TARGET	OrgBussiness Sports Rental Calendar Bussiness for Workgroup(Client)
VERSION	2,3
Packer/Protector	ASProtect v1.40 Build 04.01
LIMITACION	14 dias Trial(Impuesto por Asprotect)
OBJETIVO	UNPACKING
NIVEL DIFICULTAD	2
CRACKER	+ERISOFT
FECHA	15/12/11

Descarga:
http://www.orgbusiness.com/sportsrentalcalendarforworkgroup.html

Introducción y Liberación de Responsabilidad

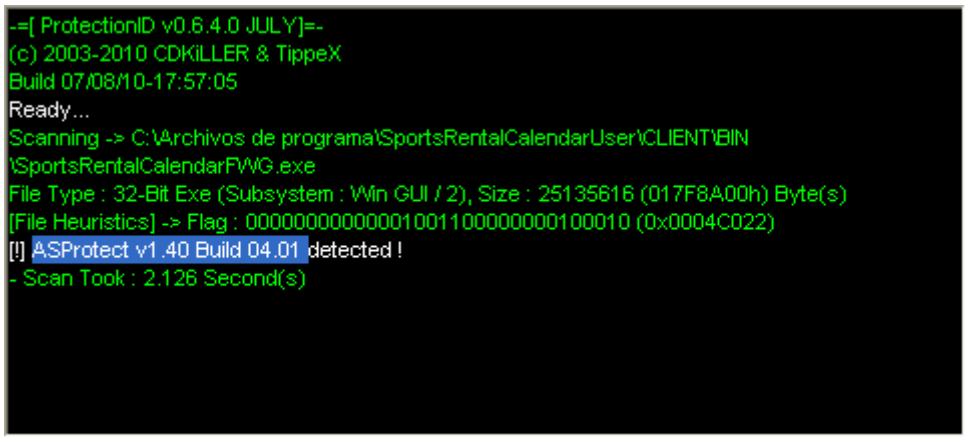
Bueno este escrito se realiza para dar mi perspectiva del unpacking de este tipo de protección para la versión indicada puede que hayan caminos mas fáciles, pero el elegido me ha funcionado y solucionado si alguien quiere denigrar el trabajo hecho o hacer saber que se puede de otra manera que postee un tutorial mejor y lo demuestre...

Este escrito esta previsto con fines educacionales si alguien o alguno de los lectores lo usa con fines ilegales el autor se libera de toda responsabilidad legal ante los hechos.

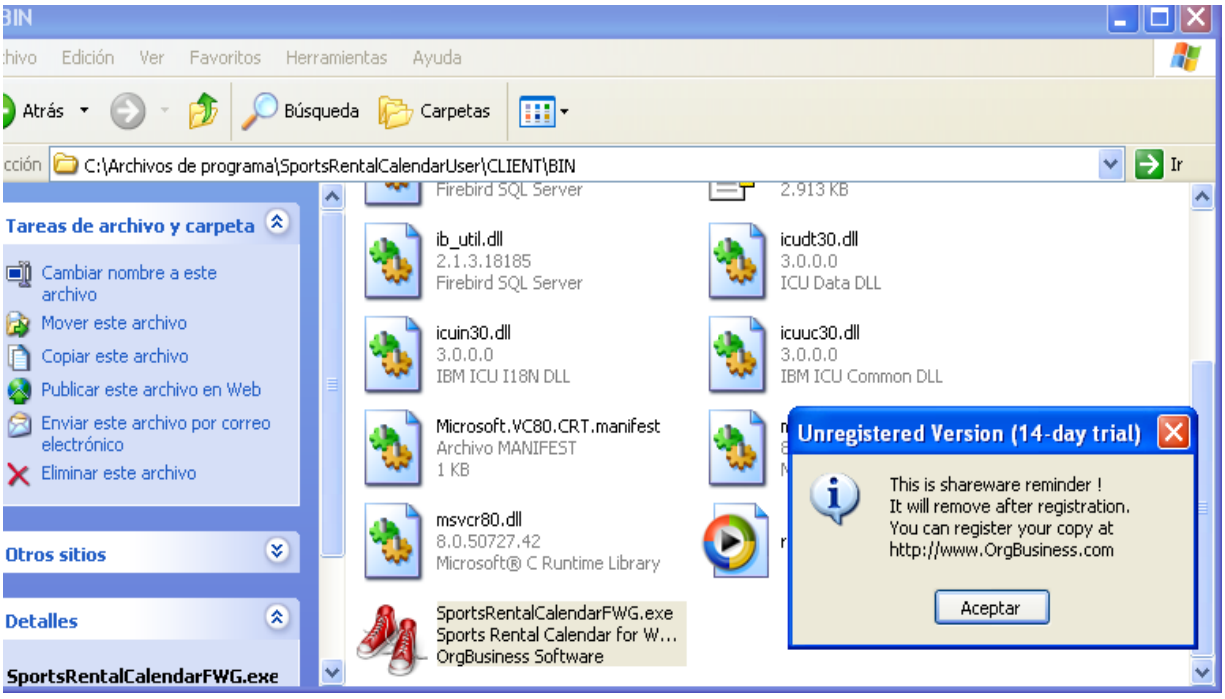
Analizando la Victima.

Yo en lo personal uso el Protección ID como detector de packers y protectors para mi tiene un poco mas de veracidad vrs el RDG este ultimo en muchos casos me dice que no tiene protectors por eso de mi decisión.

Analizamos y este es el resultado que no arroja:



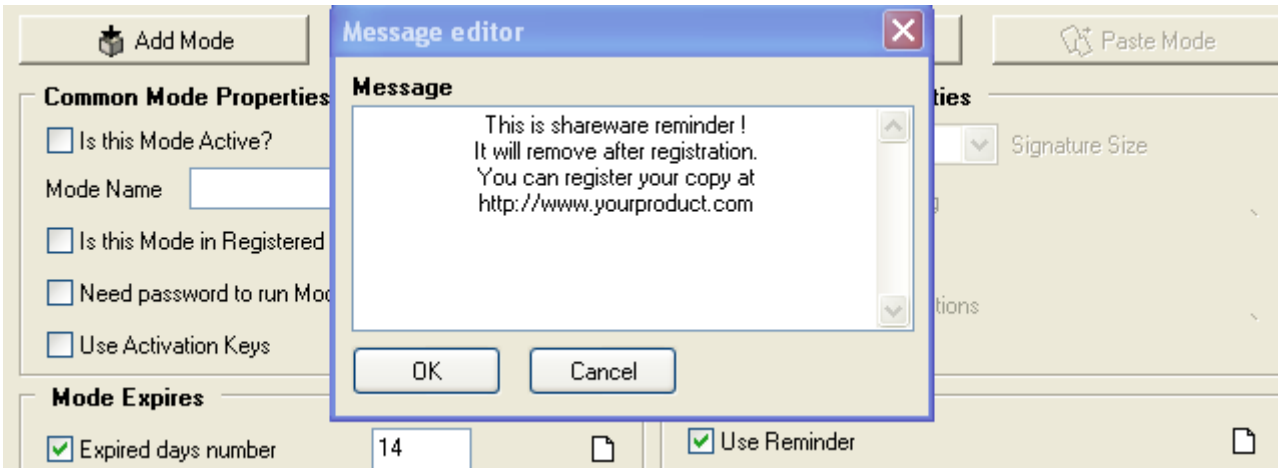
Bueno nos hace saber que es un asprotect 1,40 build 04,01 ,bien lo ponemos a correr sin olly debugger para ver las limitaciones doble click y esto nos aparece:



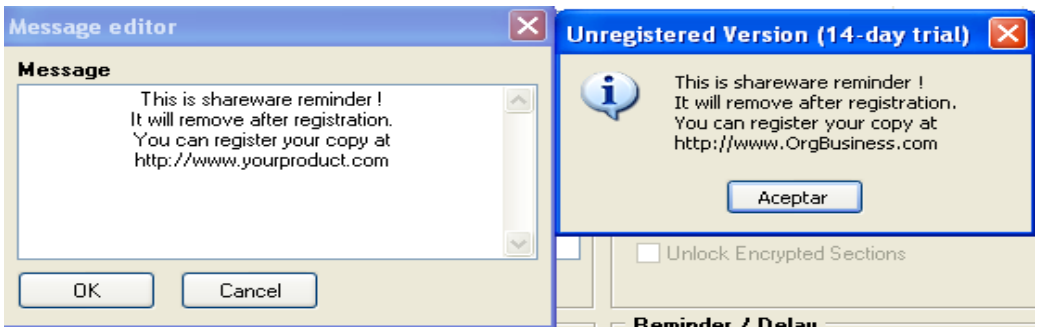
Luego damos click en aceptar y el cabroncete arranca dandonos esta caratula:

Bien hasta aca no hemos hecho nada relevante solo ver las limitaciones y un previo analisis del packer.

Sentandonos a hacer un analisis previo algunos dirian que el Messagebox de los 14 dias trial lo crea el programa cuando se ejecuta... En realidad la respuesta correcta es no, lo crea el protector y prueba de esto es la imagen que adjunto de la interfaz de asprotect:

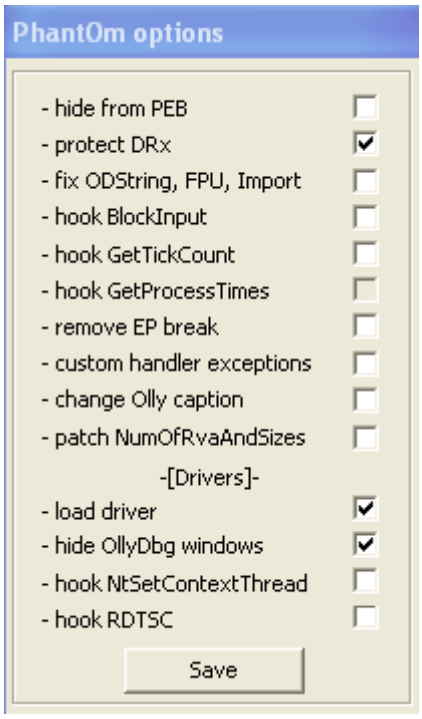


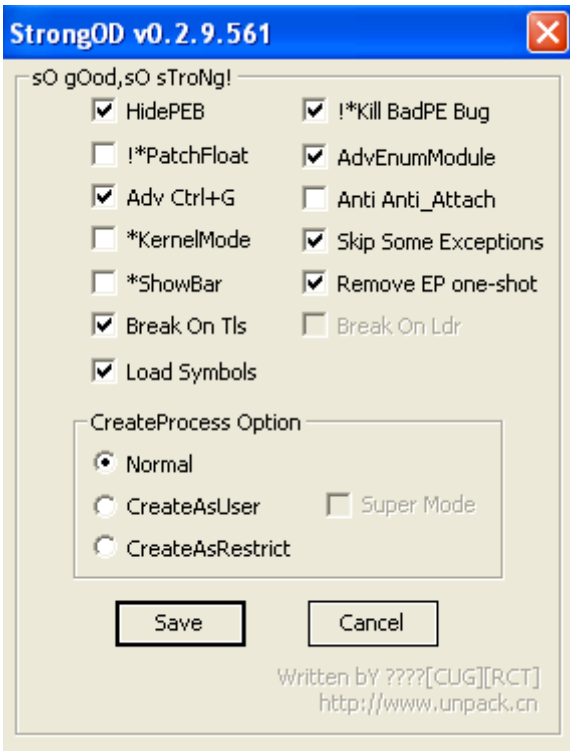
Comparamos con la del Programa joder son las mismas :) :



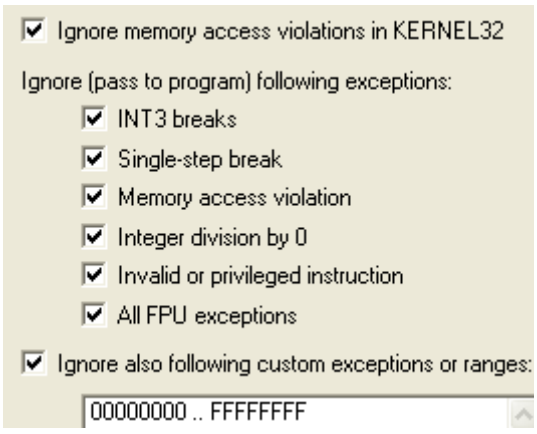
Ok entonces ya tenemos que el proggie toma los 14 dias trial, pero quien los maneja es asprotect, soluciones bueno desempacamos el .exe y se quita la limitacion de los 14 dias trial moraleja Confia en los Protectors y ellos te daran el Palo.

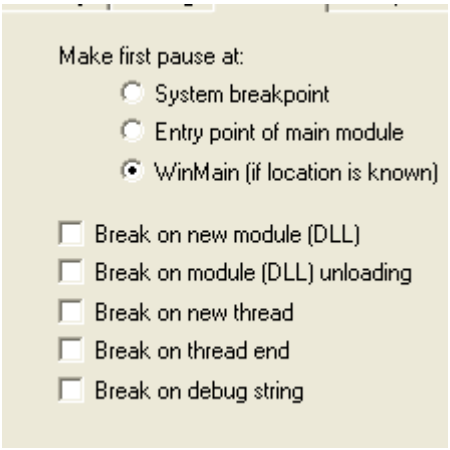
Abrimos en el Ollydebugger y miramos que este con estos plugins y asi configurado el plugin phantom y Strong Od nos curamos en salud:





Y las excepciones de Olly asi y los events:

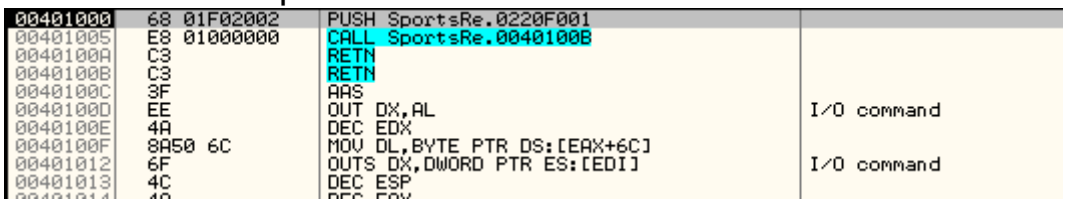




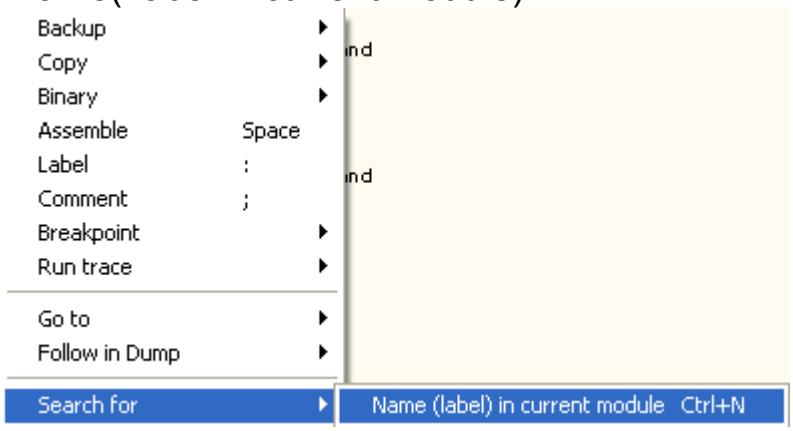
Bueno listo estamos preparados para la guerra, cabe destacar que con esta configuración pueden atacar tranquilamente un execryptor 2,41 en Xp se los digo por experiencia propia.

Atacando al Mutante.

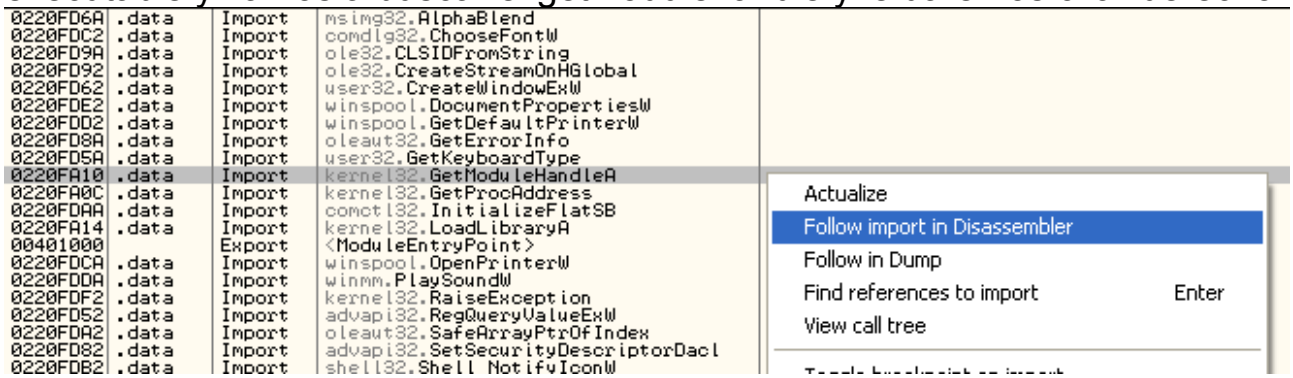
Bueno cargamos la victima en nuestro olly y vemos esto que es la tipica entrada de los asprotetas:



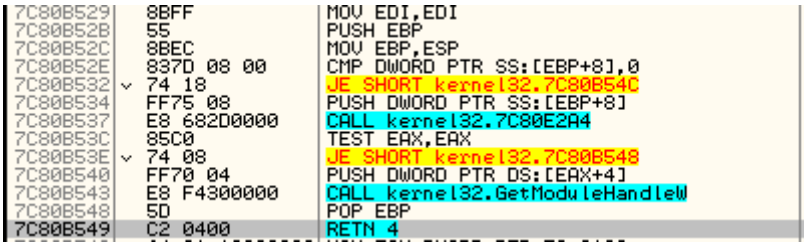
Entonces nos vamos a dar click derecho nos saldra el dialoguito siguiente y damos click en Name(Label in current Module):



Luego de dar click hay veremos lo siguiente que son los module para el executable y vamos a buscar el getmodulehandle y le daremos click derecho:

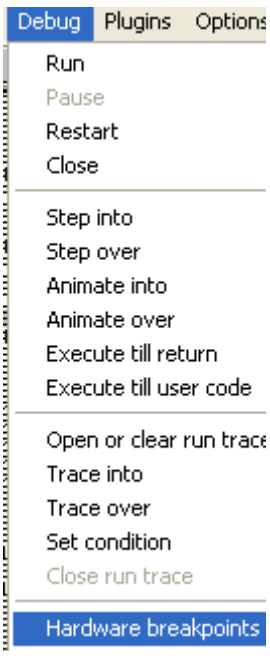


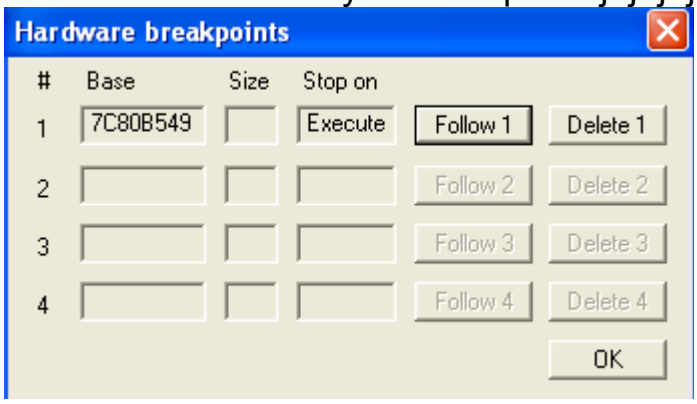
Damos en la opción anterior y nos sale lo siguiente:



Vamos a ponerle un Harware Breack Point on Execution usando el plugin Command Line en el Ret anotamos la direccion 7C80B549 de la funcion anterior y lo ponemos asi damos Enter:

Verificamos si se puso en execution asi y vemos que si jojojojojo:





Bueno ustedes estaran preguntando por que getmodulehandle bueno con esta api caeremos cerca del lugar de los hechos ojo no en el mero Oep pero veran que si muy cerca mas adelante veran el truquito jojojo.

Por que pusistes un hardware on execution en el ret y no en el inicio??

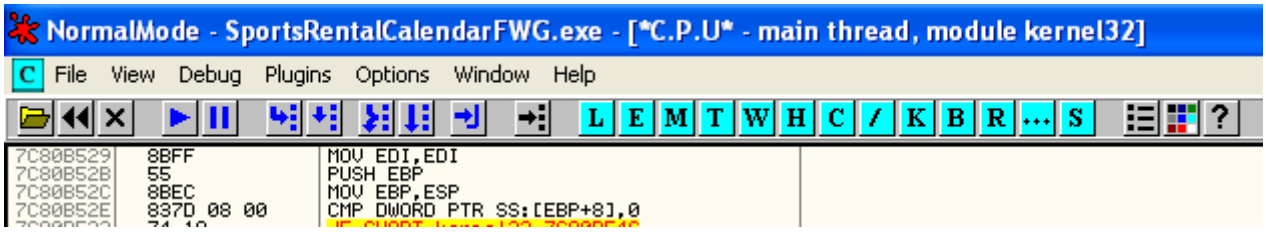
Bueno por la detección básicamente, packers como armadillo y execryptor detectan los bps y los hwbps en las 3 primeras lineas de las apis entonces el ret no esta en las 3 primeras lineas así que esa es la razón.

Y ahora que sigue nos tienes en ascuas joder me voy a leer a otro lado??

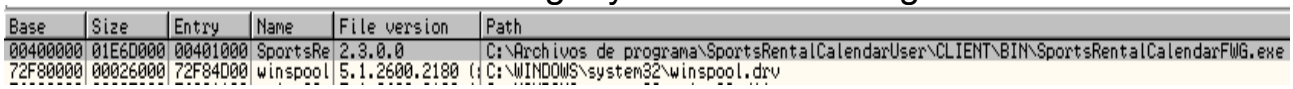
“Quien tiene paciencia, obtendrá lo que desea.””

Benjamin Franklin (1706-1790) Estadista y científico estadounidense.

Algunos veran que despues de poner el HWBP se quedo el olly aca que ese no es el codigo del ejecutable :



Como vuelvo a ver el codigo del executable y no de la api, pues simple damos click en la E(Executables Module) veremos lo siguiente damos dos click en el nombre de nuestro target y volvimos al codigo:



Ok una vez vueltos al codigo que hacemos bueno le vamos a dar click en run cual sera el objetivo pues simple, esta api parara miles de veces pero la ultima ves que pare y nos muestre la pantalla sera nuestro challenge:

Y paramos aca vamos a enfocarnos en la pila osea en el stack esta es nuestra primer parada:

Damos run y vemos la segunda parada:

Damos run y vemos la tercera parada:

Y asi sucecivamente hasta que en la parada numero 16 escuchamos el Messagebee(El pitido del messagebox) damos run tres veces consecutivas y nos sale nuestro bad boy el el taskbar, luego al tratar de ganar el enfoque el debugger para de nuevo le damos run dos veces y aparece el bichin:

Le damos click en aceptar y seguimos ya estamos muy cerca...

Luego para aca estas paradas las nombraremos despues del messagebox osea esta seria la primera despues de haber dado click en OK:

```
0012FE80  7711D624  RETURN to oleaut32.7711D624 from kernel32.GetModuleHandleA
0012FE84  7711D458  ASCII "ole32.dll"
0012FE88  0012FEBC
0012FE8C  7711D74B  RETURN to oleaut32.7711D74B from oleaut32.7711D779
0012FE90  770F49EC  oleaut32.770F49EC
0012FE94  00000000
```

Ahora vamos a bajar el stack la barrita del stack

No le daremos mas run al olly solo bajaremos la barra de desplazamiento del stack osea vamos a ver los valores que se ha empujado mas antes que este que estamos viendo y llegamos a esta parte: Jojojojojo

```
0012FF34  198C00A2  RETURN to 198C00A2 from 198C00AD
0012FF38  198C00A2  RETURN to 198C00A2 from 198C00AD
0012FF3C  00BF4C8C  SportsRe.00BF4C8C
0012FF40  00BF4C94  SportsRe.00BF4C94
0012FF44  0012FF6C
0012FF48  00405744  RETURN to SportsRe.00405744 from SportsRe.00405698
0012FF4C  00409AE7  RETURN to SportsRe.00409AE7 from SportsRe.00405700
0012FF50  00400000  ASCII "MZP"
0012FF54  00BFBBA5  RETURN to SportsRe.00BFBBA5 from SportsRe.00409AA8
0012FF58  00400000  ASCII "MZP"
0012FF5C  0012FFE0  Pointer to next SEH record
```

Bueno aca vemos dos MZP pero el que interesa es el primer valor osea el 00BFBBA5 este no es el OEP pero es el valor mas cercano a el ahora lo que haremos sera ir a ese valor en dissambler como lo hacemos asi con el command line y damos enter:

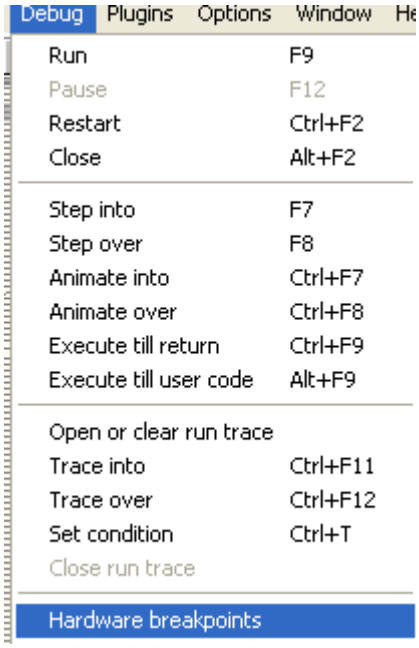
Luego de enter veremos esto, lo que subrayo de amarillo es el OEP y bueno lo que esta subrayado de naranja es la direccion a la que le hizimos follow:

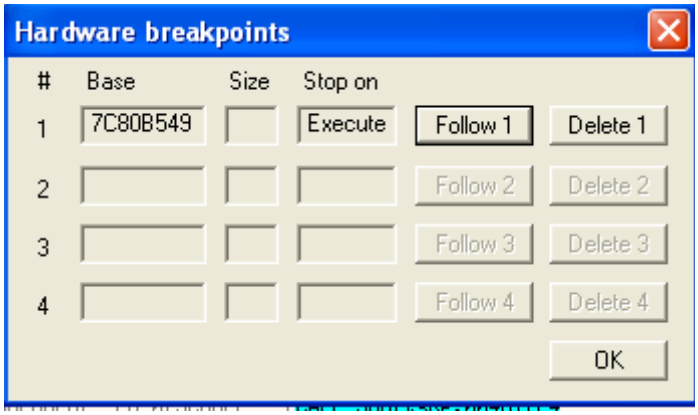
```
00BFBB94   55              PUSH EBP
00BFBB95   8BEC            MOV EBP,ESP
00BFBB97   83C4 F0         ADD ESP,-10
00BFBB9A   53              PUSH EBX
00BFBB9B   B8 8C4CBF00     MOV EAX,SportsRe.00BF4C8C
00BFBBA0   E8 03DF80FF     CALL SportsRe.00409AA8
00BFBBA5   8B1D FCC3C000   MOV EBX,DWORD PTR DS:[C0C3FC]   SportsRe.00C131E0
00BFBBAB   8B03            MOV EAX,DWORD PTR DS:[EBX]
00BFBBAD   E8 2A5C8DFF     CALL SportsRe.004D17DC
00BFBBB2   8B03            MOV EAX,DWORD PTR DS:[EBX]
00BFBBB4   B2 01           MOV DL,1
00BFBBB6   E8 95778DFF     CALL SportsRe.004D3350
00BFBBBB   8B03            MOV EAX,DWORD PTR DS:[EBX]
00BFBBBD   BA D8BCBF00     MOV EDX,SportsRe.00BFBCD8   UNICODE "Sports Rental Calendar for Workgroup"
```

Luego de aca ustedes se preguntaran joder pero no parastes en el oep y si no en unas lineas abajo ahora como coña le haremos para parar en el oep anotamos primero la direccion que en mi caso es 00BFBB94.

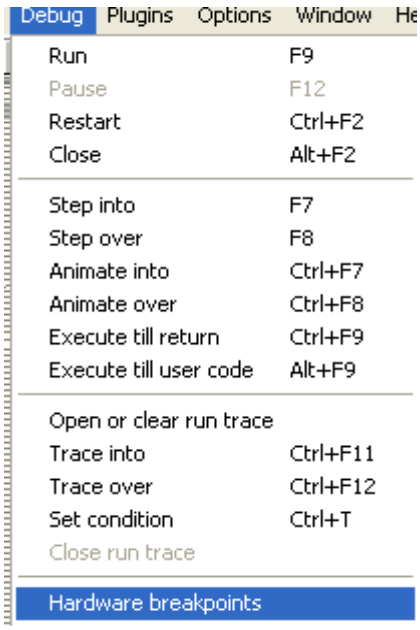
Reiniciamos ollydebugger como lo hacemos asi con el boton que subraye de amarillo vean en la parte de arriba jejeje:

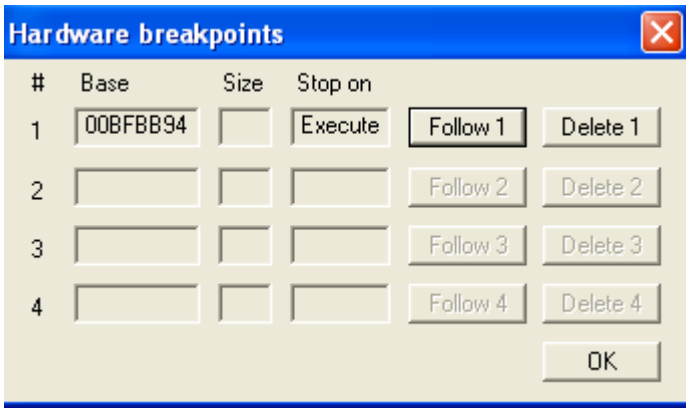
Ahora volvimos al tipico entrypoint de los asprotect borramos todos los Hardware breack point que hayamos puesto esto lo hacemos asi y nos aparecera el dialogo y le damos en delete1:





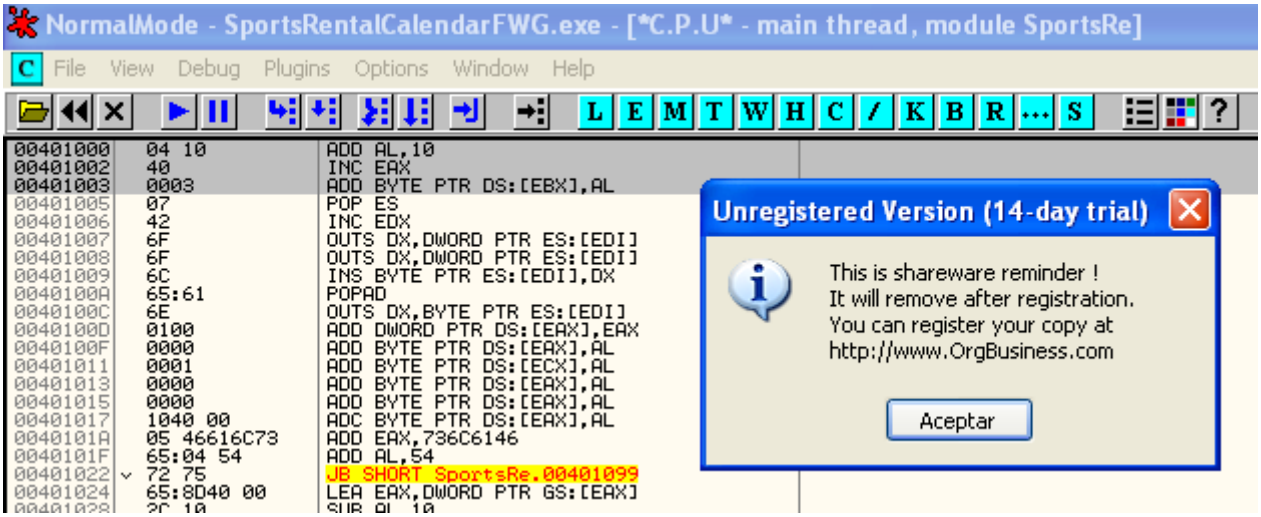
Ok ahora si que estamos en blanco y en el entry point tipico de los asprotetas simple nos toca parar en el OEP para eso pondremos un Hardware Break Point on Execution de esta manera damos enter ,verificamos que esta puesto:



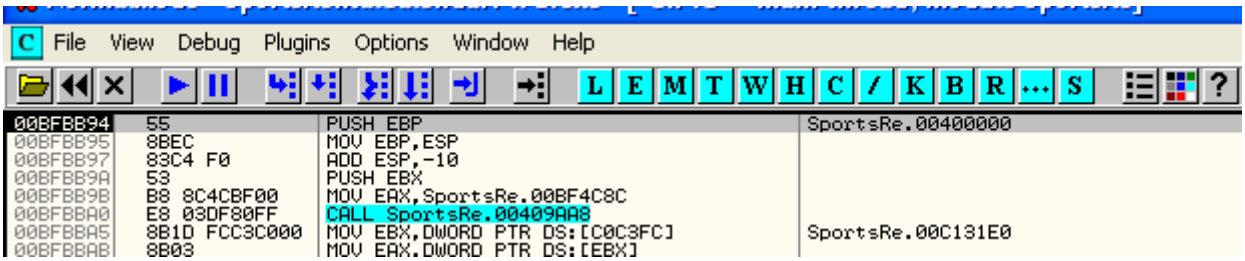


Luego damos click en Run:

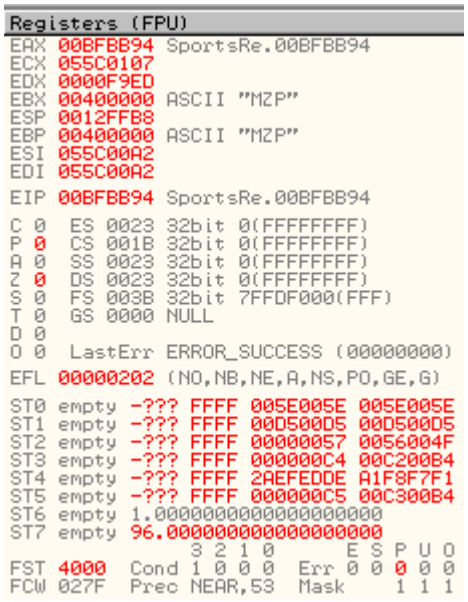
Y sale nuestro bad boy:



Le damos click en aceptar y vemos esto Estamos parados en el OEP:

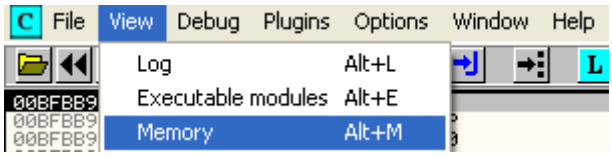


Los registros vemos esto y en el stack:

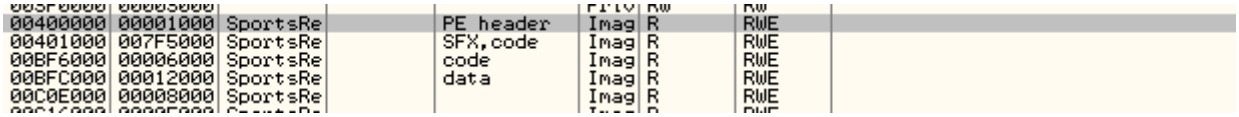


Dumpeando e Historias de la IAT

Ojo no cerramos el olly lo tenemos que dajar parado en el OEP, estando parados en el oep vamos a proceder con el dumping antes sacaremos el RVA del OEP previamente anotamos la direccion del OEP y utilizaremos la casa SirPe para hacer el dump, para proceder con el dump vamos a ver de cuanto es el start address y el EntryPoint nos vamos a ver el memory asi que lo hacemos asi y vemos esto:



Vemos lo siguiente:

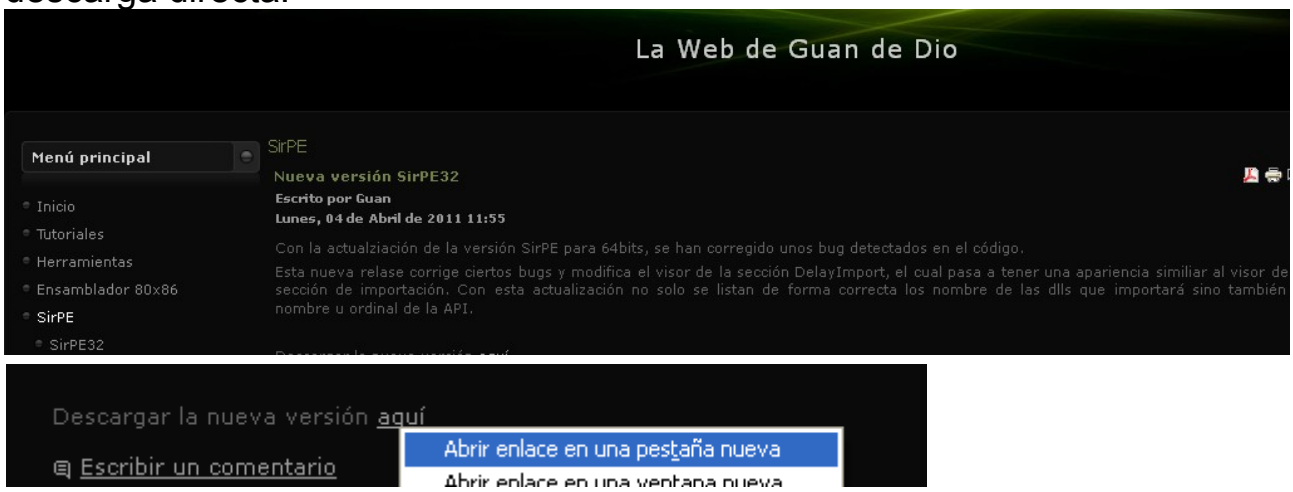


Ok Entrypoint: 400000

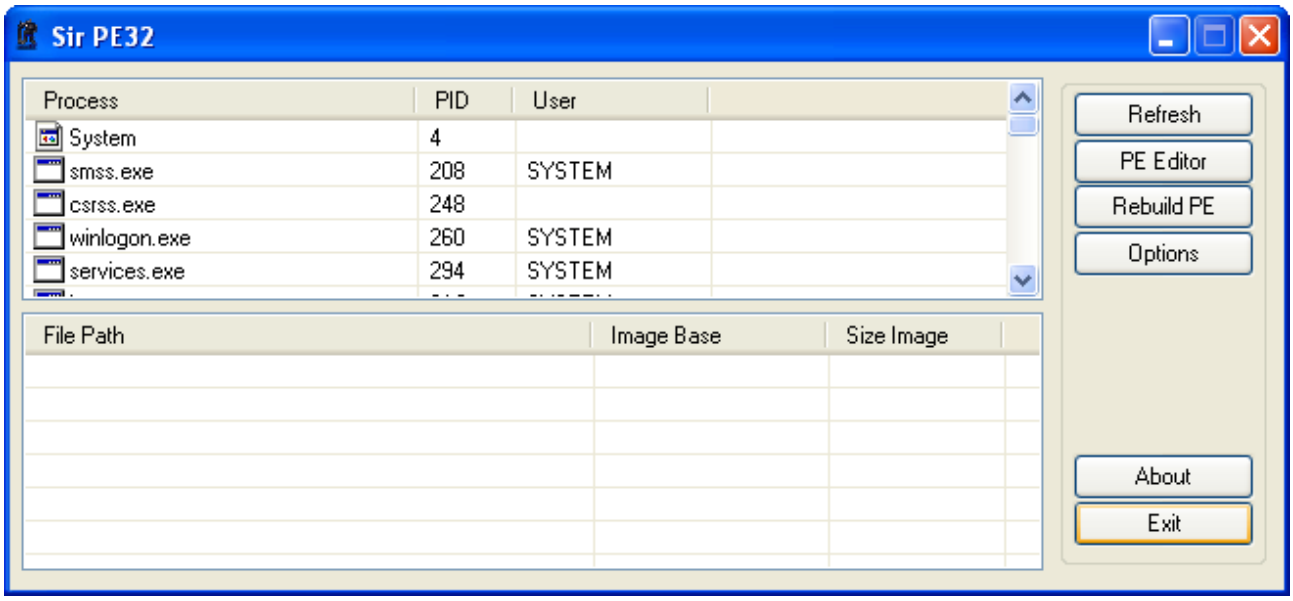
RVA OEP= DIRECCION OEP-ENTRYPOINT

OK ese es nuestro RVA OEP=007FBB94 si el que nos pedira el ImportRec...

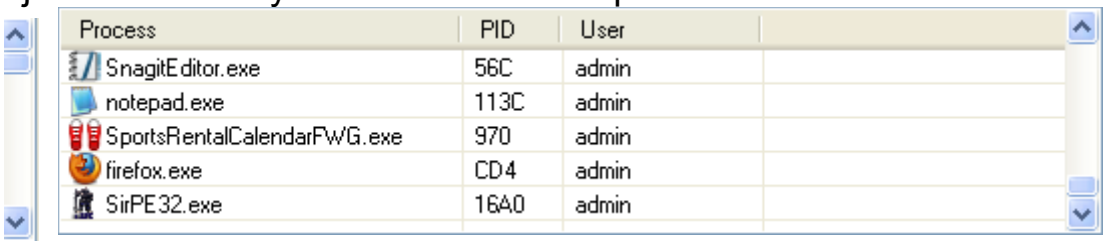
Ahora procedemos a hacer el dump para eso tiramos la casa por la ventana y nos prendemos con la tool que hizo guan de dio llamada SirPe esta por descarga directa:



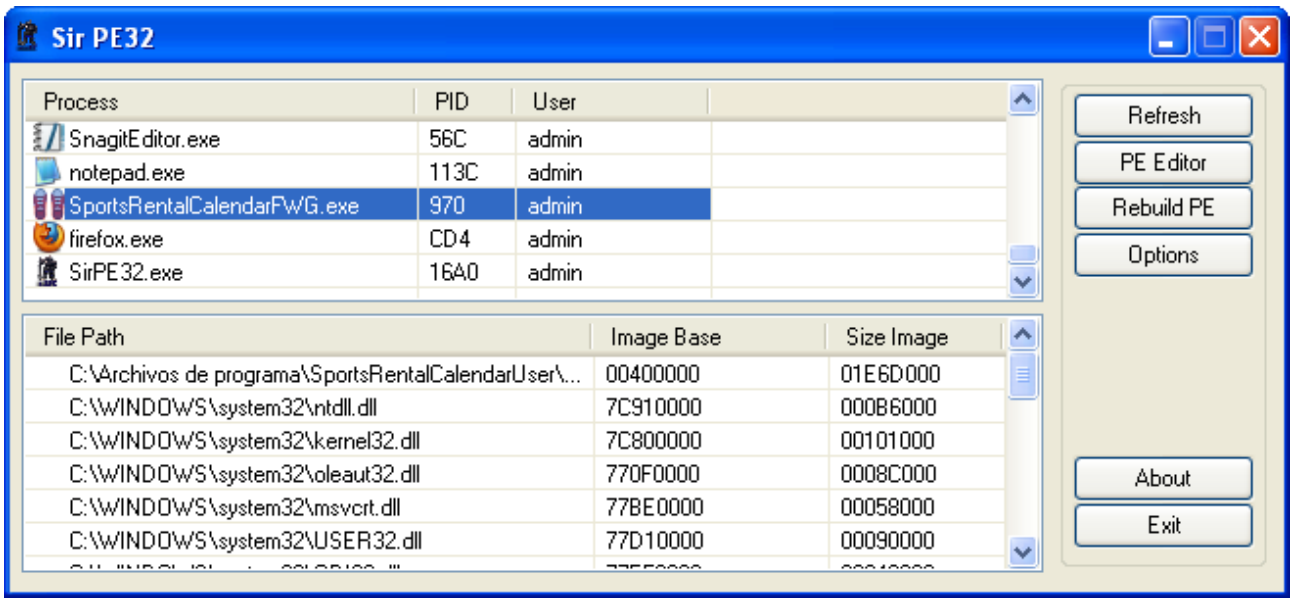
Ya que la bajamos procedemos a usarla asi que abrimos el ejecutable llamado SirPe.exe y vemos esto:



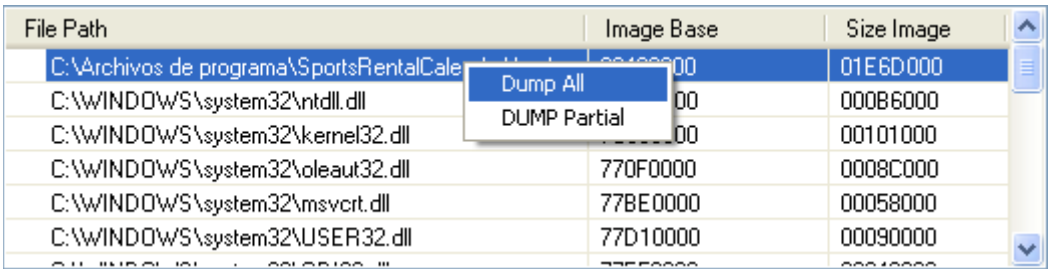
Bajamos la barra y buscamos nuestro proceso:



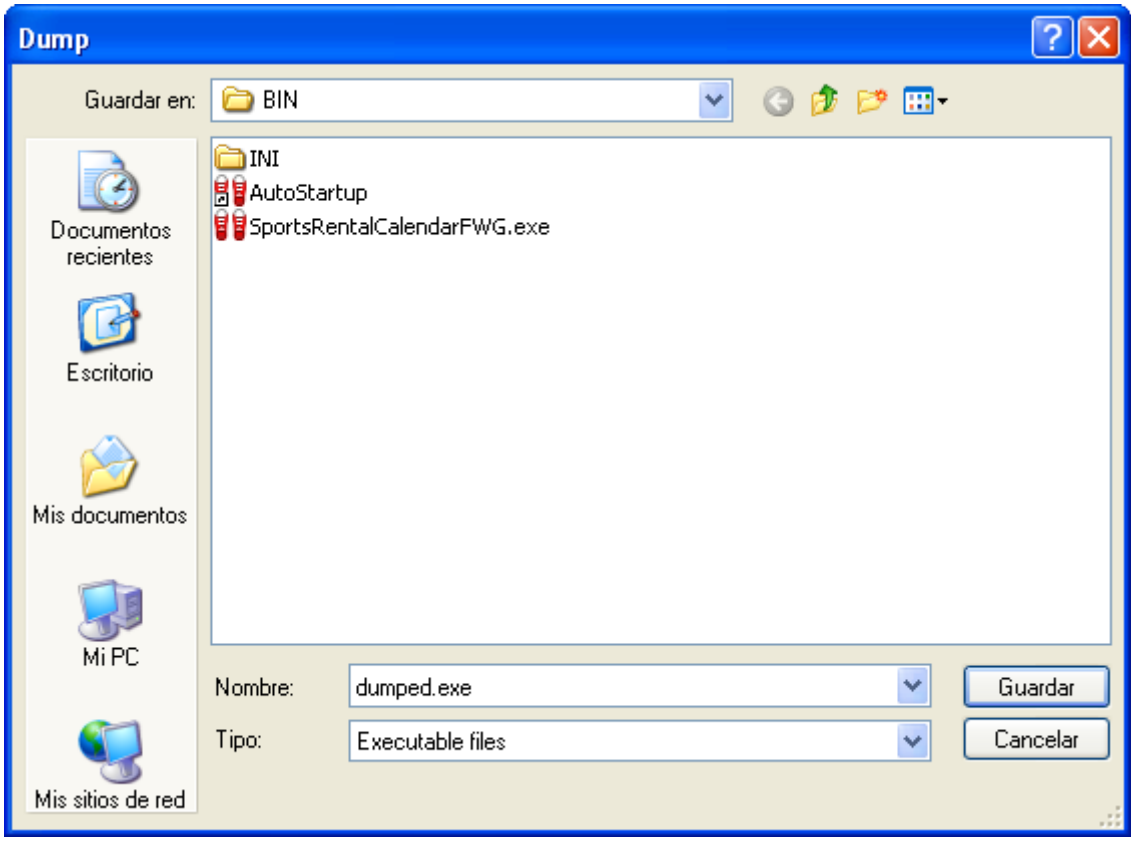
En nuestro caso es SportRentalCalendarFWG.exe damos un click seleccionándolo y veremos esto:



Seleccionamos la primera opcion que es nuestro .exe en donde dice filepath damos click derecho y le damos en dump All:

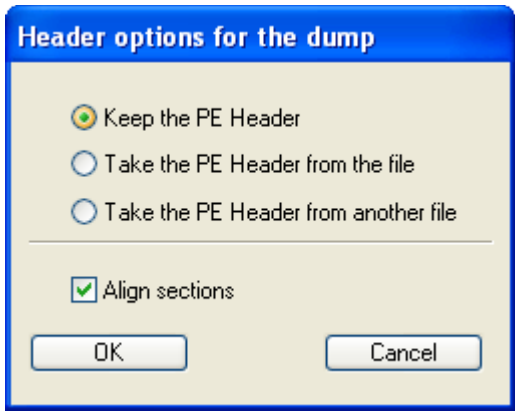


Luego nos sale una ventana pidiendo donde guardamos el dump le damos el nombre en nuestro caso dumped y la extension .exe y damos click en guardar:



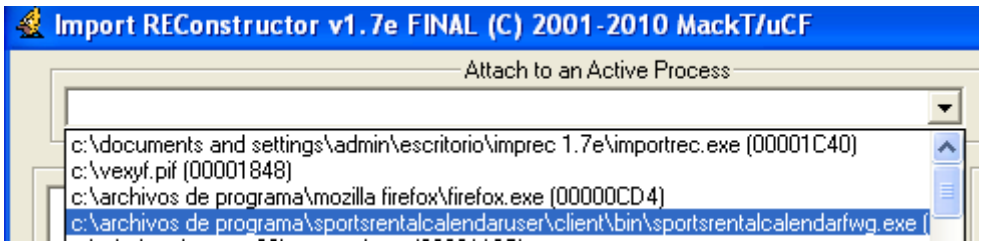
Ahora nos sale un dialogo que dice:

Luego otro dialoguito lo dejamos tal cual y damos en OK.

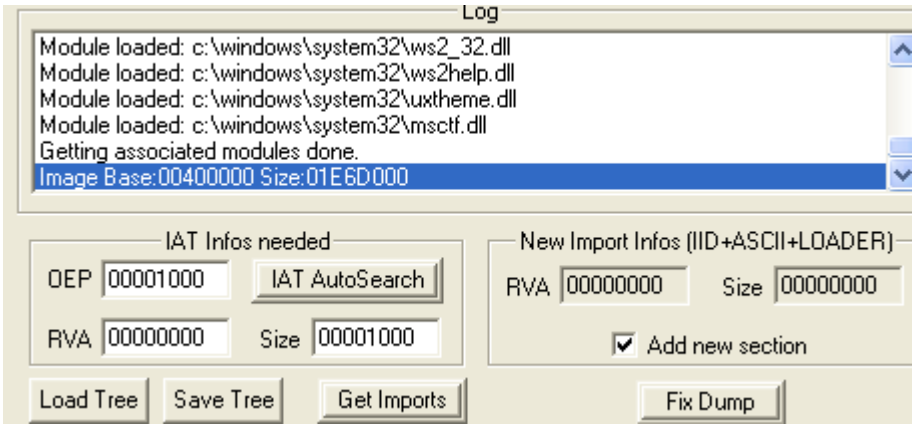


Y listo gracias despues de dar click en Ok agradecer a guan por la toolsita que nos deja dumpeado y alineadito el dumped.....

Teniendo nuestro olly parado en la direccion del OEP seguimos con Import Rec abrimos el import rec seleccionamos el proceso en este caso es este:

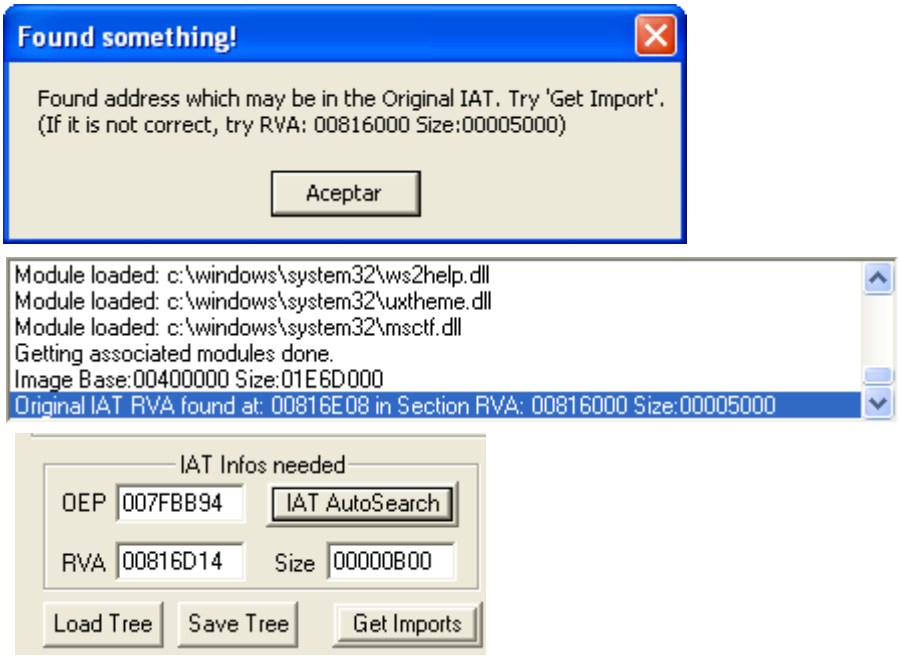


Luego veremos esto:

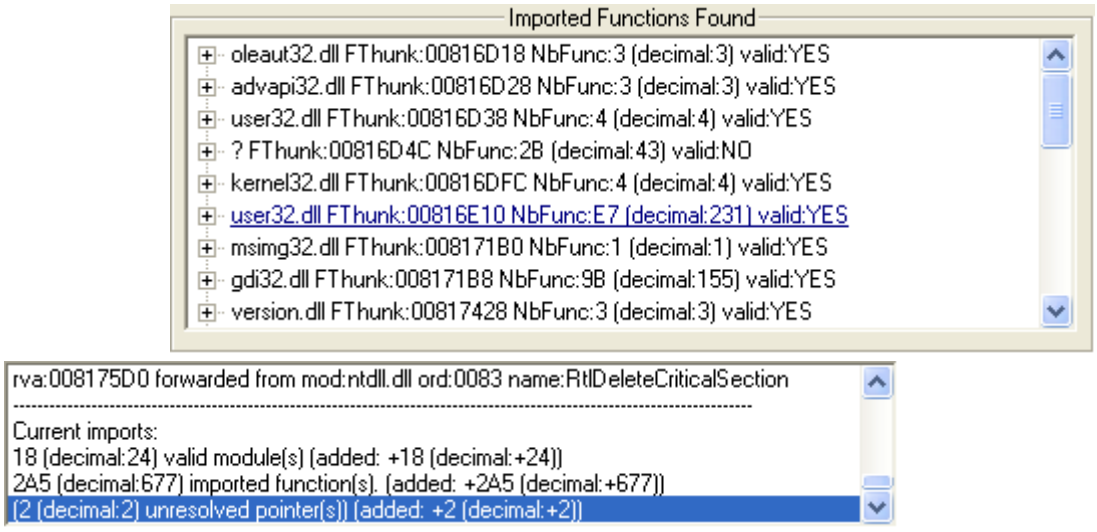


Ok lo primero que haremos sera poner donde dice OEP el valor que calculamos antes de hacer el dump recuerdan si el OEP=007FBB94 bueno ahora es hora de colocarlo donde dice OEP y damos click en donde dice IAT AUTOSEARCH.

Nos dara este resultado

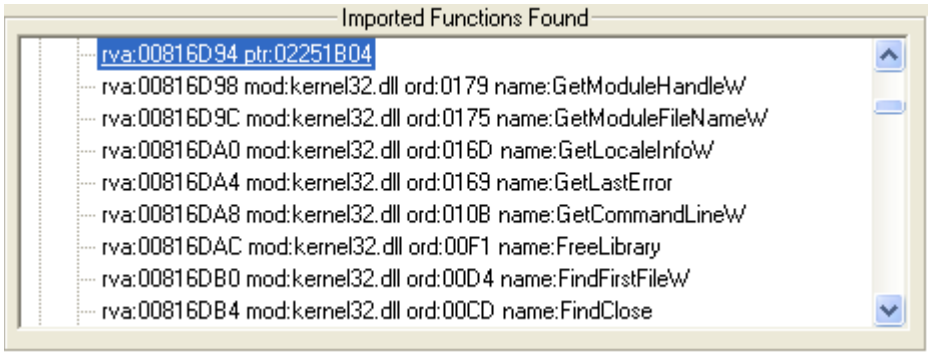


Viendo este panorama que no puede ser mejor pues le damos en Get Imports y miramos esto:

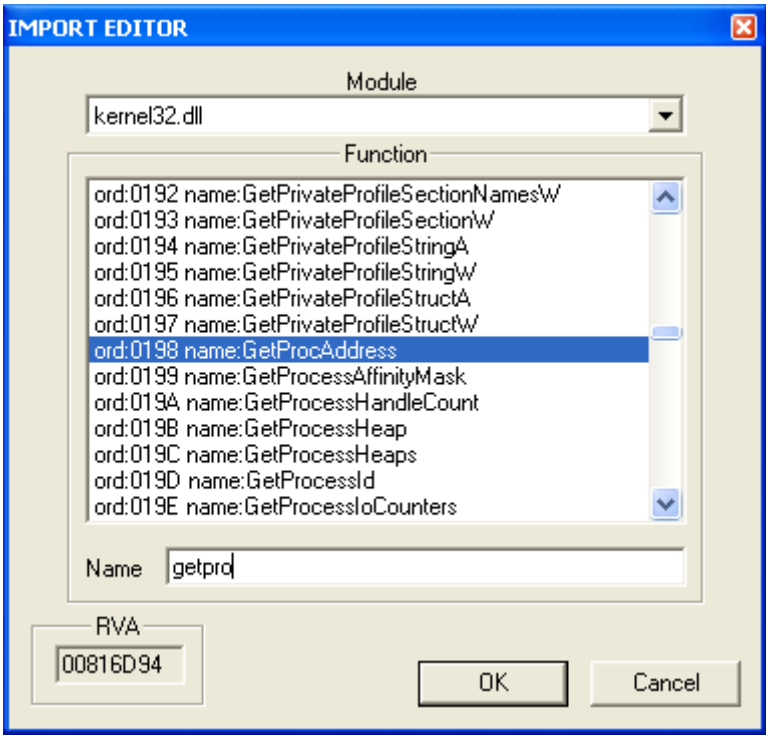


Joder lo que nos dice aca que dos imports no pudieron ser resueltas a muchos dirian dale click en cut thunks pero no , no sirve ese toque en este caso son validas.

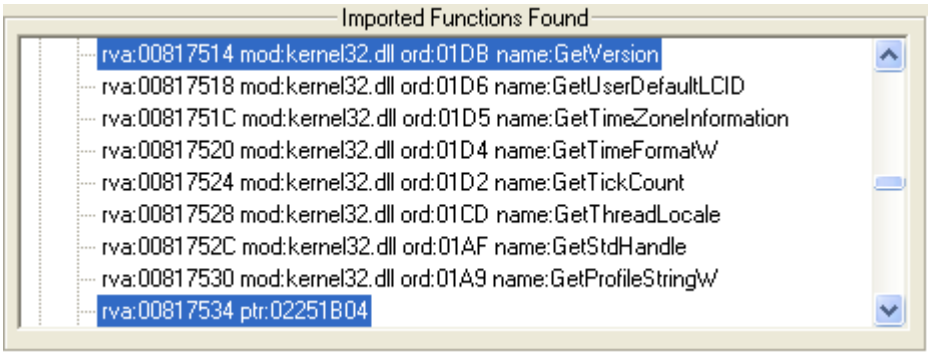
Ahora demos click en show invalid si es una opcion que apàrece al lado derecho del import rec, para que nos muestre el import rec cuales son las 2 imports malas y vemos esto:



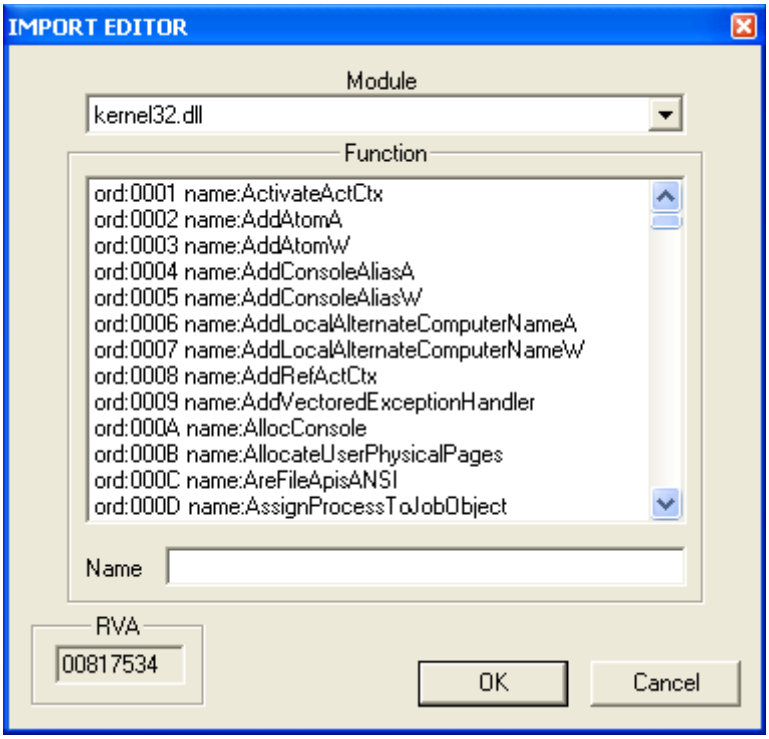
Ok señores aca les va un tip este packer se roba por lo general una api que es de kernel32 llamada getprocaddress asi que le damos doble click sobre la import mala y le vamos a poner getprocaddress le damos click en ok al finalizar:



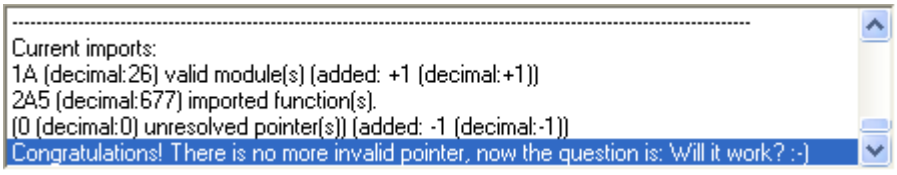
Luego volvemos a dar click en show invalid y nos muestra esta otra invalid la de abajo:



Igual el mismo procedimiento poner en name getprocaddres y dar click en Ok:

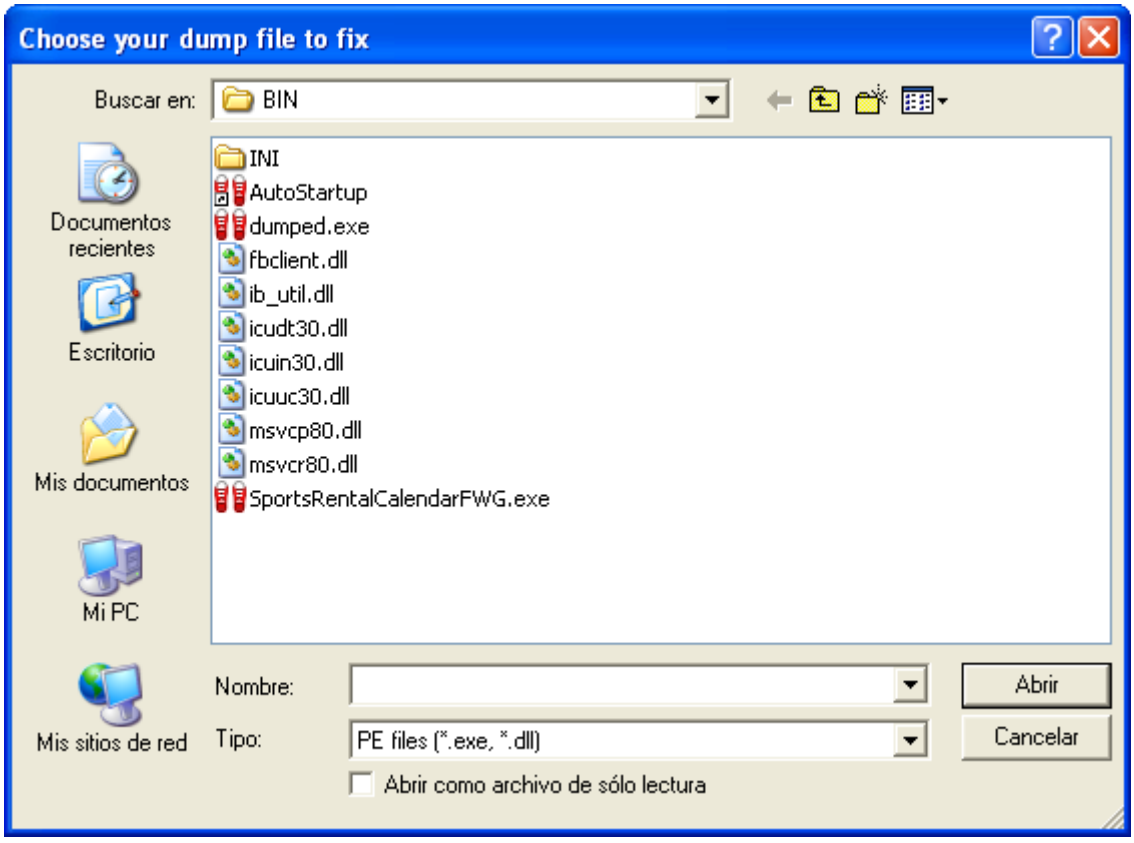


Luego nos aparecera esto:

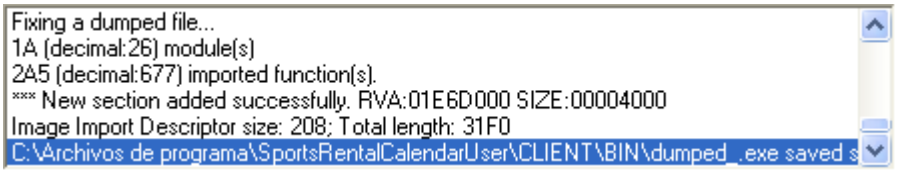


Y ahora si vamos a darle fix dump a nuestro dumped.exe que lo habiamos hecho con sirPE.

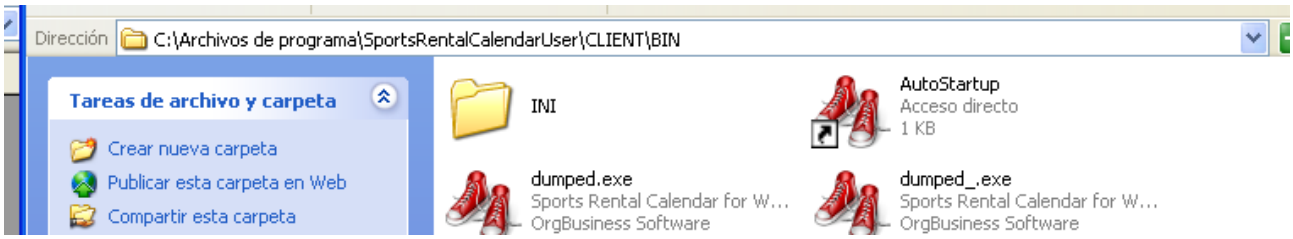
Nos sale esta ventanita y bueno seleccionamos nuestro dumped.exe y damos click en abrir y listo:



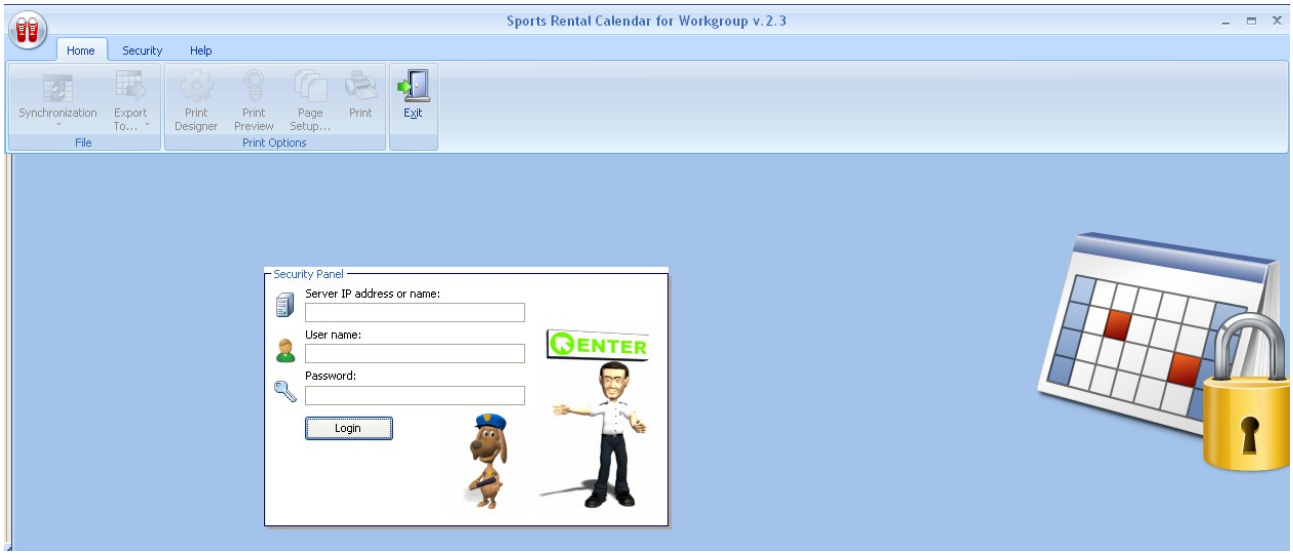
Ventanita y listo:



Vamos a donde esta instalado el proggie y vamos a abrir el dumped_.exe y a ver que tal:



Y bueno como dice The_Swash Joder Mola el cracking:



Ups se fueron las limitaciones de 14 dias bueno esto ha sido todo espero que alguien le sirva estas 19 paginas que escribi el que no le gusta pues joder, y al que le gusta pues que agradezca que esto de escribir no es nada facil...

Saludos especiales a Guan de Dio(Gracias por el SirPe), Torrescrack(Pinche Mexicano inside), a los que pidieron tute, Tena Crack siempre Prendido y bueno al maestro Ricnar que se le esta callendo el pelo de tanto andar moderando pero esta bueno el accionar.....Ojo no me moderes el tuto jajaja xd Son bromas...

+Erisoft(Erick Alfaro Esquivel)

Desde la Costa mas Rica Aguante Costa Rica.....