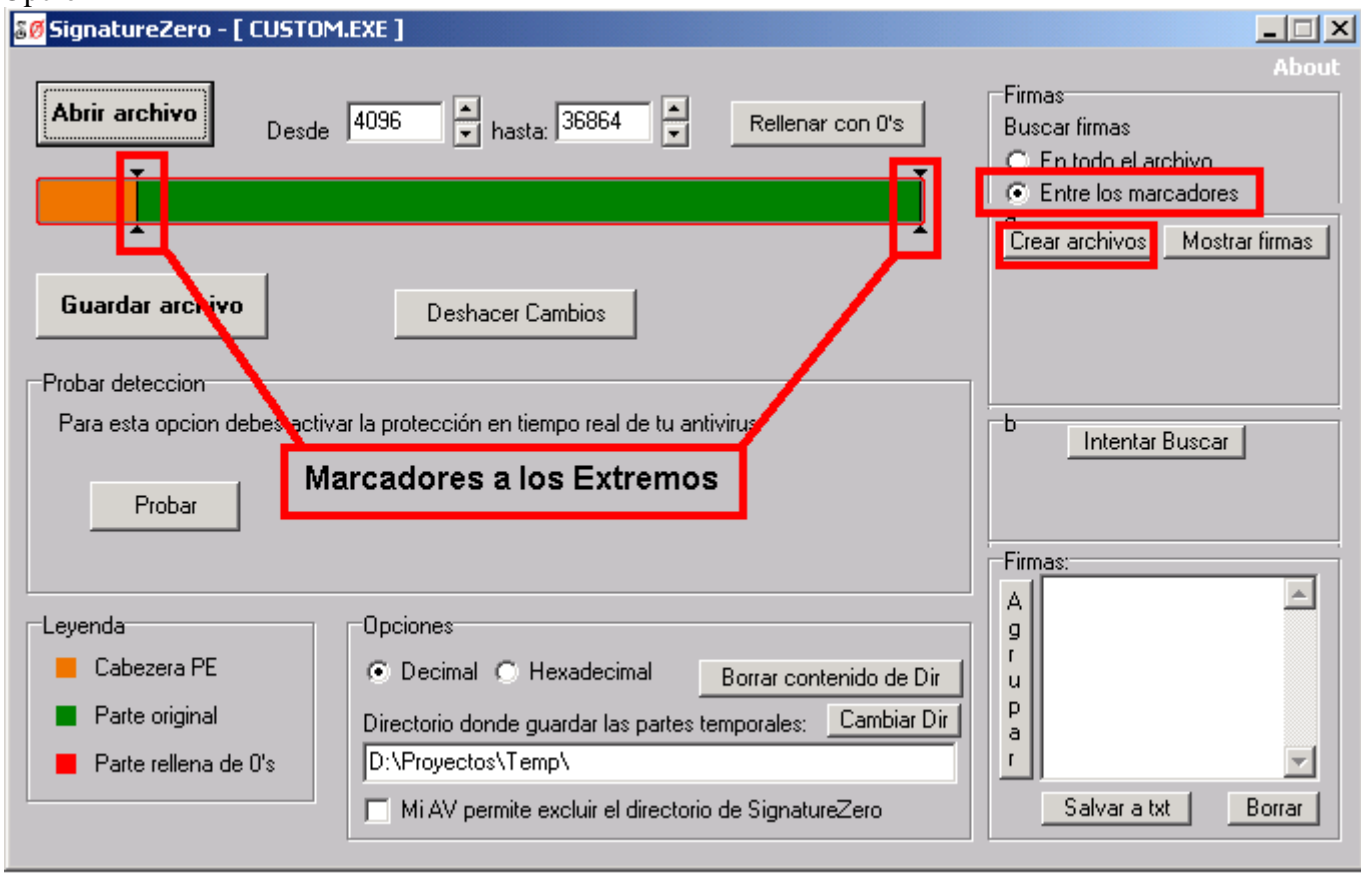
a-squared - Backdoor.Win32 .Bifrose!IK
Avira AntiVir - Nothing found!
Avast - Win32:Bifrose-DXJ [trj]
AVG - Nothing found!
BitDefender - Backdoor.Gener ic.144576
ClamAV - Nothing found!
Comodo - Backdoor.Win32 .Bifrose.~AJX
Dr.Web - Win32.HLLW.MyB ot
Ewido - Nothing found!
F-PROT 6 - Nothing found!
G DATA - Backdoor.Win32 .Poison.rao A
IkarusT3 - Backdoor.Win32 .Bifrose
Kaspersky - Backdoor.Win32 .Poison.rao
McAfee - Nothing found!
MHR (Malware Hash Registry) - Nothing found!
NOD32 v3 - Nothing found!
Norman - Nothing found!
Panda - Nothing found!
Quick Heal - Nothing found!
Solo Antivirus - Nothing found!
Sophos - Nothing found!
TrendMicro - Nothing found!
VBA32 - Backdoor.Win32 .Bifrose.ajlb
Virus Buster - Nothing found!

Scan report generated by
http://novirusthanks.org]NoVirusThanks. org

Ya ahora podemos comenzar, yo voy empezar a buscar firmas con Avast ustedes pueden empezar con el que gusten...
Con el antivirus instalado y actualizado (si no desean tener que estar desinstalando su antivirus para instalar otro pueden usar una VirualBox y instalar en esta los Avs que van a usar) abrimos el SignatureZero y buscamos nuestro Stub.
Aqui tenemos dos formas de encontrar nuestra firma/as, podemos dejar los marcadores a los extremos y seleccionar "Entre los marcadores" y darle al boton Crear archivos y cuando termine escanear la carpeta Temp con nuestro Av`s asi nos quedaran solo los archivos donde esta nuestra firma o la segunda opcion es ir rellenando con ceros por pedazitos hasta cercar nuestra firma. Es bueno aclarar que la primer ocion solo es recomdable dependiendo del peso del stub si nuestro stub pesa unos 500 kb no es para nada recomdable usar esta opcion ya que se crean un archivo por cada offset por lo cual tendriamos unos 500.000 archivos de 500 kb y esto se pondria pesado. Pero tambien se pueden utilizar ambas opciones es decir vamos rellenando con ceros y ponemos los

marcadores solo en la parte verde como para cercar exactamente nuestra firma.
IMPORTANTE: para la primera opcion nuestro antivirus tiene que estar desactivado para la segunda es necesario tenerlo activado en tiempo real.

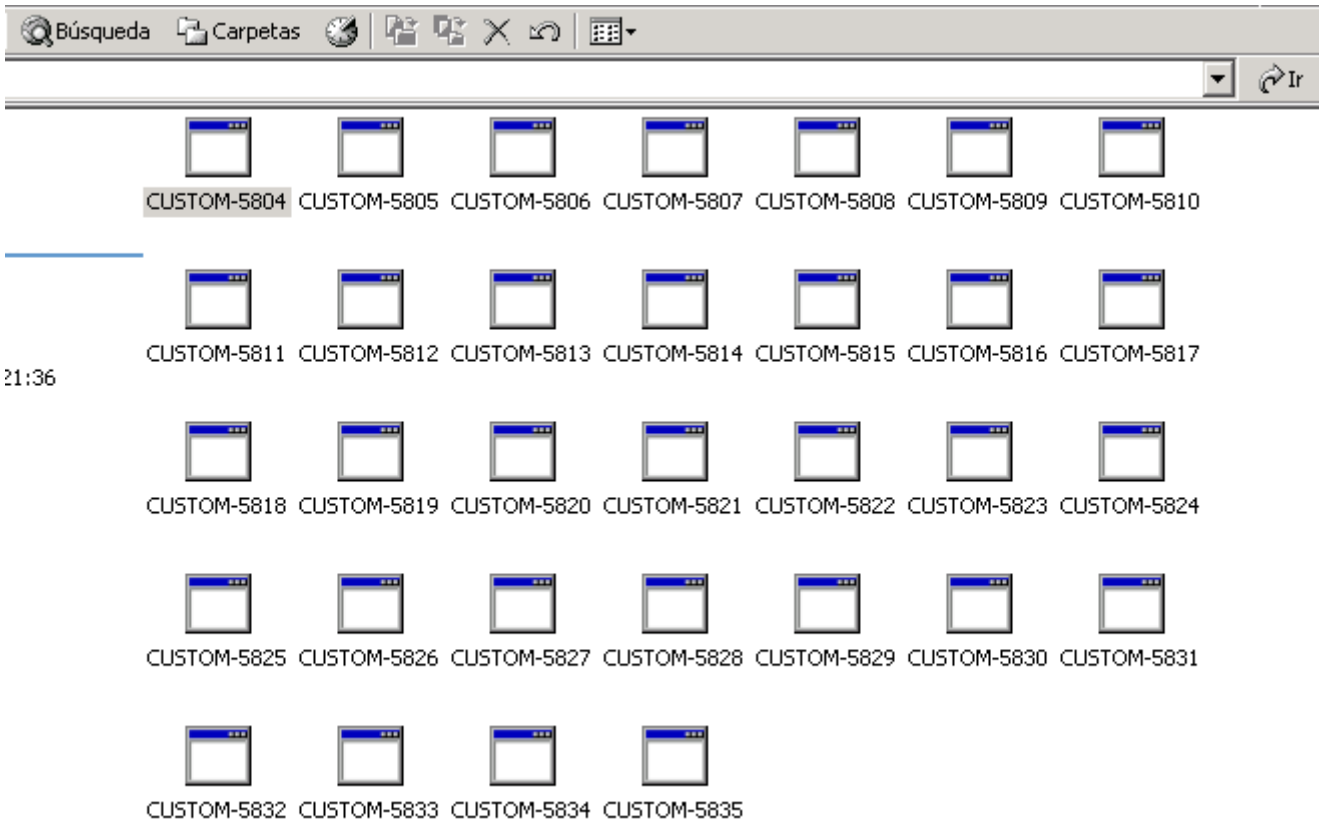
Opcion 1



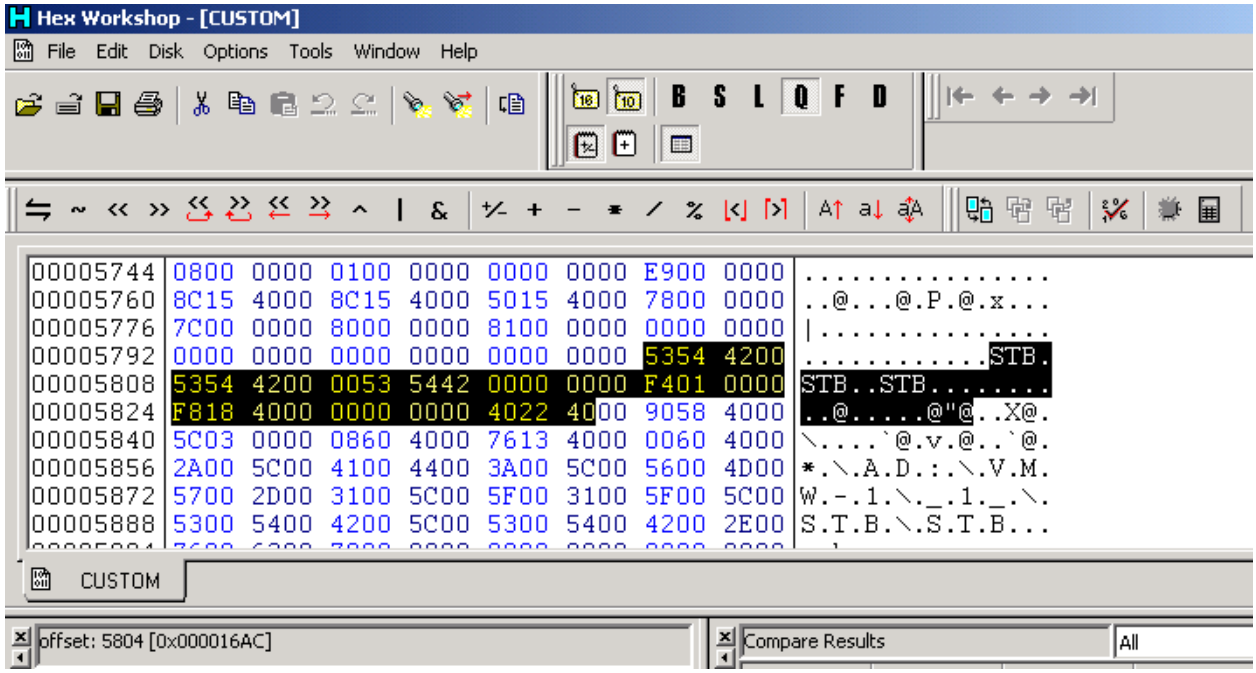
Opcion 2

imagen solo para guiarse, aqui no esta cercada la firma.

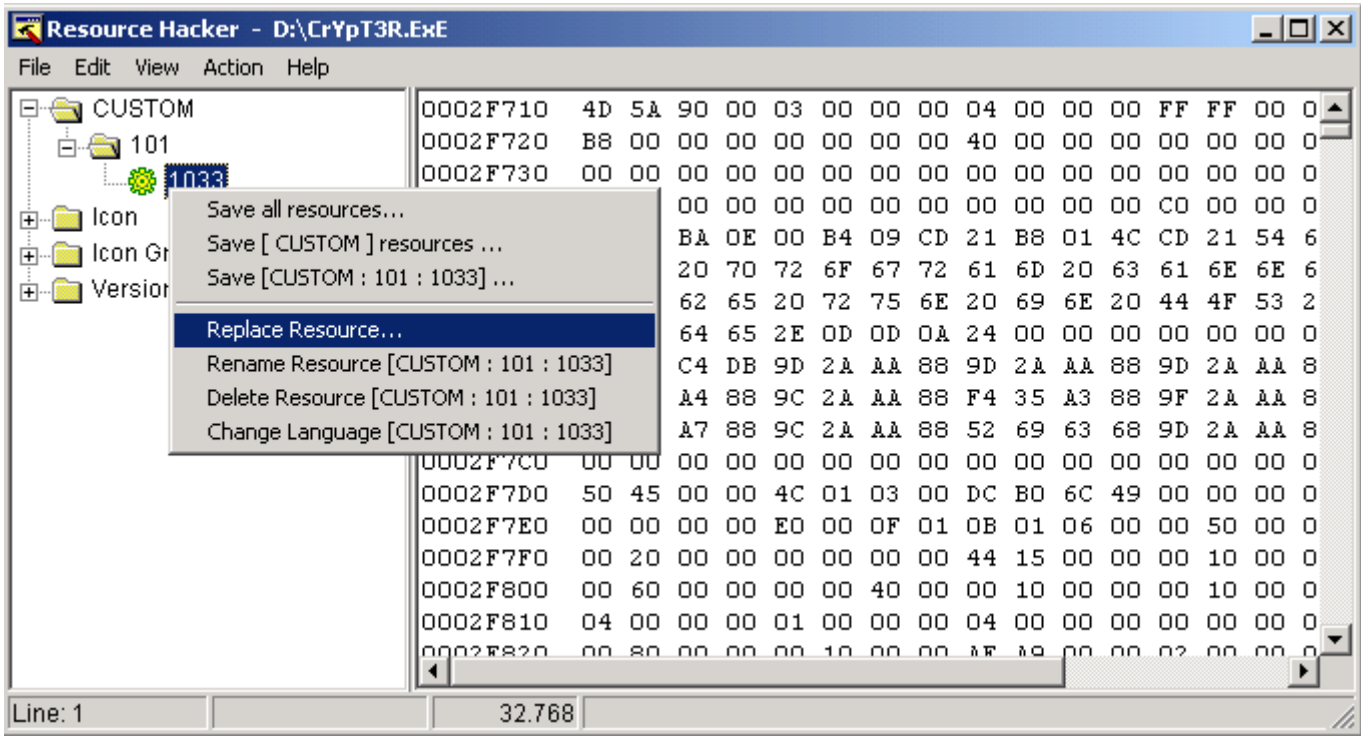
Ok ya tenemos nuestra firma cercada para este antivirus (Avast) la firma esta entre los offsets 5804 y 5835. (utilize la primer opcion rellenando primero como en la imagen de arriba gran parte con ceros)



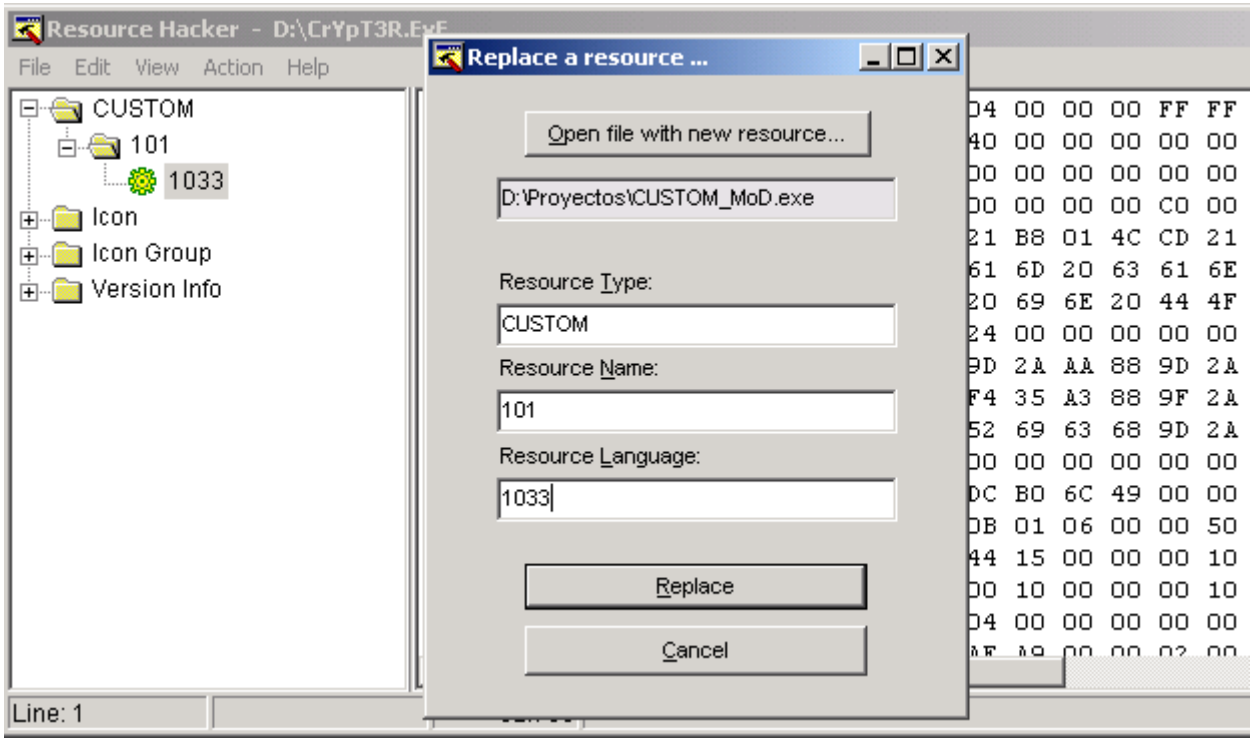
bien aqui podemos pasar al editor Hexadecimal (HexWorkShop) o directamente al Olly, yo siempre primero lo miro en el editor Hexadecimal ya que aveces se puede modificar muy facilomente y evitar el trabajo mas latoso con el Olly... bueno veamos nuestra firma...



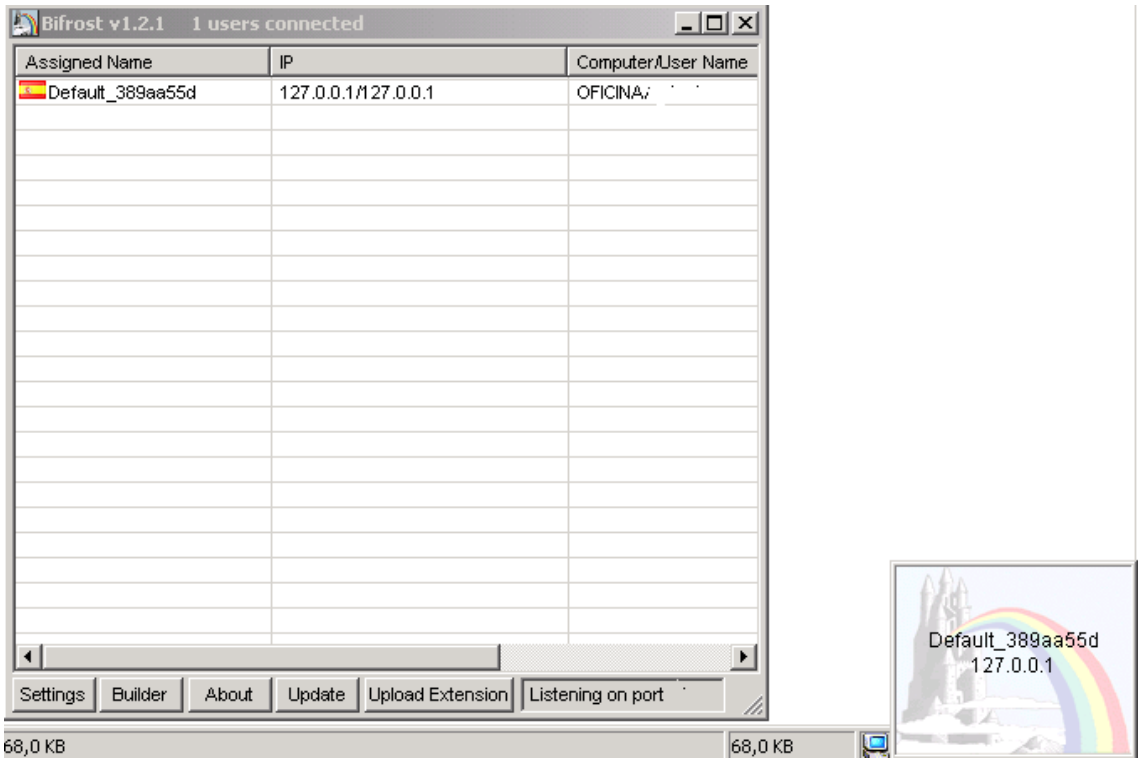
Como ven ahi tenemos nuestra firma, aqui podemos intentar modificar algo a ver si nos evitamos ir al Olly. Bueno aqui tendran que ir probando de ir cambiando una letra de Mayuscula a Minuscula, un numero por otro, un caracter por otro y asi, ahora si aparece en la firma Kernel32.dll o algo similar no se gasten en tocar esta parte porq quedara inservible, Aqui ya juega un poquito la practica y el sentido comun.
Yo directamente fui a las " que aparecian en la firma que es igual al numero 22 y lo cambie por 23 y lo guardamos, una tontera Tongue, bien ahora le pasamos nuestro antivirus y seguramente no lo detectara pero funcionara? como lo sabemos? Bueno vamos nuevamente al ResHack y abrimos nuestro stub y nos posicionamos como muestra la imagen y click con el boton derecho y vamos a Remplace Resource...



Buscamos nuestro stub con la modificacion lo cargamos y escribimos los datos como los tenemos en el ResHack y se ve en la imagen y le damos en Remplace... Despues vamos a File, Save as y lo guardamos como queramos.



Y ahora lo probamos si funciona o rompimos el stub, yo voy a juntar y encriptar solo el server del Bifrost sin ningun otro archivo.



Como ven funciona y si volvemos a escanear nuestro stub modificado en NoVirusThaks.o rg vemos que no solo nos saltamos la firma del Avast si no de otros

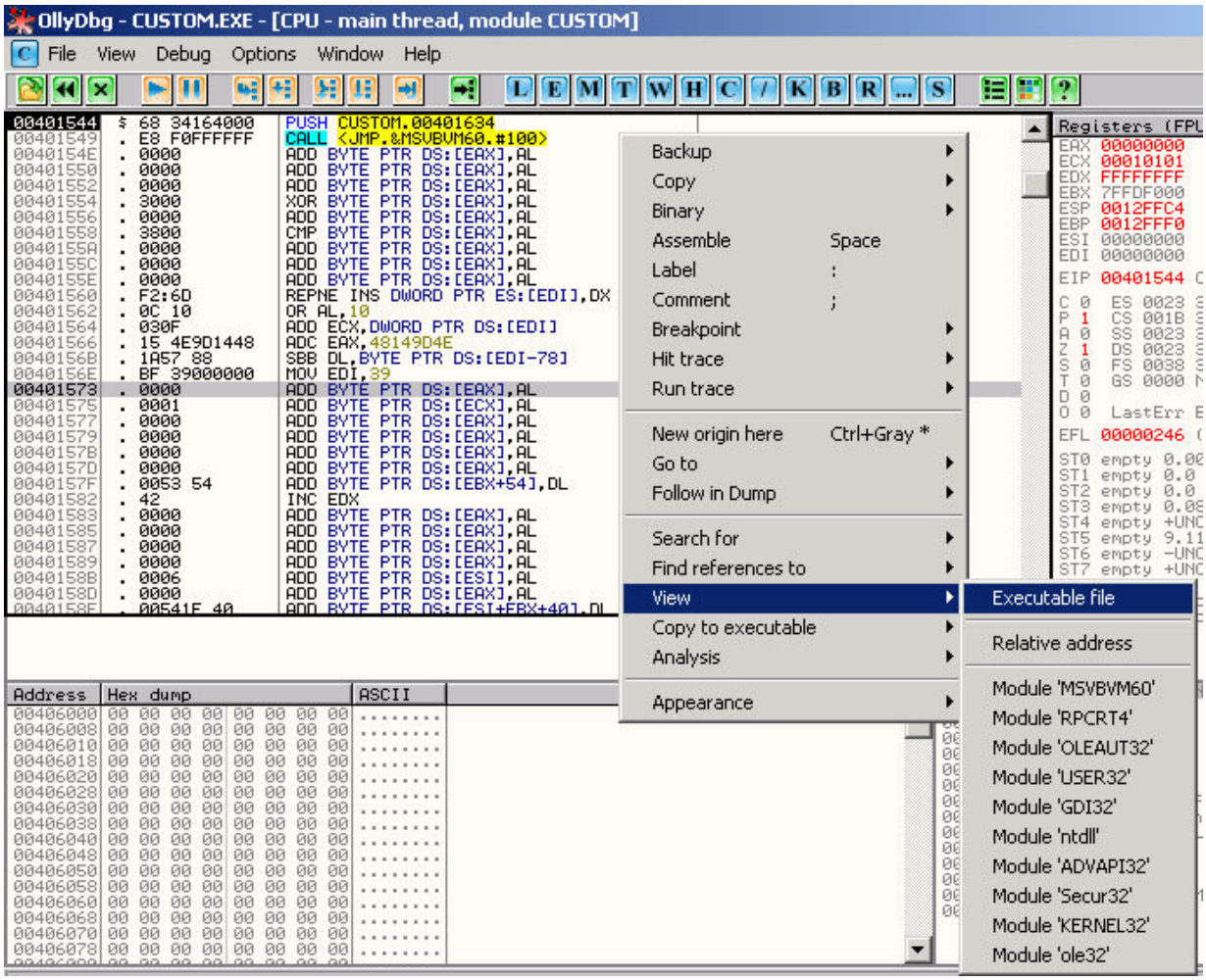
dos y ya solo nos los detectan 6 de los 9 que lo detectaban en un principio.

Detection rate: 6 on 24

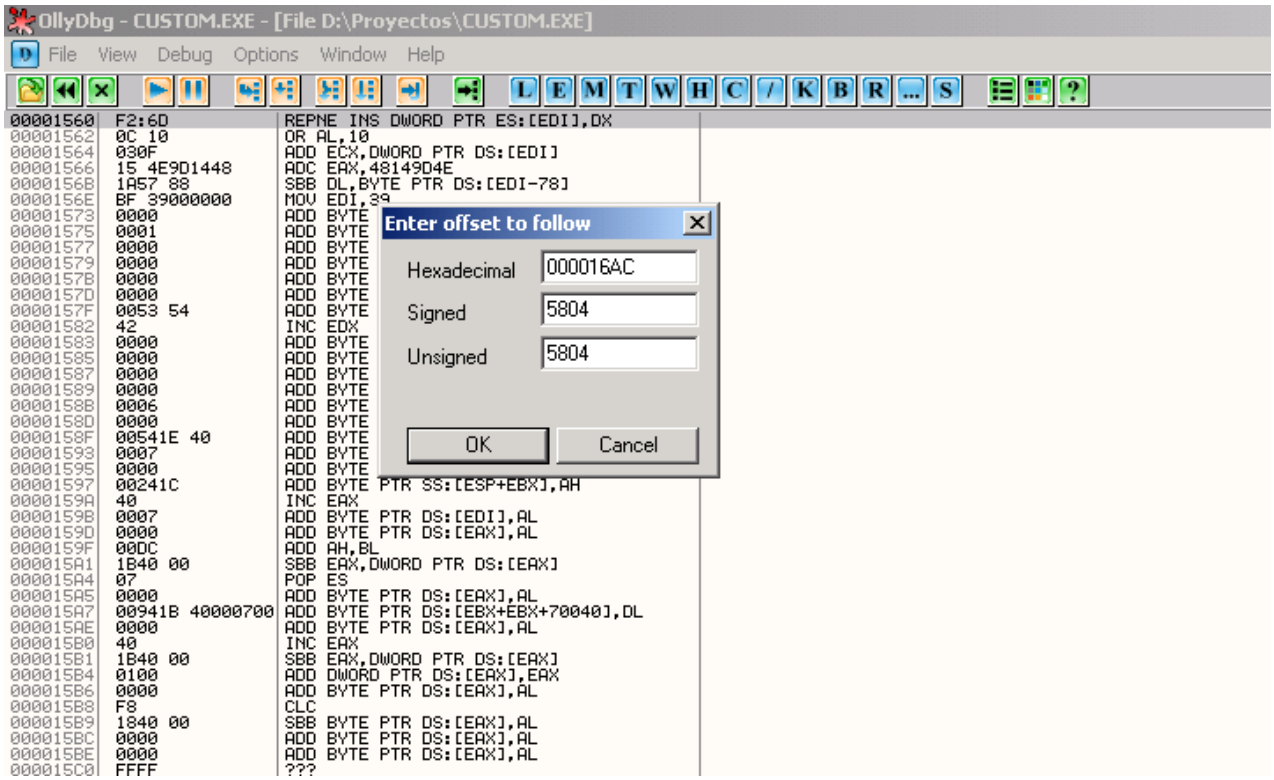
Detections

a-squared - Backdoor.Win32 .Bifrose!IK
Avira AntiVir - Nothing found!
Avast - Nothing found!
AVG - Nothing found!
BitDefender - Nothing found!
ClamAV - Nothing found!
Comodo - Backdoor.Win32 .Bifrose.~AJX
Dr.Web - Win32.HLLW.MyB ot
Ewido - Nothing found!
F-PROT 6 - Nothing found!
G DATA - Backdoor.Win32 .Poison.rao A
IkarusT3 - Backdoor.Win32 .Bifrose
Kaspersky - Backdoor.Win32 .Poison.rao
McAfee - Nothing found!
MHR (Malware Hash Registry) - Nothing found!
NOD32 v3 - Nothing found!
Norman - Nothing found!
Panda - Nothing found!
Quick Heal - Nothing found!
Solo Antivirus - Nothing found!
Sophos - Nothing found!
TrendMicro - Nothing found!
VBA32 - Nothing found!
Virus Buster - Nothing found!

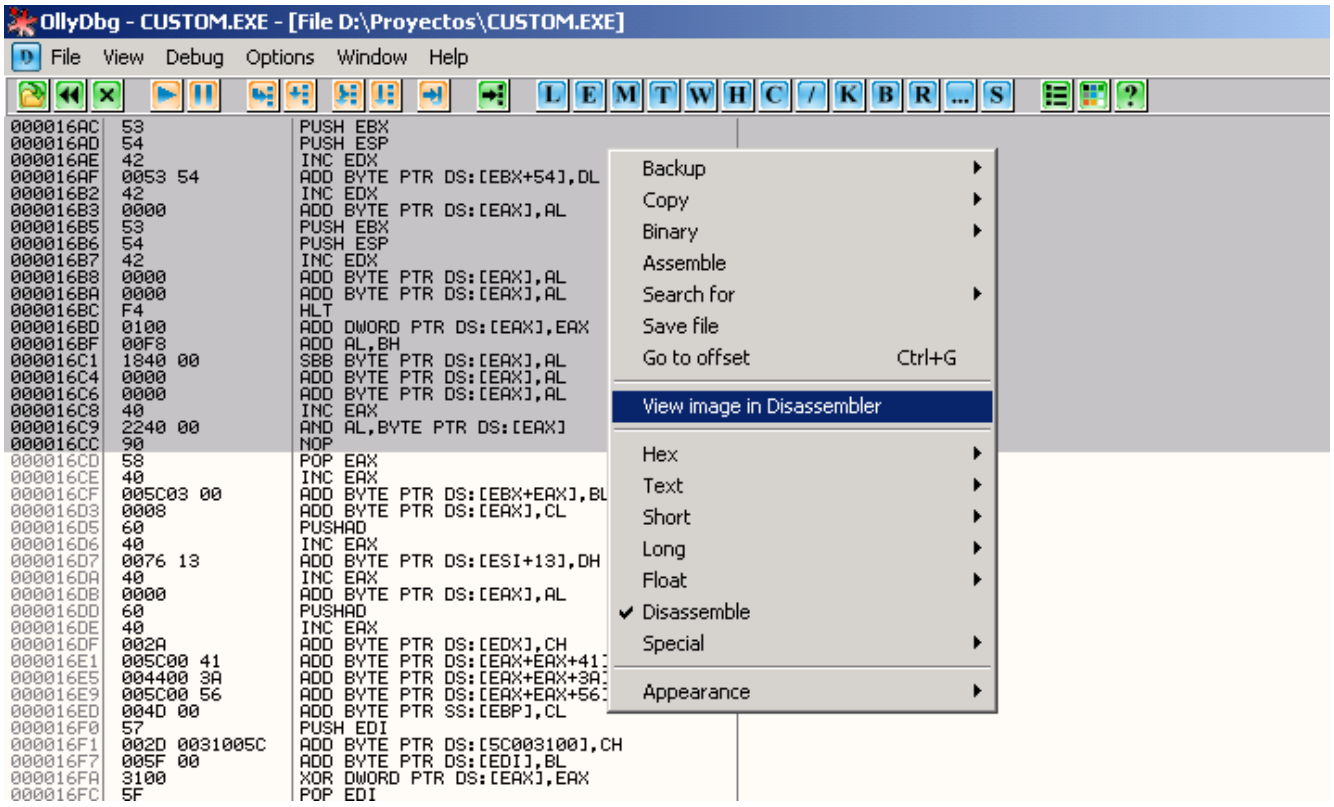
Pero supongamos que esta forma de modificar no funcionara, tendriamos que usar otro metodo, podemos usar el Metodo RIT o el Metodo XOR... aqui usare el RIT que me parece un poquito mas latoso que el XOR y mejor explicar lo mas complicado.
Ok abrimos el Olly y buscamos nuestro stub (es el sin modificar ya que suponemos que no funciono lo anterior). Vamos a View, Executable file tal cual lo muestra la imagen...



en la pantalla de Executable file apretamos Control + G y ponemos el offset donde teniamos nuetra firma (5804). unavez que nos lleva a esta firma podemos hacer otra vez lo mismo poniendo el offset donde terminaba la firma pero solo para ver la direccion donde terminaba asi vemos donde empieza y termina.

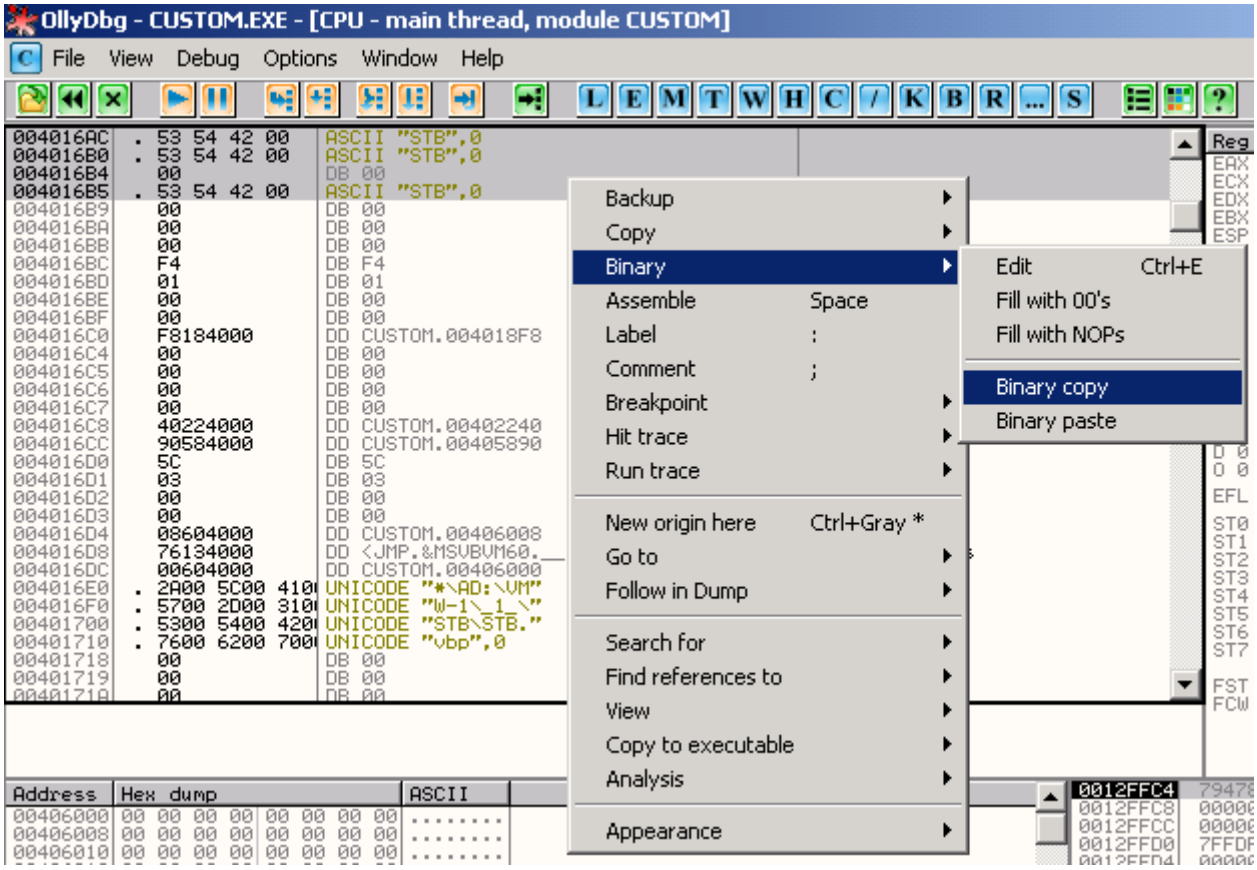


Bueno una vez que tenemos localizada y seleccionada nuestra firma hacemos click boton derecho y vamos a View image in Disassembler...

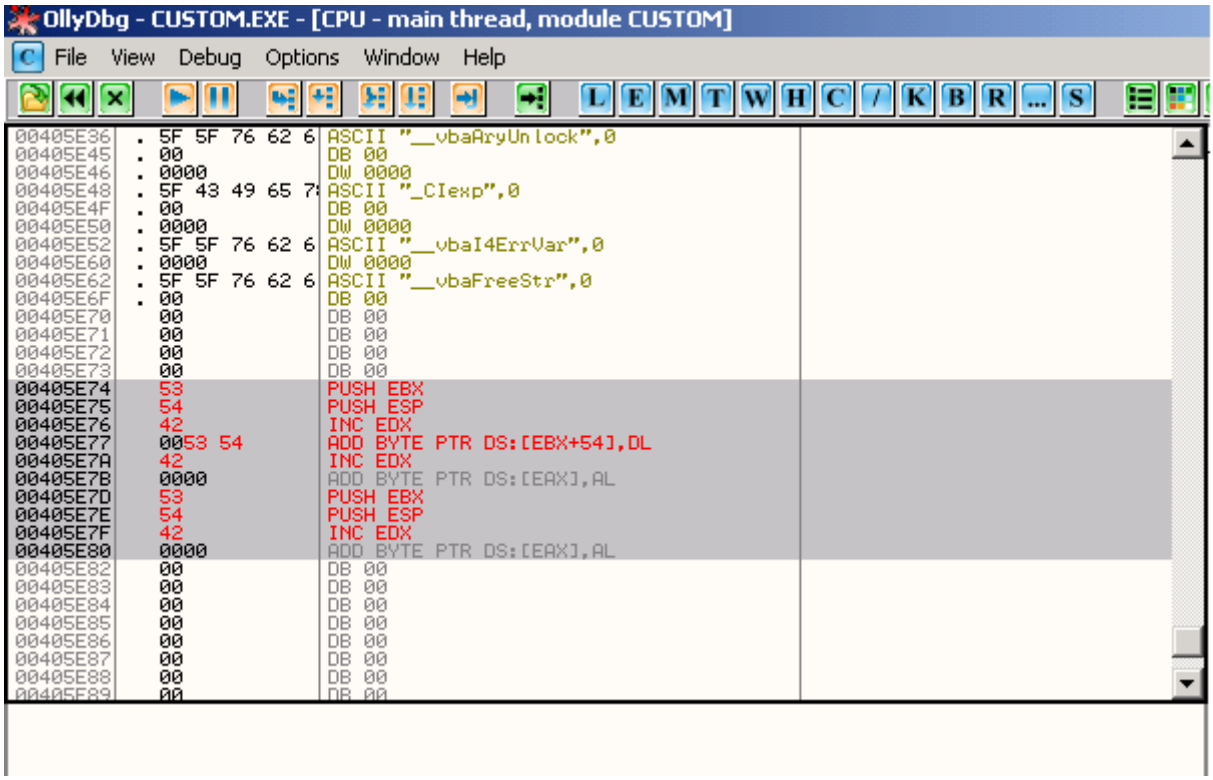


Bueno nos llevara a la la primer pantalla marcandonos toda nuestra firma, aqui

seleccionaremo s una parte y haremos un JUMP de esta, yo eleji desde la direccion 004016AC hasta 004016B5, teniendo seleccionada esta parte hacemos click boton derecho y vamos a Binary, Binary Copy...



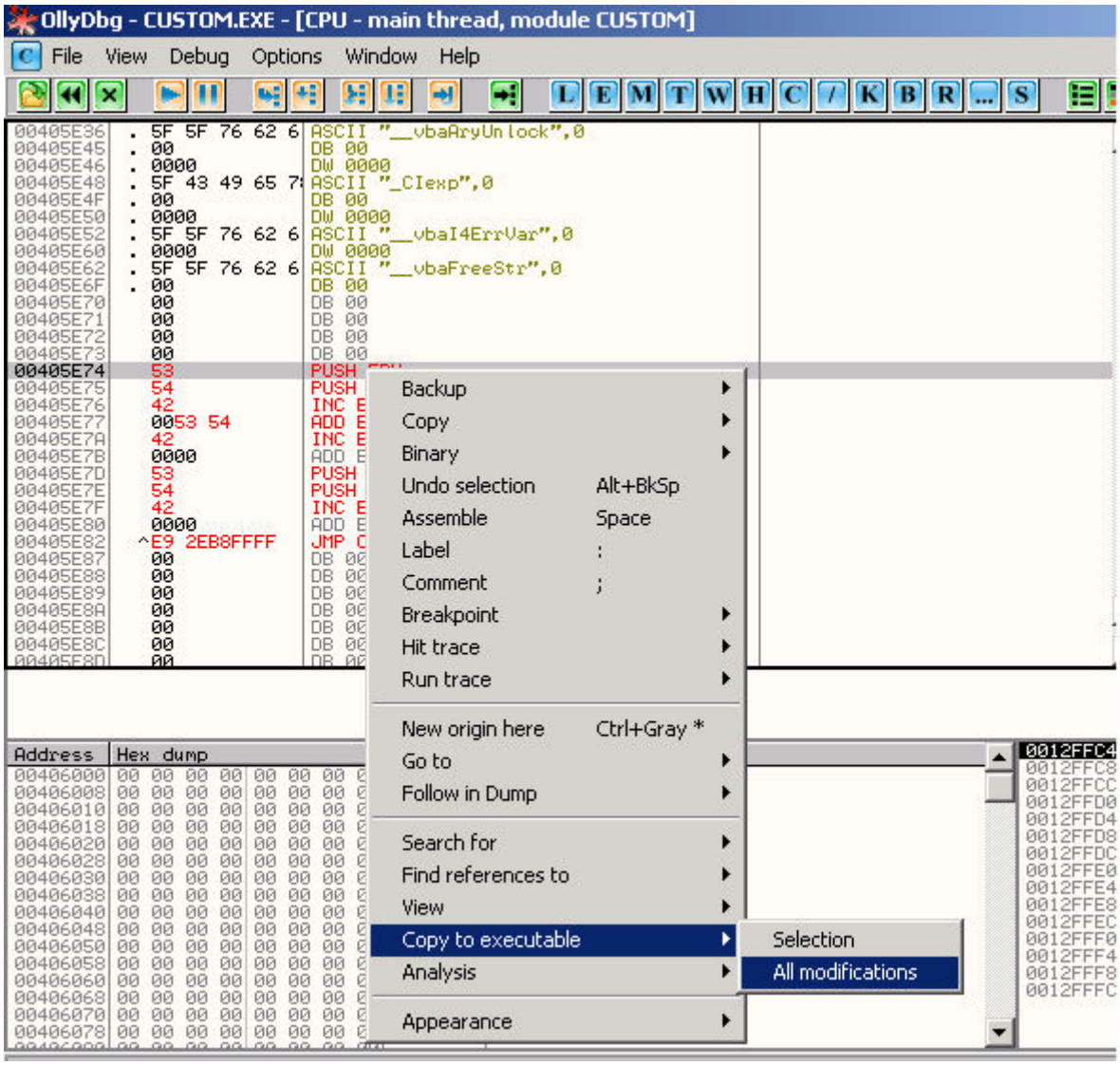
Aqui nos vamos al final de nuetrso stub donde tenemos bytes libres y vamos a pegar esto que copiamos, siguiendo basicamente el mismo paso Binary, Binary Paste en vez de Copy, se daran cuenta que no nos quedo como lo que copiamos pero a no preocupar que esta todo bien igual.



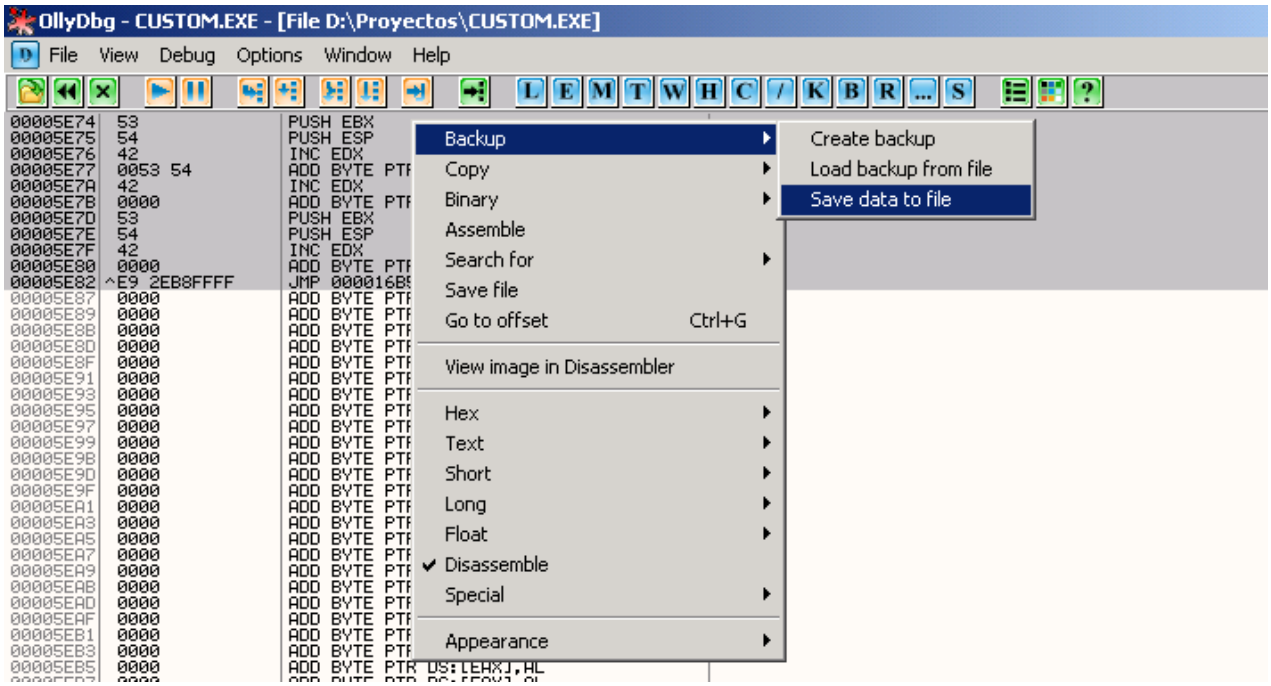
Ahora tenemos que hacer el JUMP, para ello volvemos al pedazito de firma que copiamos y nos posicionamos desde donde comenzamos a copiar y hacemos click boton derecho y vamos a Assembler o apretando la barra espaciadora y ponemos "JMP 00405E74" y le damos Assembler, 00405E74 es la direccion donde comienza la firma que hemos copiado al final de nuetrso stub, si observan las imagenes se daran cuenta, esto siempre tienen que anotarlo para asi no tener que estar volviendo para atras cuando necesiten la direccion a la cual tienen que hacer el JUMP.

Hacemos lo mismo pero desde donde termina la firma que copiamos hacia donde termina la firma original...

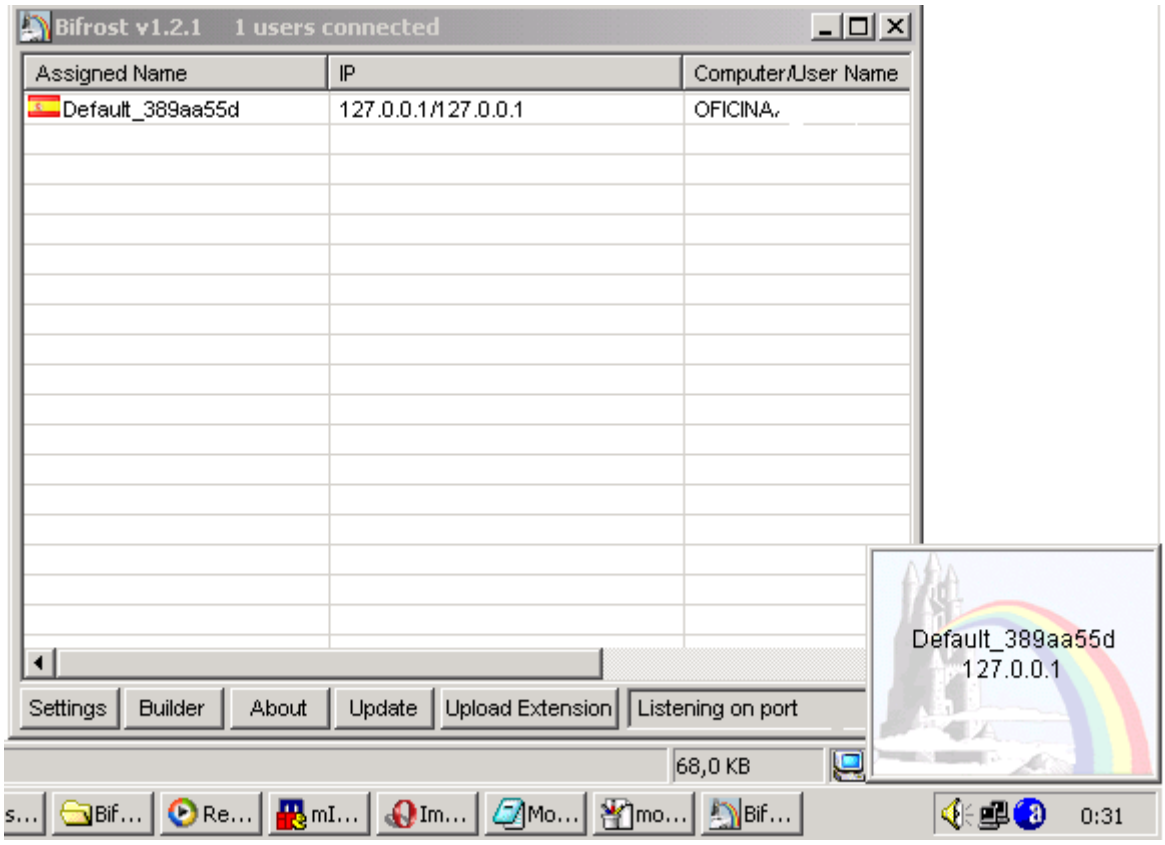
Una vez hecho esto nos posicionamos sobre alguna de las modificaciones otra vez click boton derecho y vamos a Copy to executable, All Modifications y por ultimo Copy All.



En esta pantalla solo hacemos click boton derecho y vamos a Backup, Save data to file.
y lo guardamos como Custom_Mod o con el nombre que queramos.



Bien ahora repetimos el paso que habiamos hecho con el ResHack y volvemos a cargar nuetrso stub modificado al crypter y lo probamos, antes probamos que se salte nuestro Antivirus tambien...



Y funciona!!!

Bueno espero les haya gustado el tutorial y sirva para que haya menos ¿Como hago mi troyano indetectable? y haya mas crypters indetectables.

NOTA: Yo aqui explique el Metodo RIT pero tambien pueden utilizar el Metodo XOR o ambos ya que a veces hay firmas que no se pueden hacer un JUMP y tendran que recurrir al otro metodo. Saludos y hasta la proxima cLaRoScUrO.

No Suban sus mods a VirusTotal

&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&
& Tutorial de como modificar los crypters hecho por cLaRoScUrO. &
& 23 de Enero de 2009 &
& &
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&