Hace poco Ricardo presentó a la lista la herramienta de Nicolás Economou turbodiff.

Turbodiff es un pluggin para IDA que hace una comparación binaria de dos programas, por supuesto va más allá que una mera comparación. Para ver una primera aproximación a como usarlo podéis mirar este tute de Ricardo:
http://ricardonarvaja.info/WEB/OTROS/EXPLOIT/USAR%20TURBODIIFF%20PARA%20HALLAR%20PARCHES%20Y%20FUNCIONES%20VULNERABLES.doc.7z

El turbodiff podéis bajarlo de la página de Core:
http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=tool&name=turbodiff

Para instalarlo simplemente hay que copiar el archivo turbodiff.plw en la carpeta de pluggins de IDA.

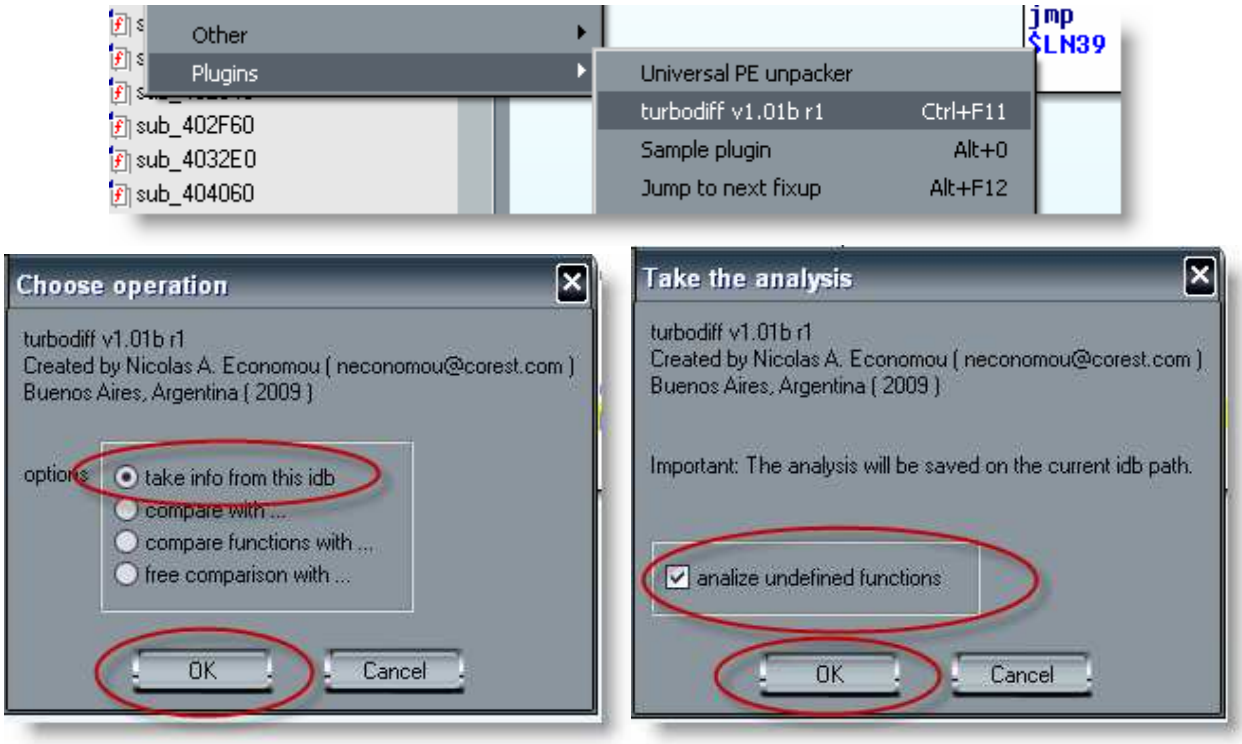
Turbodiff está pensado para comparar dos versiones de un programa para comprobar si la nueva mantiene alguna vulnerabilidad de la antigua. En este tutorial lo usaremos para algo más prosaico, como es comparar un programa "original" con el "parcheado" e intentar aplicar el parche a una versión más nueva.

Trabajaremos sobre DiagramStudio 5.4 con un parche de Invisible team, a estas alturas no tengo el enlace, pero seguro que hay copias de seguridad colgadas de la red.

Al día de hoy la Versión 5.5 trial se puede descargar de la página oficial:
http://www.gadwin.com/

Lo primero claro está es instalarnos las versiones 5.4 y 5.5, y aplicar el parche a la 5.4 (el mismo parche hace una copia de DiagramStudio.exe que yo he renombrado a anterior.exe, además con esto ya sabemos que fichero es el que se parchea).

Abrimos el anterior.exe en IDA y esperamos a que termine el análisis (ahora es buen momento para irse a la nevera por una cervecilla). Una vez acabado el análisis lo salvamos con ctrl.+W y vamos en edit-> pluggins al turbodiff:

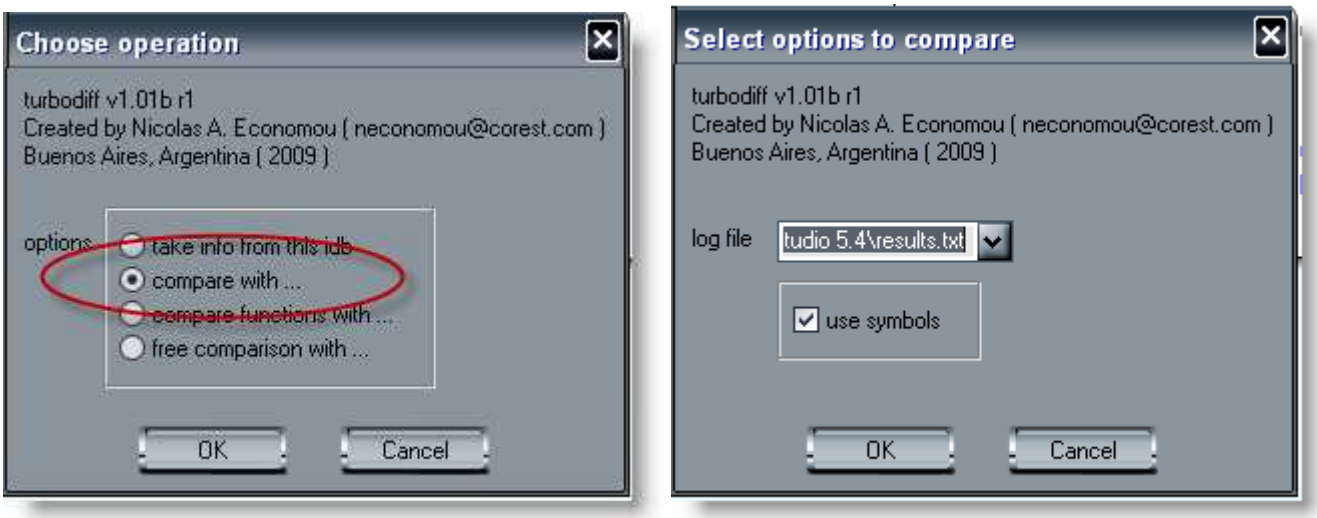


En la segunda ventana marco la opción de analize undefined functions porque de otra forma al comparar me tira una excepción.

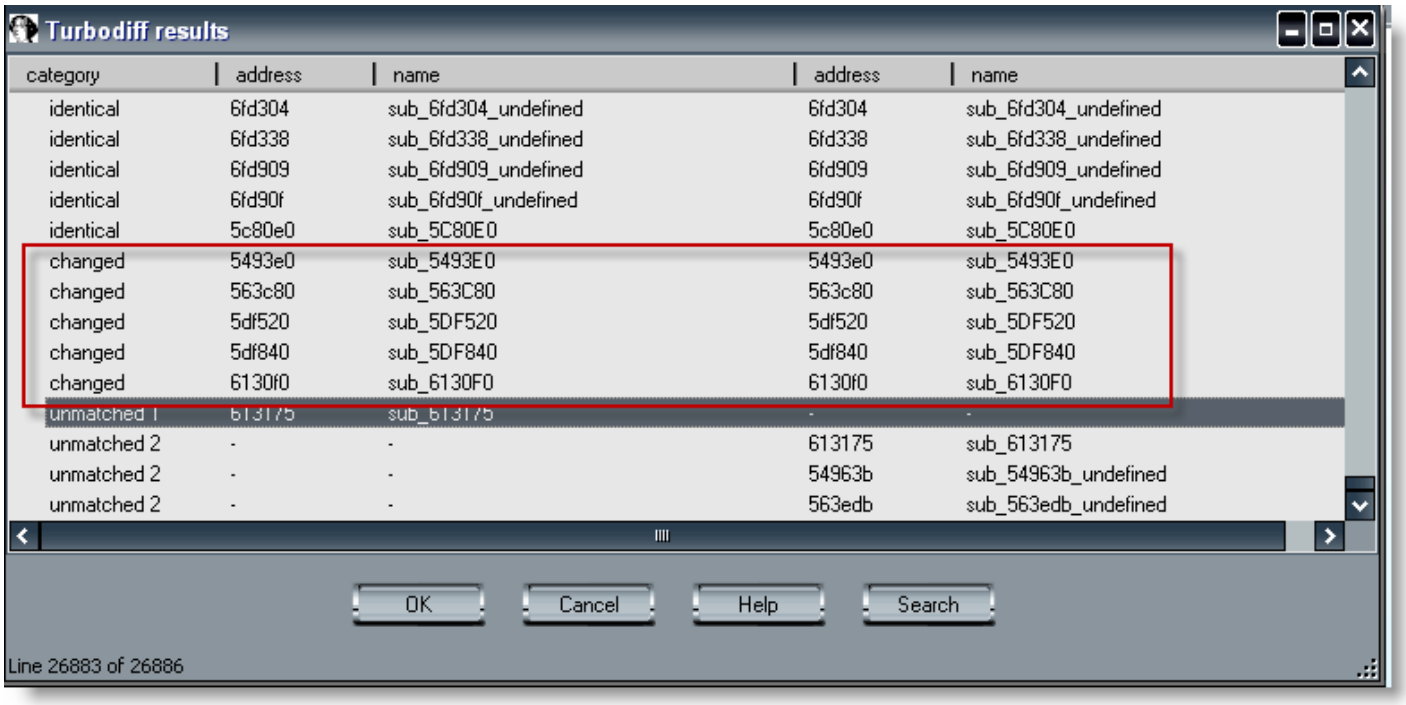
El ordenador no se ha colgado, es que tarda un rato, acabamos la cerveza y vamos por otra y nos preparamos algo para picar.

Este proceso lo repetimos para los archivos DiagramStudio.exe de la versión 5.4 y 5.5.

Después de 6 cervezas y tres bocatas, abrimos el anterior.exe (el 5.4 sin parchear), y en menú->edit->pluggins abrimos el turbodiff y procedemos a comparar:

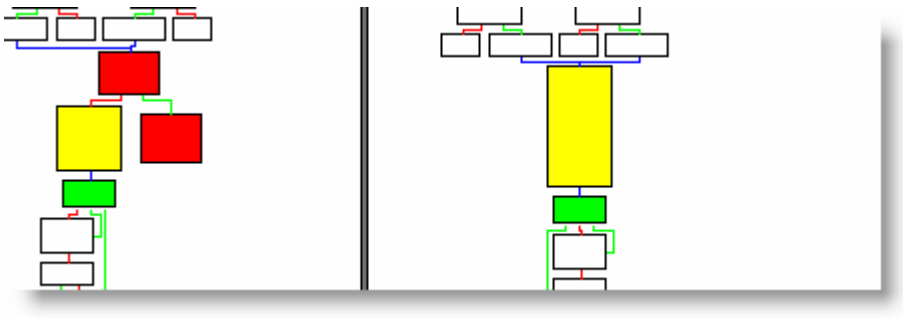


Elegimos el DiagramStudio.exe de la versión 5.4 y en un momento tenemos la ventana con todas las funciones “matcheadas”, al final vemos las que han cambiado y algunas que no pudo matchear:

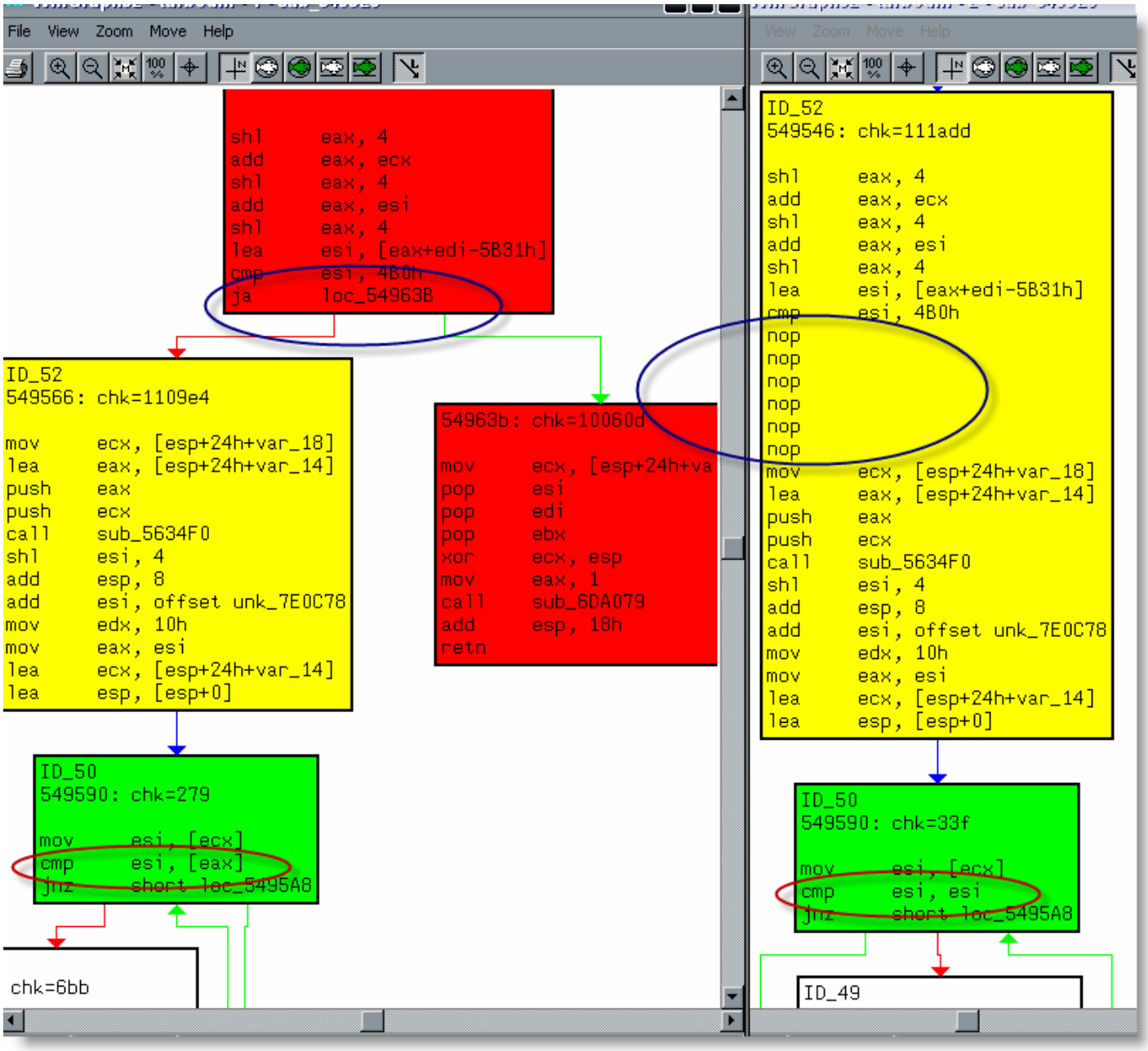


Nosotros nos fijaremos en las marcadas como changed, (cuando hayamos visto la modificación podemos hacer una búsqueda con el ultracompare para verificar que efectivamente todos los cambios están en estas cinco funciones).

Pues doble click en la primea (5493E0) y tenemos los dos gráficos:



Si los ampliamos al 100% podemos ver el cambio:

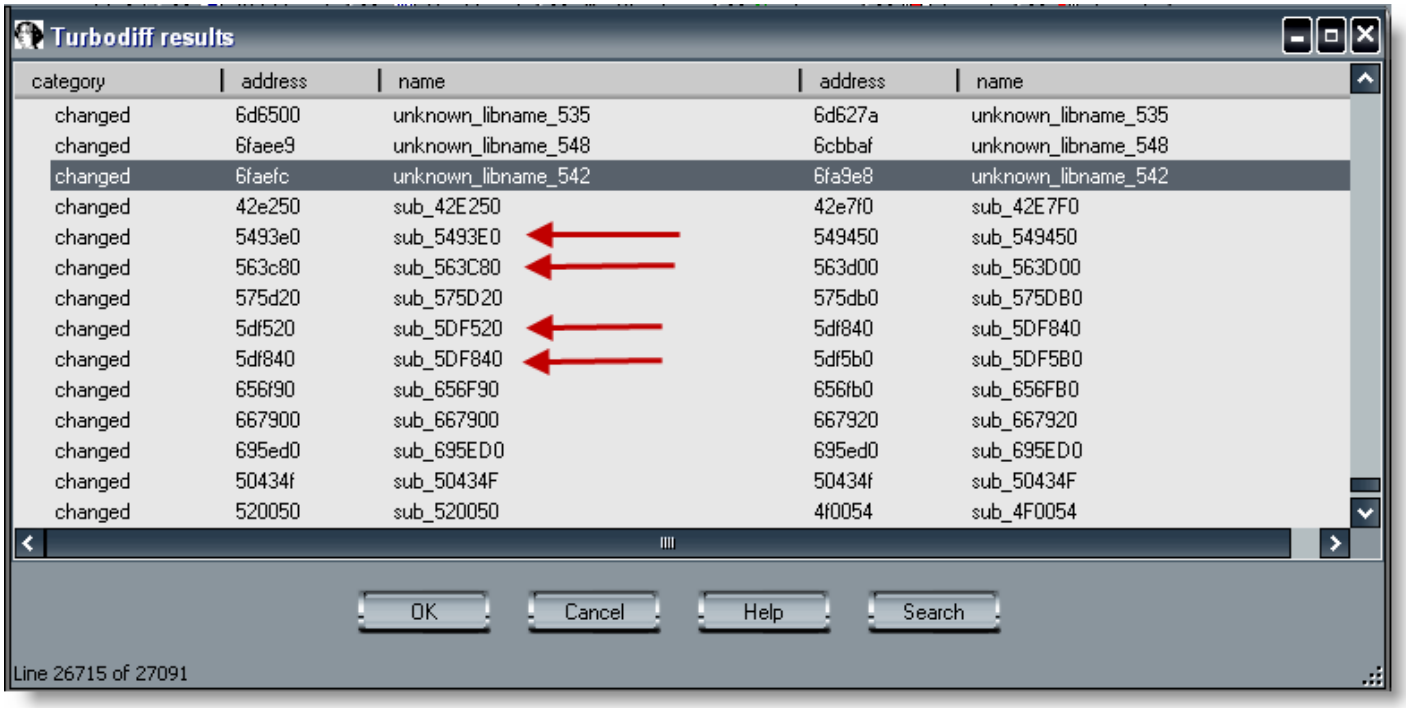


Sencillamente nopearon el ja 54963B y cambiaron la comparación cmp esi, [eax] por cmp esi, esi.

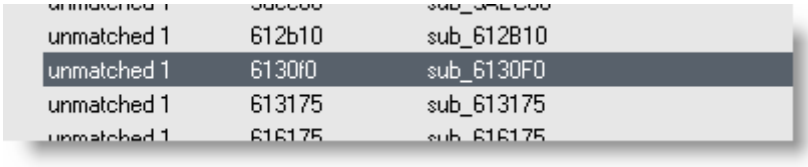
Podemos examinar las cinco funciones y veremos que el cambio es esencialmente igual, solo se diferencia el la comparación (cmp esi,[ecx] por ejemplo), y el la posición de dicha comparación que puede estar un poco más lejos.

Pues con esto ya hemos visto los cambios que hace el patcher en el ejecutable, lo siguiente es comparar el parcheado con el original de la versión 5.5.

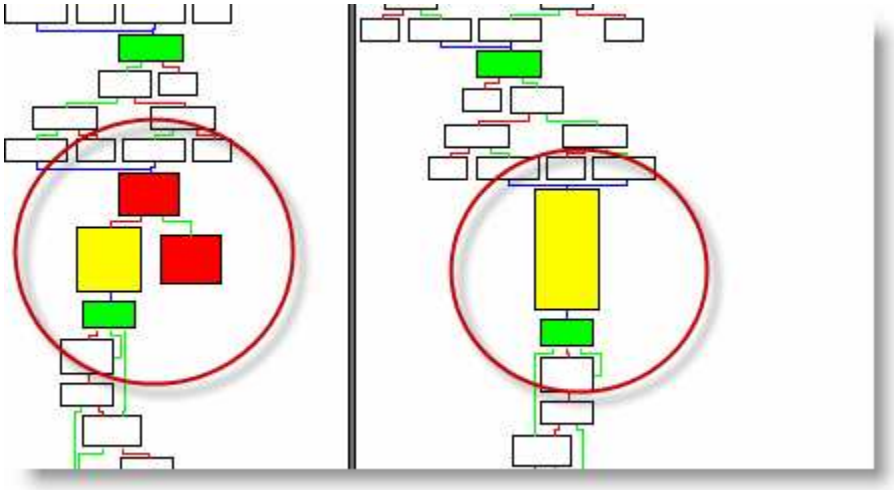
Pues vamos al lío, abrimos en IDA el DiagramStudio.exe del la versión 5.4 (el parcheado) y lo comparamos el turbodiff con el DiagramStudio.exe 5.5 (el que queremos parchear), podemos ver que hay muchas más funciones changed y unmatched, pero nosotros ya sabemos las cinco que queremos:



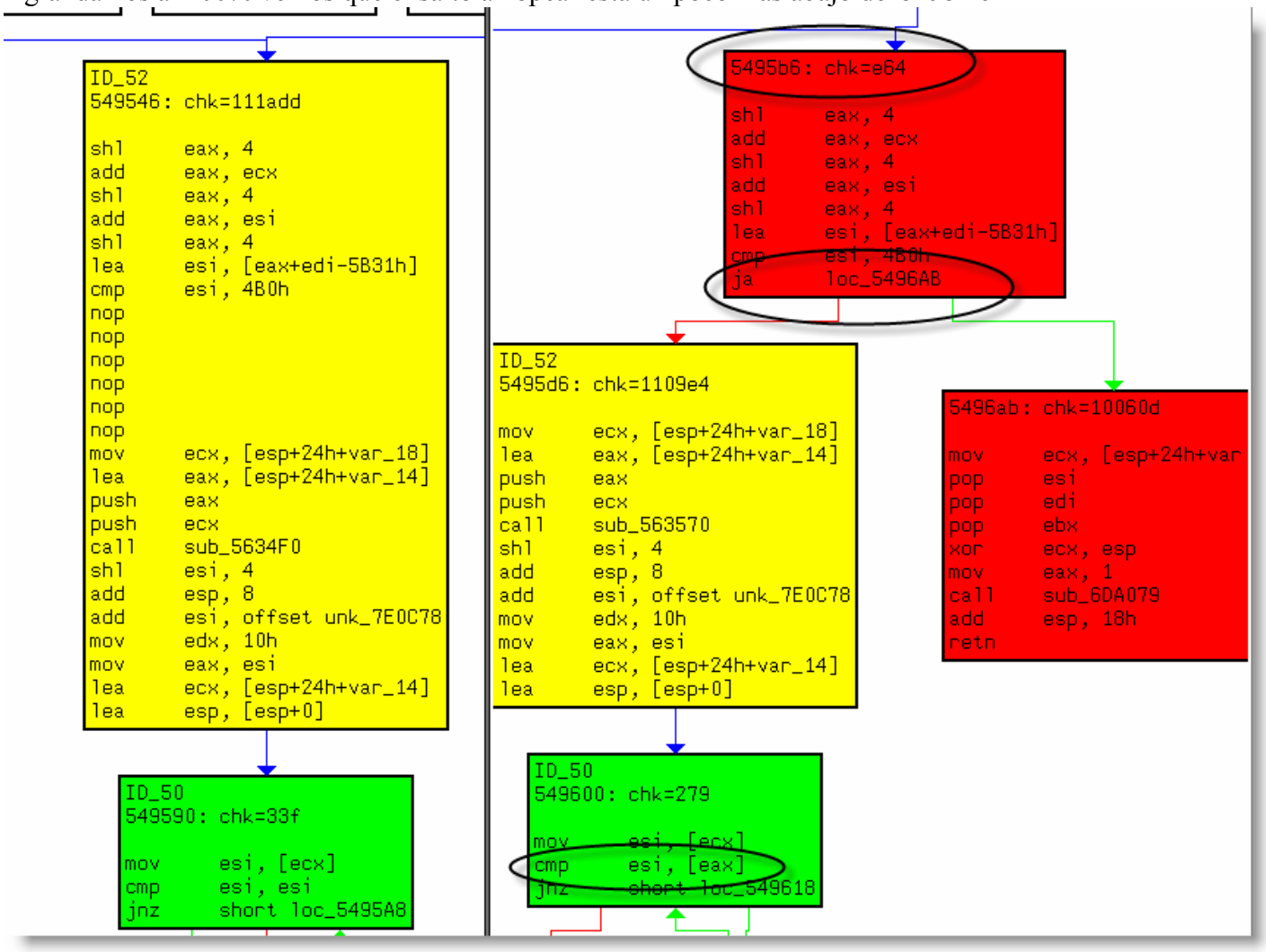
Vemos que falta la 6130F0 que está unmatched. Esa la dejaremos para el final:



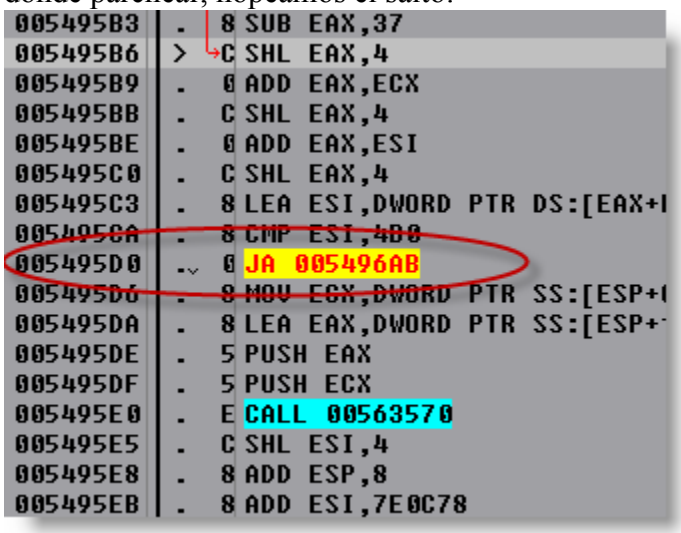
Si hacemos doble click sobre 5493E0 nos aparecen los dos gráficos, y vemos fácilmente donde hay que parchear:

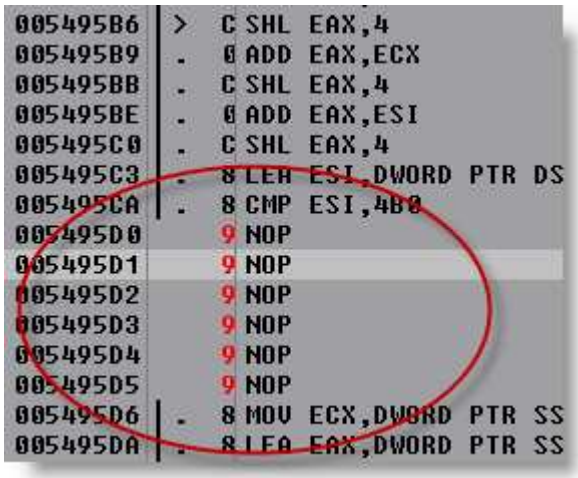


Agrandamos al 100% vemos que el salto a nopear está un poco más abajo de 5495B6

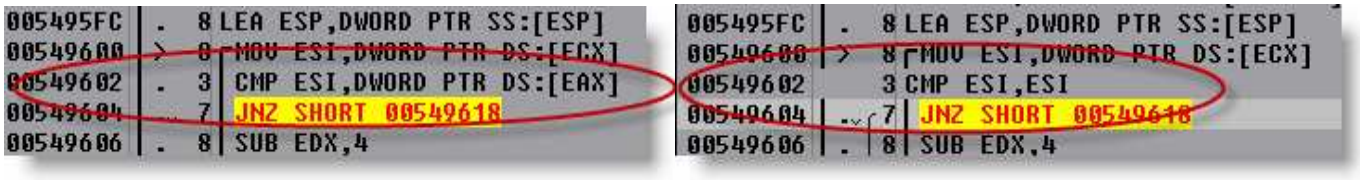


Ahora cargamos el DiagramStudio.exe 5.5 en Olly y desde el EP con ctrl.+b buscamos 5495B6 y ya tenemos donde parchear, nopeamos el salto:





Y cambiamos la comparación que está algo más abajo:

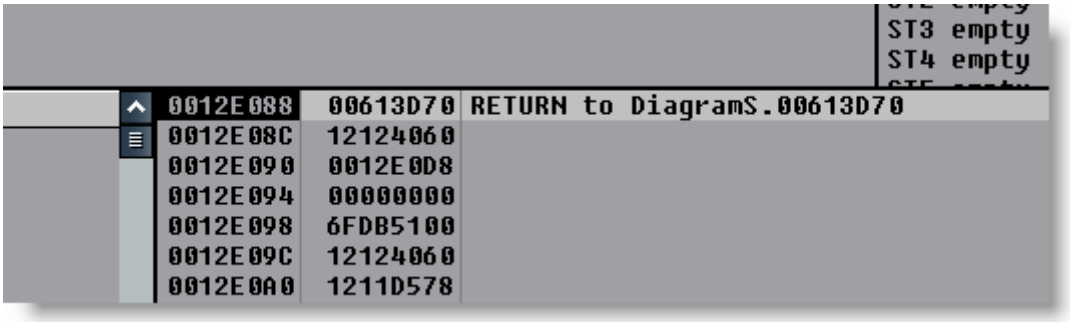


Pues el proceso es el mismo para las otras tres funciones.

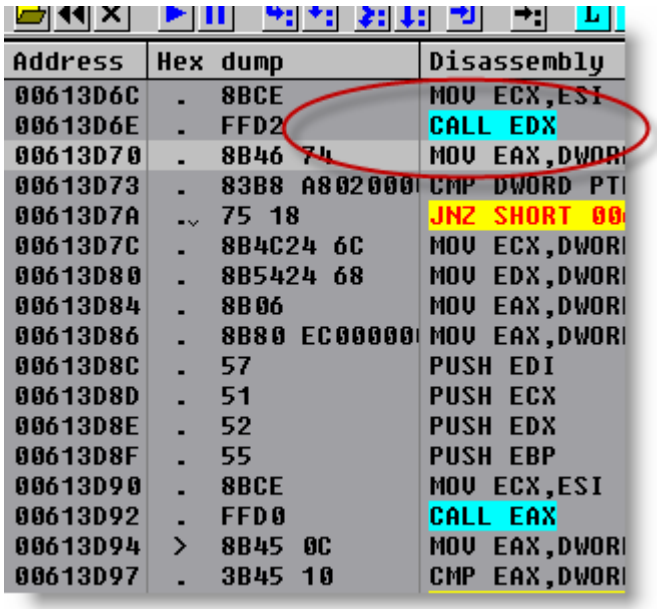
A estas alturas ya os habréis dado cuenta que todos los parches responden al patrón:
cmp esi, 4B0
ja xxxxxxxx

Si en Olly buscamos el comando cmp esi, 4B0 encontraremos fácilmente todas las zonas a parchear, pero como estamos jugando con turbodiff, buscaremos con el la que nos falta.

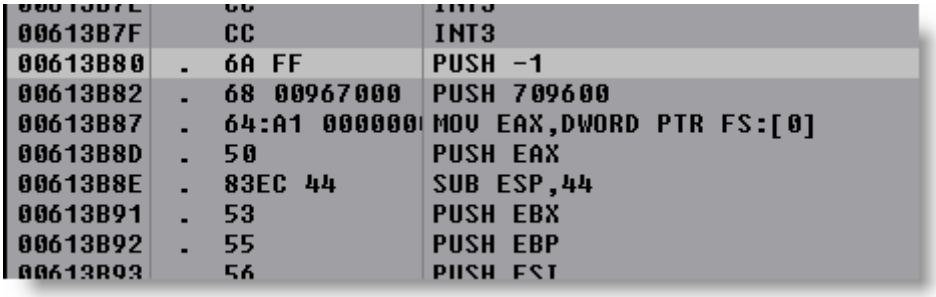
Abramos en Olly una instancia, ponemos un BP en 6130F0 y cuando para vemos retornará a 613D70



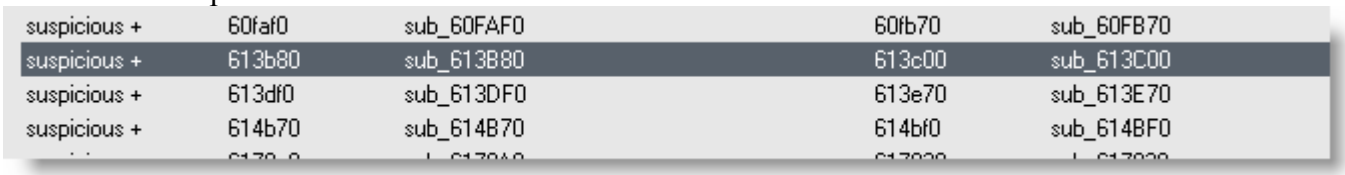
Si nos vamos a 613d70 vemos el punto donde retorna:



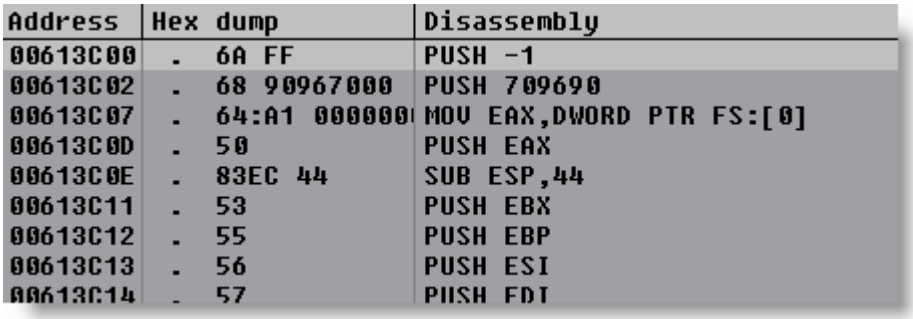
Ahora subimos hasta el inicio de la función:



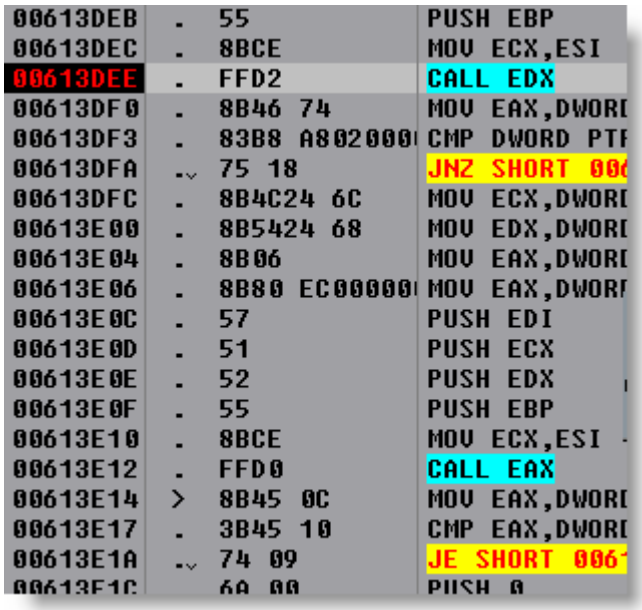
Vemos que está el 613B80, pues si buscamos la cadena 613B80 en la ventana del turbodiff la encontramos marcada como sospechosa:



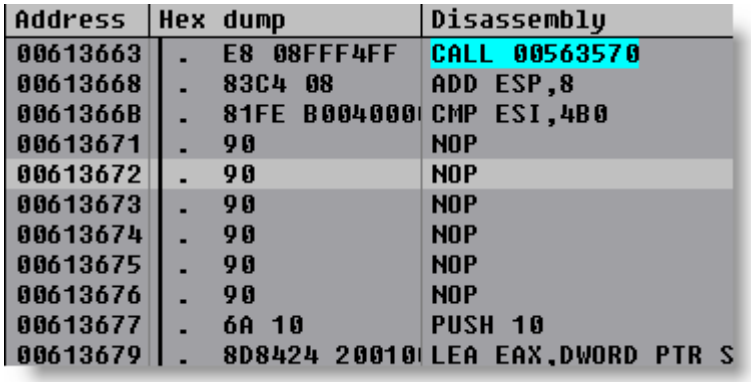
Y en el DiagramStudio 5.5 corresponde a la posición 613C00, abramos un Olly cargamos la 5.5 y lo comprobamos:



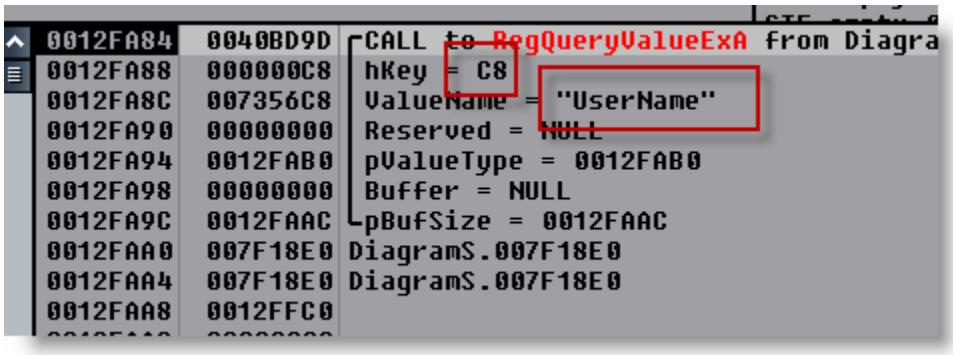
Ya tenemos donde buscar, Bajamos y vemos el call edx:



Y si entramos y bajamos en la función vemos la zona a parchear:

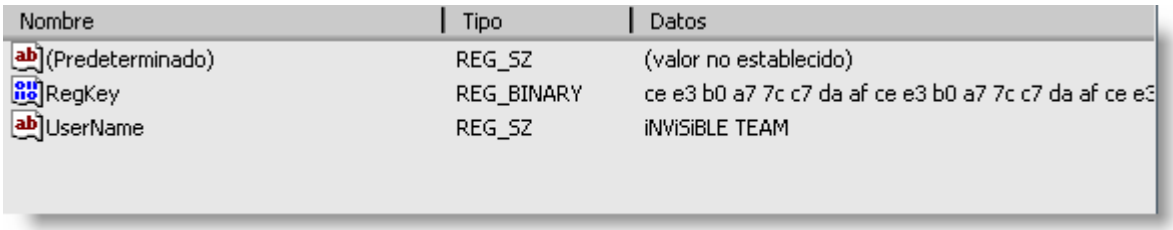


Con esto ya tenemos arreglado el programa, pero si probamos vemos que aún nos sale como no registrado ¿Qué pasa?, sencillamente el patcher también toca el registro, si abrimos en olly el DiagramStudio 5.4 y ponemos un hbp en RegQueryValueExA vemos que después de unas cuantas paradas lee el user name:



En View->Handles buscamos el C8 y vemos la clave:
HKEY_CURRENT_USER\Software\Gadwin Systems\DiagramStudio 5.4

La buscamos con el regedit:



Pues nos las creamos en HKEY_CURRENT_USER\Software\Gadwin Systems\DiagramStudio 5.5, copiamos el RegKey y en UserName ponemos el que queramos y ya está apañado.

Ya solo queda agradecer a Nico por su estupenda herramienta, a Ricardo por dárnosla a conocer y a ti por leerme.

En Getafe a 15 de Enero de 2.010

: