



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

Turbodiff es un plugin 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%20TURBODIFF%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 plugins 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.

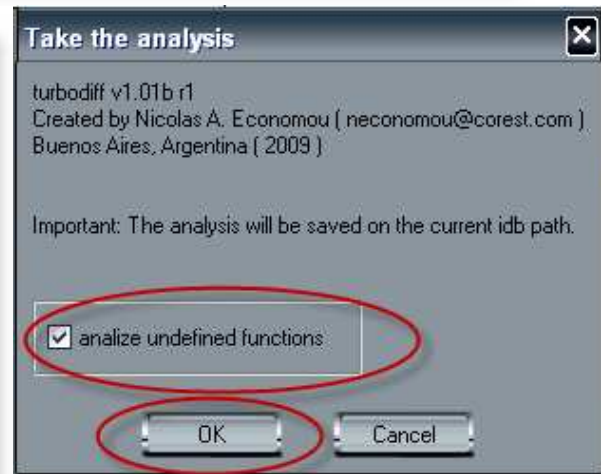
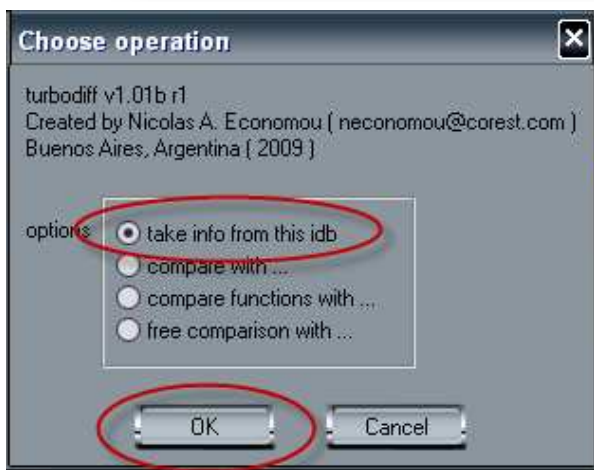
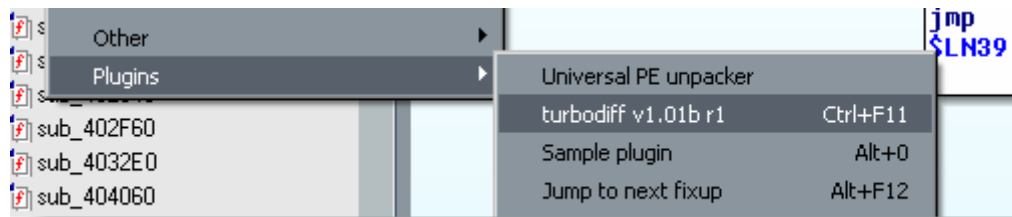
Trabajaremos sobre DiagramStudio 5.4 con un parche de Invisible team, a estas alturas no tengo el enlace, pero seguro que hay copias de seguridad colgadas de la red.

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-> plugins al turbodiff.

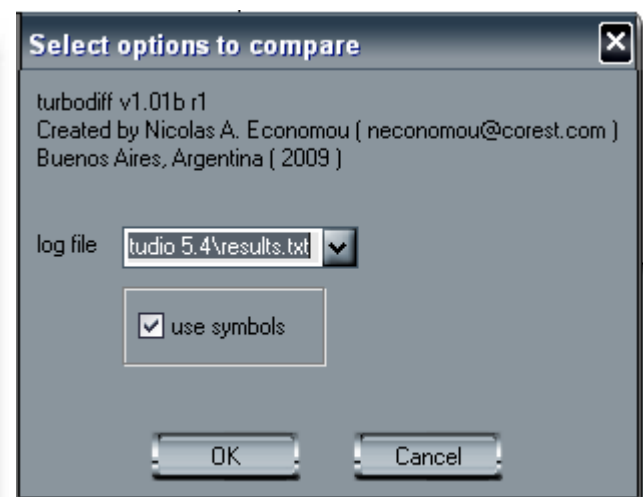
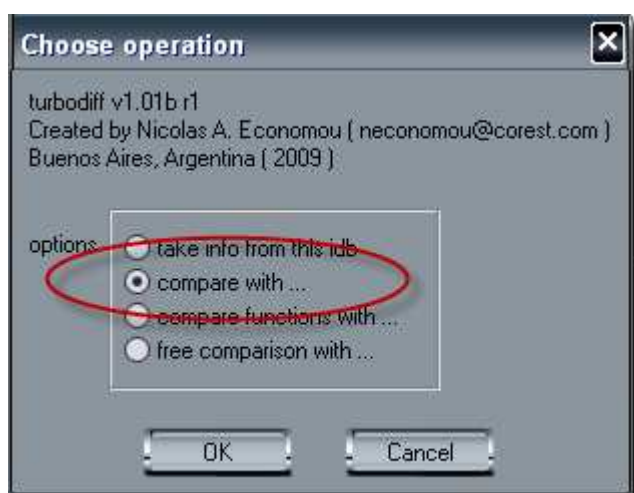


En la segunda ventana marco la opción de analize undefined functions porque de otra forma al comparar me tira una excepción.

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:



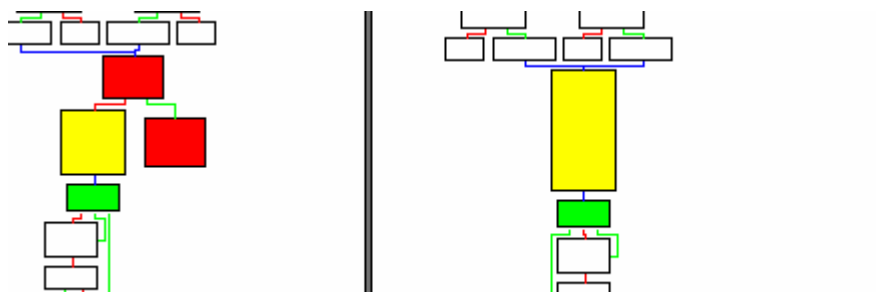
Elegimos el DiagramStudio.exe de la versión 5.4 y en un momento tenemos la ventana con todas las funciones “matcheadas”, al final vemos las que han cambiado y algunas que no pudo matchear:

Turbodiff results				
category	address	name	address	name
identical	6fd304	sub_6fd304_undefined	6fd304	sub_6fd304_undefined
identical	6fd338	sub_6fd338_undefined	6fd338	sub_6fd338_undefined
identical	6fd909	sub_6fd909_undefined	6fd909	sub_6fd909_undefined
identical	6fd90f	sub_6fd90f_undefined	6fd90f	sub_6fd90f_undefined
identical	5c80e0	sub_5C80E0	5c80e0	sub_5C80E0
changed	5493e0	sub_5493E0	5493e0	sub_5493E0
changed	563c80	sub_563C80	563c80	sub_563C80
changed	5df520	sub_5DF520	5df520	sub_5DF520
changed	5df840	sub_5DF840	5df840	sub_5DF840
changed	6130f0	sub_6130F0	6130f0	sub_6130F0
unmatched 1	613175	sub_613175	-	-
unmatched 2	-	-	613175	sub_613175
unmatched 2	-	-	54963b	sub_54963b_undefined
unmatched 2	-	-	563edb	sub_563edb_undefined

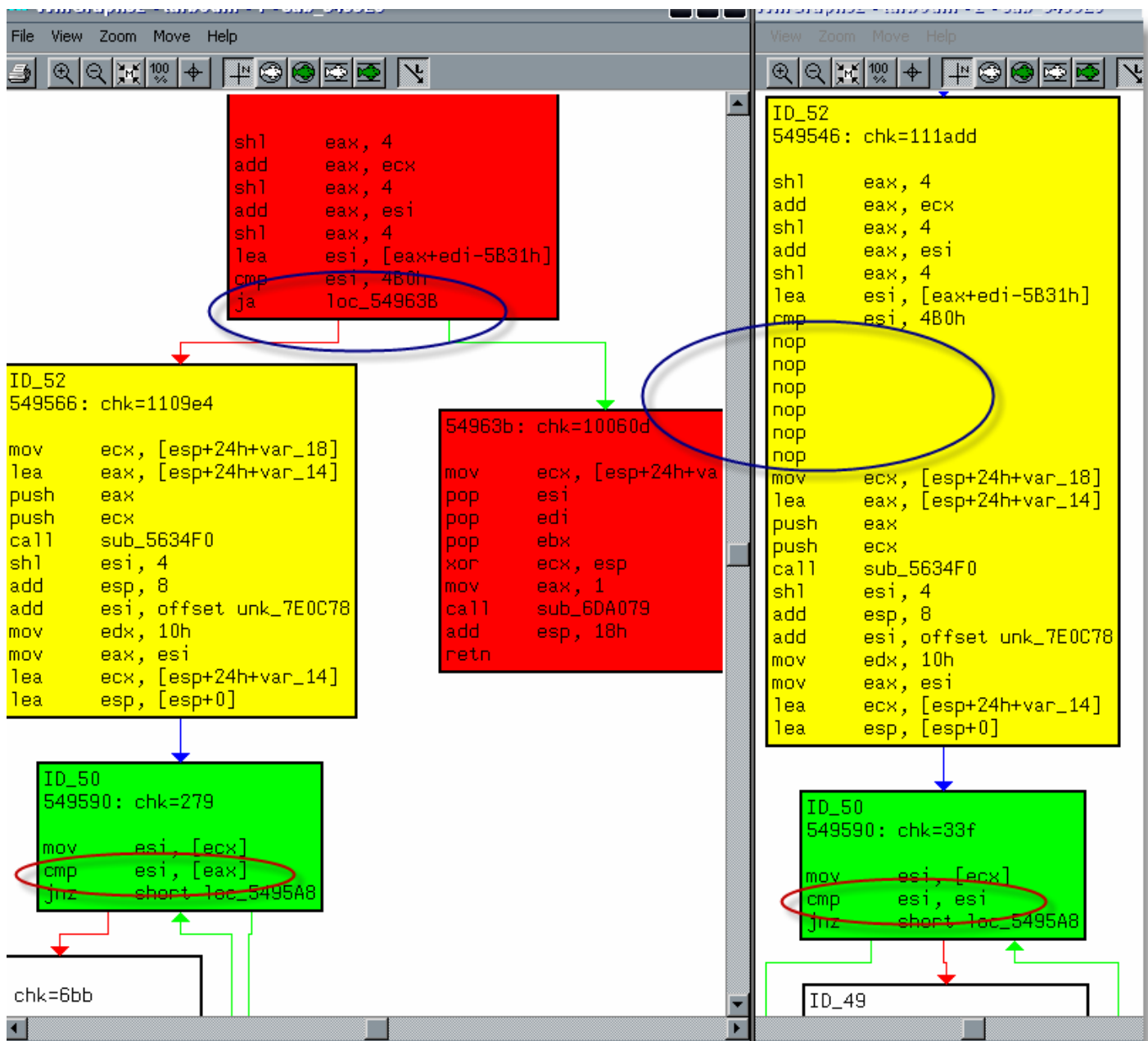
Line 26883 of 26886

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:

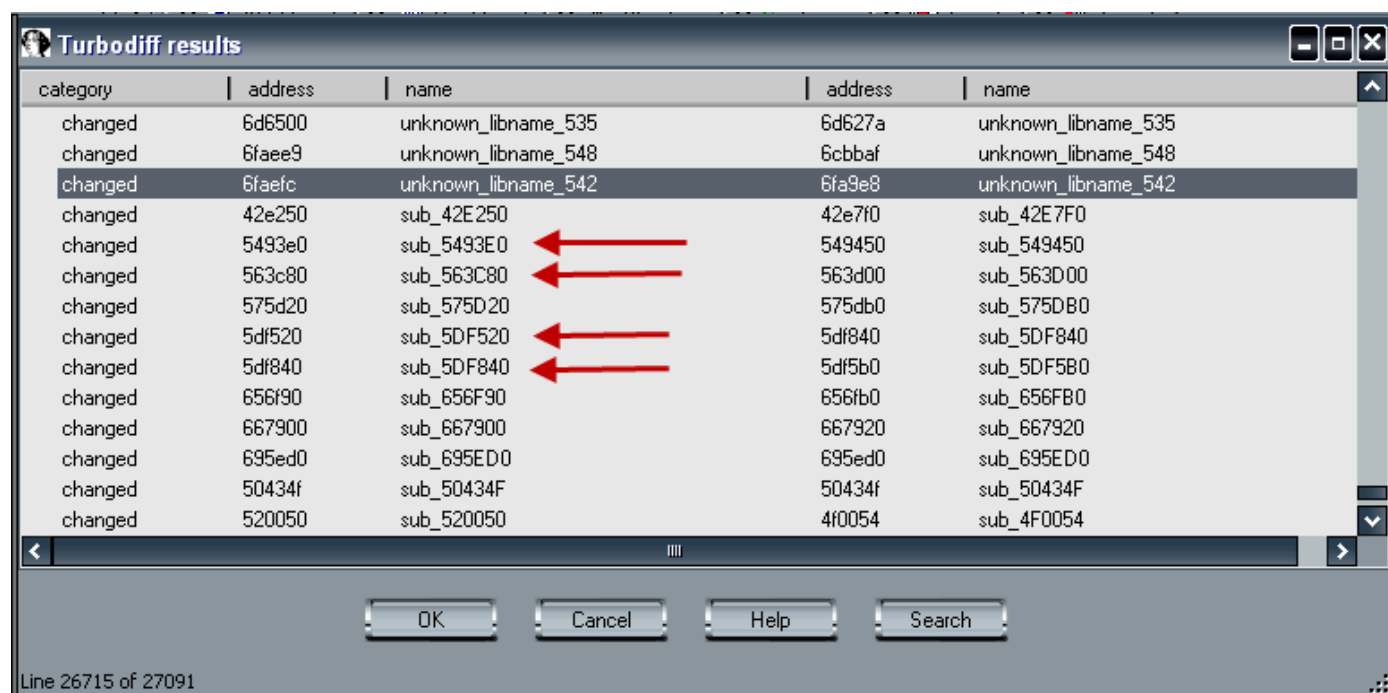


Sencillamente nopearon el ja 54963B y cambiaron la comparación `cmp esi, [eax]` por `cmp esi, esi`.

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.

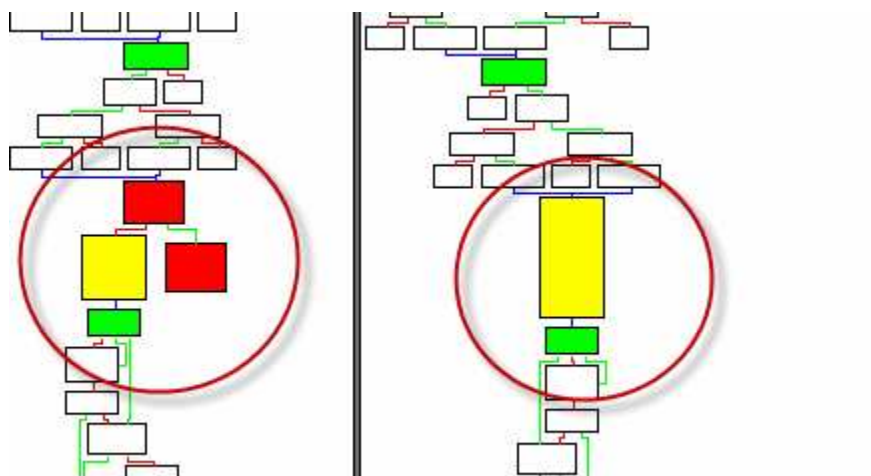
Pues vamos al lío, abrimos en IDA el DiagramStudio.exe de la versión 5.4 (el parcheado) y lo comparamos el turbotdiff con el DiagramStudio.exe 5.5 (el que queremos parchear), podemos ver que hay muchas más funciones changed y unmatched, pero nosotros ya sabemos las cinco que queremos:



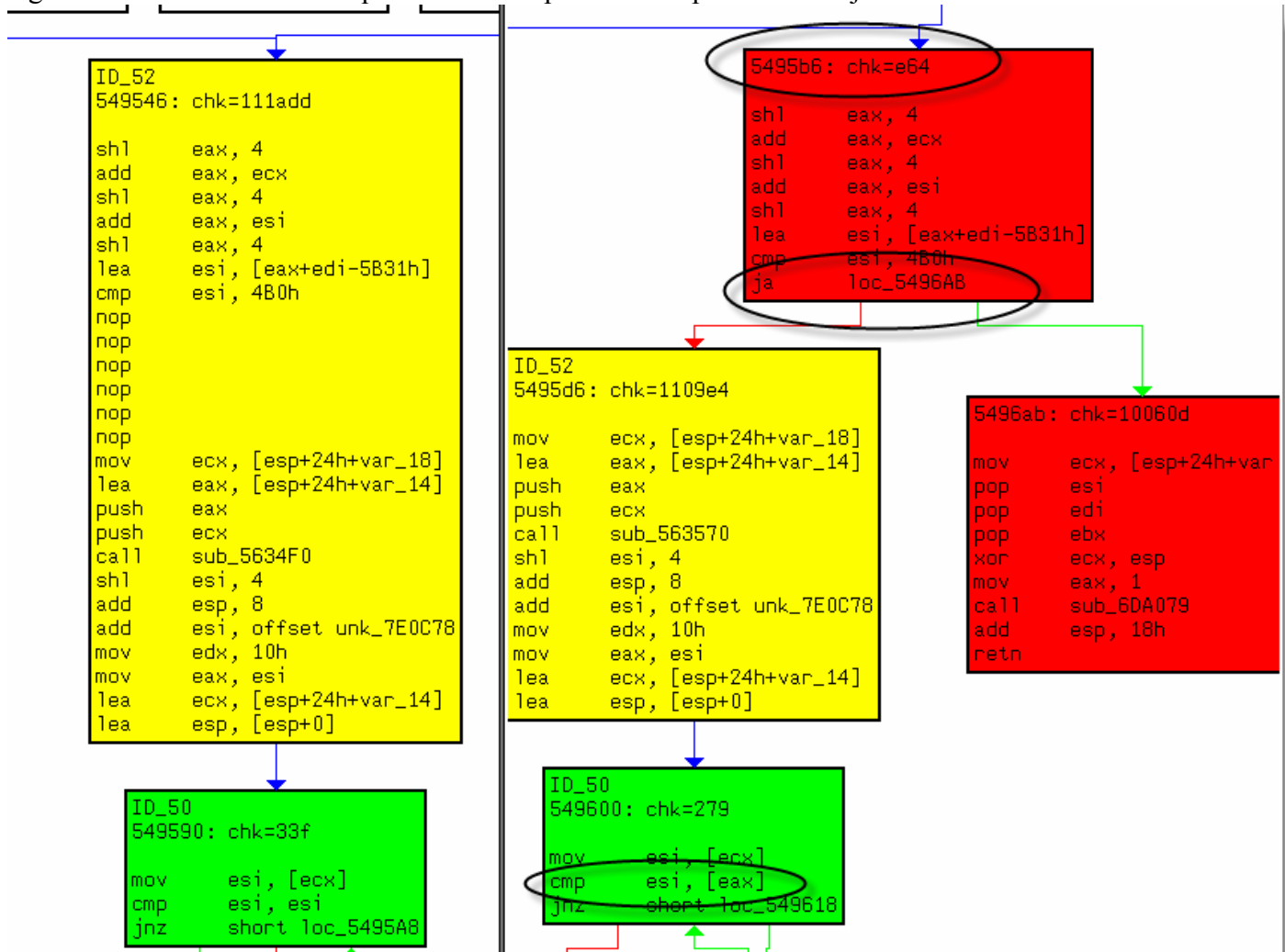
Vemos que falta la 6130F0 que está unmatched. Esa la dejaremos para el final:

unmatched 1	612b10	sub_612B10
unmatched 1	6130f0	sub_6130F0
unmatched 1	613175	sub_613175
unmatched 1	616175	sub_616175

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:

```

005495B3 . 8 SUB EAX,37
005495B6 > C SHL EAX,4
005495B9 . 0 ADD EAX,ECX
005495BB . C SHL EAX,4
005495BE . 0 ADD EAX,ESI
005495C0 . C SHL EAX,4
005495C3 . 8 LEA ESI,DWORD PTR DS:[EAX+1
005495C6 . 8 CMP ESI,4B0
005495D0 . 0 JA 005496AB
005495D6 . 8 MOV ECX,DWORD PTR SS:[ESP+1
005495DA . 8 LEA EAX,DWORD PTR SS:[ESP+
005495DE . 5 PUSH EAX
005495DF . 5 PUSH ECX
005495E0 . E CALL 00563570
005495E5 . C SHL ESI,4
005495E8 . 8 ADD ESP,8
005495EB . 8 ADD ESI,7E0C78
  
```

```

005495B6 > C SHL EAX,4
005495B9 . 0 ADD EAX,ECX
005495BB . C SHL EAX,4
005495BE . 0 ADD EAX,ESI
005495C0 . C SHL EAX,4
005495C3 . 8 LEA ESI,DWORD PTR DS
005495C6 . 8 CMP ESI,4B0
005495D0 . 9 NOP
005495D1 . 9 NOP
005495D2 . 9 NOP
005495D3 . 9 NOP
005495D4 . 9 NOP
005495D5 . 9 NOP
005495D6 . 8 MOV ECX,DWORD PTR SS
005495DA . 8 LEA EAX,DWORD PTR SS
  
```

Y cambiamos la comparación que está algo más abajo:

005495FC	. 8	LEA ESP,DWORD PTR SS:[ESP]	005495FC	. 8	LEA ESP,DWORD PTR SS:[ESP]
00549600	> 8	MOV ESI,DWORD PTR DS:[ECX]	00549600	> 8	MOV ESI,DWORD PTR DS:[ECX]
00549602	. 3	CMP ESI,DWORD PTR DS:[EAX]	00549602	. 3	CMP ESI,ESI
00549604	. 7	JNZ SHORT 00549618	00549604	. 7	JNZ SHORT 00549618
00549606	. 8	SUB EDX,4	00549606	. 8	SUB EDX,4

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

			ST3 empty
			ST4 empty
			ST5 empty
	0012E088	00613D70	RETURN to DiagramS.00613D70
	0012E08C	12124060	
	0012E090	0012E0D8	
	0012E094	00000000	
	0012E098	6FDB5100	
	0012E09C	12124060	
	0012E0A0	1211D578	

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

Address	Hex dump	Disassembly
00613D6C	. 8BCE	MOV ECX,ESI
00613D6E	. FFD2	CALL EDX
00613D70	. 8B46 74	MOV EAX,DWORD PTR DS:[ECX]
00613D73	. 83B8 A8020000	CMP DWORD PTR DS:[000200A8],EAX
00613D7A	. 75 18	JNZ SHORT 00613D84
00613D7C	. 8B4C24 6C	MOV ECX,DWORD PTR DS:[00246C4C],EAX
00613D80	. 8B5424 68	MOV EDX,DWORD PTR DS:[0024684C],EAX
00613D84	. 8B06	MOV EAX,DWORD PTR DS:[00000006],EAX
00613D86	. 8B80 EC000000	MOV EAX,DWORD PTR DS:[000000EC],EAX
00613D8C	. 57	PUSH EDI
00613D8D	. 51	PUSH ECX
00613D8E	. 52	PUSH EDX
00613D8F	. 55	PUSH EBP
00613D90	. 8BCE	MOV ECX,ESI
00613D92	. FFD0	CALL EAX
00613D94	> 8B45 0C	MOV EAX,DWORD PTR DS:[00000045],EAX
00613D97	. 3B45 10	CMP EAX,DWORD PTR DS:[00000045],EAX

Ahora subimos hasta el inicio de la función:

00613B7E	CC	INT3
00613B7F	CC	INT3
00613B80	. 6A FF	PUSH -1
00613B82	. 68 00967000	PUSH 709600
00613B87	. 64:A1 000000	MOV EAX,DWORD PTR FS:[0]
00613B8D	. 50	PUSH EAX
00613B8E	. 83EC 44	SUB ESP,44
00613B91	. 53	PUSH EBX
00613B92	. 55	PUSH EBP
00613B93	. 56	PUSH ESI

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

suspicious +	60faf0	sub_60FAF0	60fb70	sub_60FB70
suspicious +	613b80	sub_613B80	613c00	sub_613C00
suspicious +	613df0	sub_613DF0	613e70	sub_613E70
suspicious +	614b70	sub_614B70	614bf0	sub_614BF0

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

Address	Hex dump	Disassembly
00613C00	. 6A FF	PUSH -1
00613C02	. 68 90967000	PUSH 709690
00613C07	. 64:A1 000000	MOV EAX,DWORD PTR FS:[0]
00613C0D	. 50	PUSH EAX
00613C0E	. 83EC 44	SUB ESP,44
00613C11	. 53	PUSH EBX
00613C12	. 55	PUSH EBP
00613C13	. 56	PUSH ESI
00613C14	. 57	PUSH EDI

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

00613DEB	. 55	PUSH EBP
00613DEC	. 8BCE	MOV ECX,ESI
00613DEE	. FFD2	CALL EDX
00613DF0	. 8B46 74	MOV EAX,DWORD PTR DS:[ESI+74]
00613DF3	. 83B8 A8020000	CMP DWORD PTR DS:[ESI+A8020000],0
00613DFA	. 75 18	JNZ SHORT 00613E00
00613DFC	. 8B4C24 6C	MOV ECX,DWORD PTR DS:[ESI+6C]
00613E00	. 8B5424 68	MOV EDX,DWORD PTR DS:[ESI+68]
00613E04	. 8B06	MOV EAX,DWORD PTR DS:[ESI+6]
00613E06	. 8B80 EC000000	MOV EAX,DWORD PTR DS:[ESI+EC000000]
00613E0C	. 57	PUSH EDI
00613E0D	. 51	PUSH ECX
00613E0E	. 52	PUSH EDX
00613E0F	. 55	PUSH EBP
00613E10	. 8BCE	MOV ECX,ESI
00613E12	. FFD0	CALL EAX
00613E14	. 8B45 0C	MOV EAX,DWORD PTR DS:[ESI+0C]
00613E17	. 3B45 10	CMP EAX,DWORD PTR DS:[ESI+10]
00613E1A	. 74 09	JE SHORT 00613E20
00613E1C	. 6A 00	PUSH 0

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

Address	Hex dump	Disassembly
00613663	. E8 08FFF4FF	CALL 00563570
00613668	. 83C4 08	ADD ESP,8
0061366B	. 81FE B0040000	CMP ESI,4B0
00613671	. 90	NOP
00613672	. 90	NOP
00613673	. 90	NOP
00613674	. 90	NOP
00613675	. 90	NOP
00613676	. 90	NOP
00613677	. 6A 10	PUSH 10
00613679	. 8D8424 200100	LEA EAX,DWORD PTR S

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:

0012FA84	0040BD9D	CALL to RegQueryValueExA from DiagramStudio
0012FA88	000000C8	hKey = C8
0012FA8C	007356C8	ValueName = "UserName"
0012FA90	00000000	Reserved = NULL
0012FA94	0012FAB0	pValueType = 0012FAB0
0012FA98	00000000	Buffer = NULL
0012FA9C	0012FAAC	pBufSize = 0012FAAC
0012FAA0	007F18E0	DiagramS.007F18E0
0012FAA4	007F18E0	DiagramS.007F18E0
0012FAA8	0012FFC0	

En View->Handles buscamos el C8 y vemos la clave:

HKEY_CURRENT_USER\Software\Gadwin Systems\DiagramStudio 5.4

La buscamos con el regedit:

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
RegKey	REG_BINARY	ce e3 b0 a7 7c c7 da af ce e3 b0 a7 7c c7 da af ce e3
UserName	REG_SZ	INVISIBLE TEAM

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

: