Nombre : Abacre Restaurant pos v 5.1

Link : http://www.abacre.com/download/arpos.zip

Funcion: Software para gestión de Restaurantes,Punto de venta Tactil

Fecha de salida : 12/7/2011

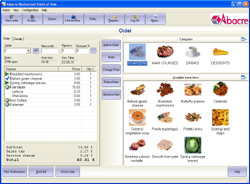
Cracker : EmO

Proteccion : SKD Untedectable

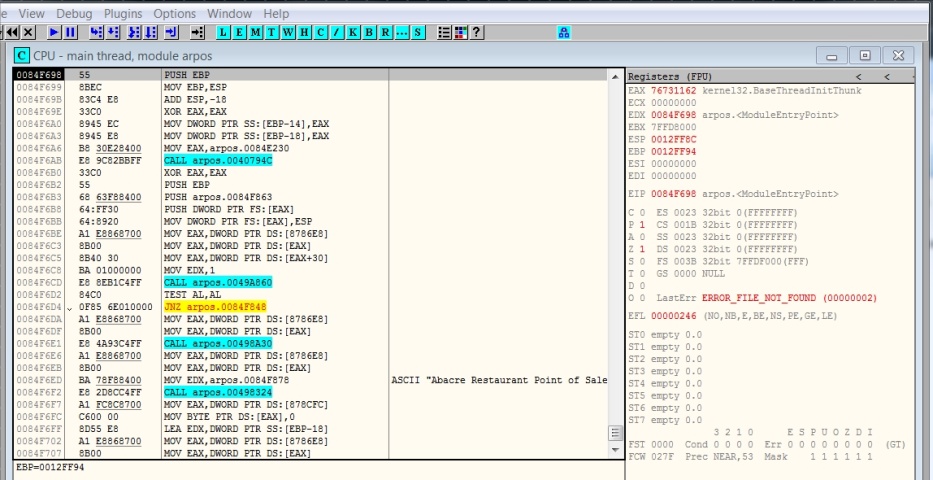
Instrumentos utilizados : RDG ,ollydbg

Limitaciones : El programa viene completo (versión Professional)por un periodo de prueba de 30 dias,para registrarlo se necesita un código de registro y una activación online u offline . Existen 4 versiones de licencia,lite,standard,ultralite y profesional,cada una de las cuales activa varias funciones suplementares .

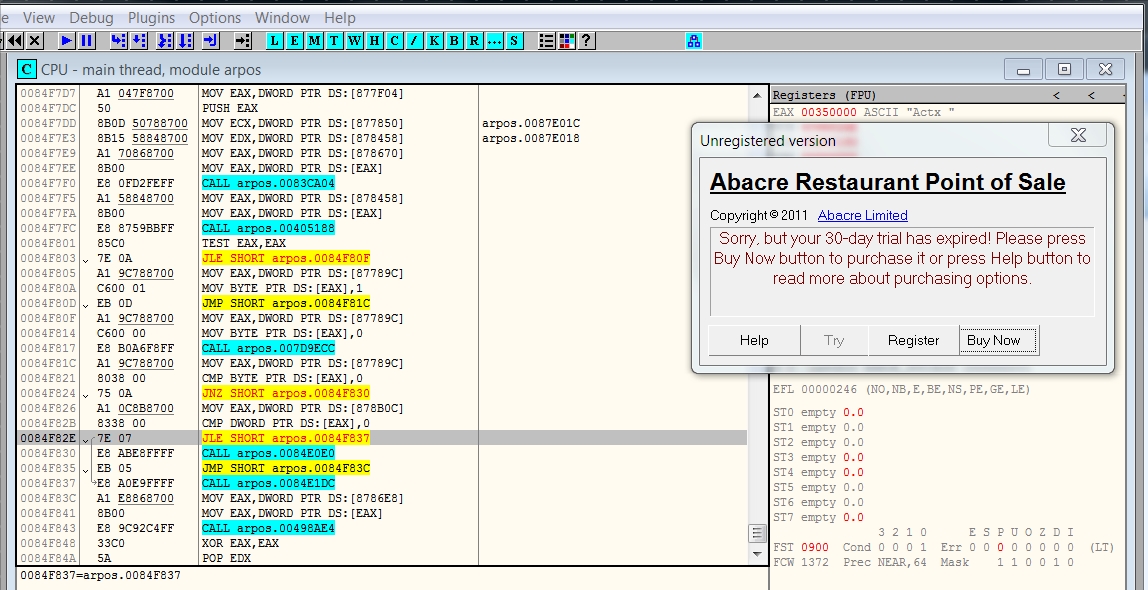
Metodo de ataque : Saltar comprobación de registro inicial y activación cazando inicialmente las nags ,utilizar las strings para registrarlo en versión profesional.



Empezamos analizando el exe con RDG y aparece encriptado con SKD Unteteclaber (beta).

Abrimos arpos.exe con olly.

Estamos en el EP del programa.

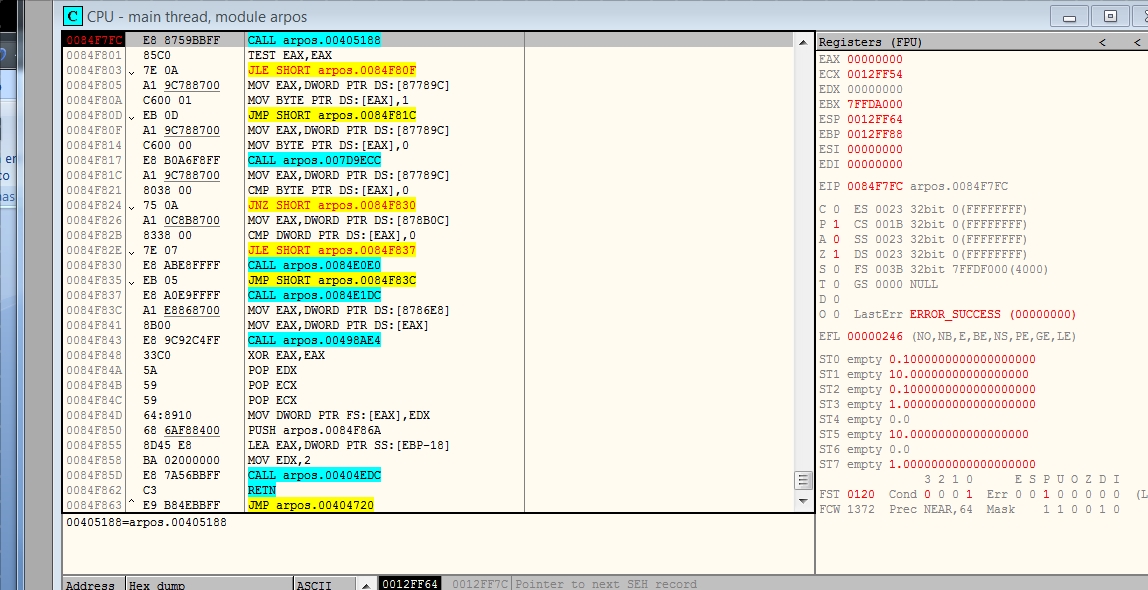
Ejecutamos con f8 hasta encontrar la primera nag. 

La nag empieza en 84f82e

En mi caso el periodo de 30 dias caduco y el programa no activa el botón TRY.

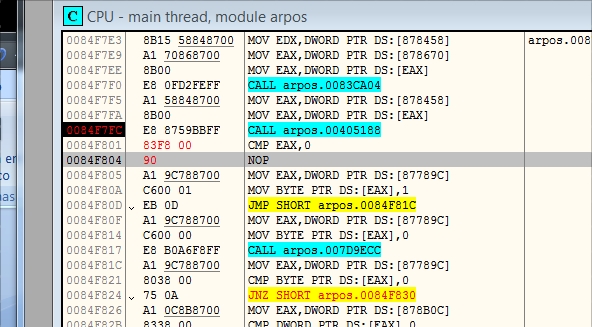
Si veo hacia arriba encuentro una call en 84f7fc ,la ultima antes de los saltos a la nag.

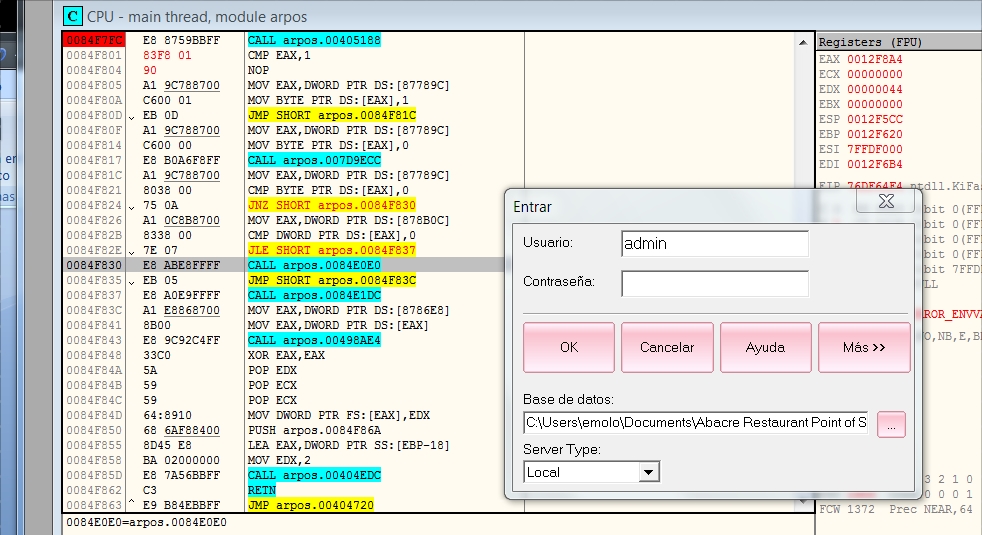
Reinicio y pongo un BP 84f7fc. Doy f9 y para en dicha call.



Veo que antes de la call eax==0 y si ejecuto con f8 tambien a la salida eax==0,seguramente la comprobación del registro vendrádesde calls anteriores,no me preocupo mucho porque me imagino que los saltos siguientes serán los que me mandan a la nag de registrado o no registrado.La instrucción que sigue es propiamente un TEST eax,eax y como vale 0 ,el salto en 84f803 se realiza.

Modifico en 84f801 el TEST eax,eax con CMP EAX,1 para q no salte



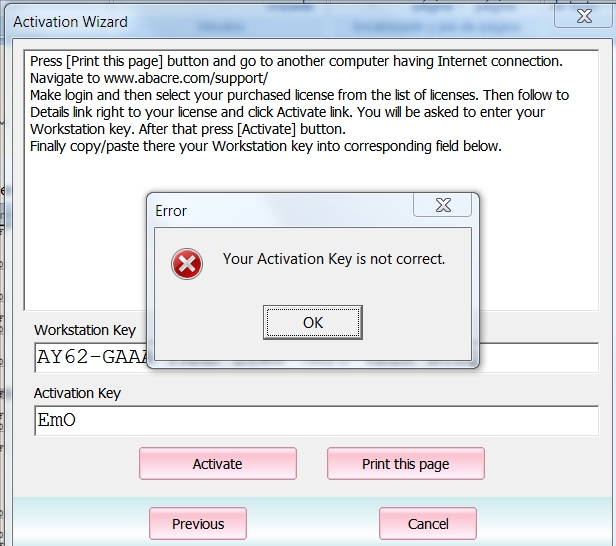
Doy f8 y el programa en 84f830 me abre una nag de login 

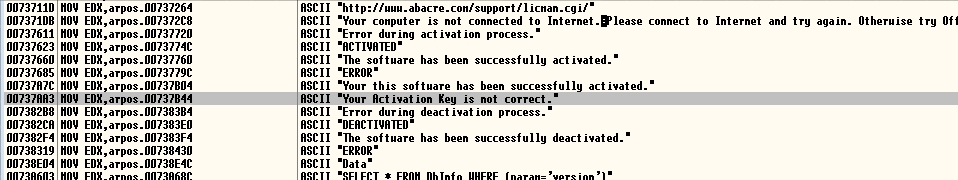
La contrasena es 111111 por default como nos recuerda el programa si nos equivocamos …

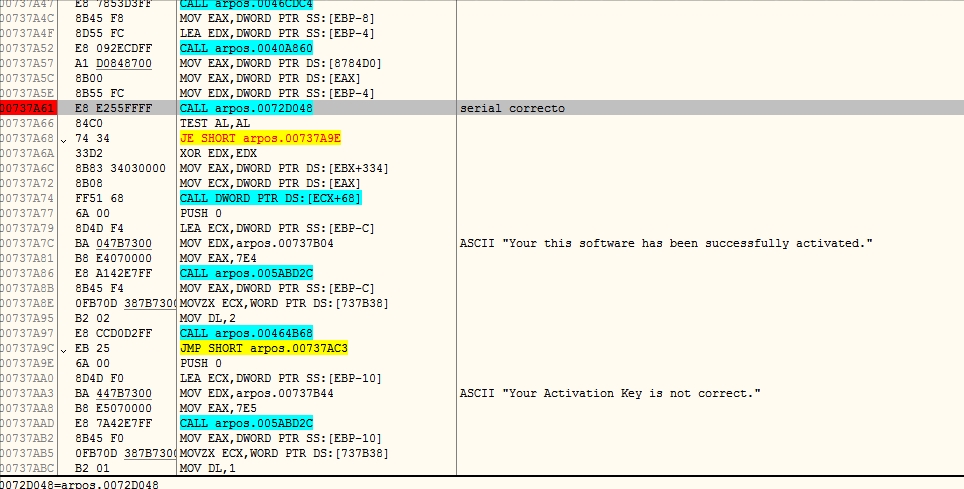
Entonces doy f9 y meto la contrasena.

Ahora me abre una nag de activacion ,le damos a Make Activation y podemos ver que puede ser online u offline,seleccionas offline y seguimos viendo q pasa.

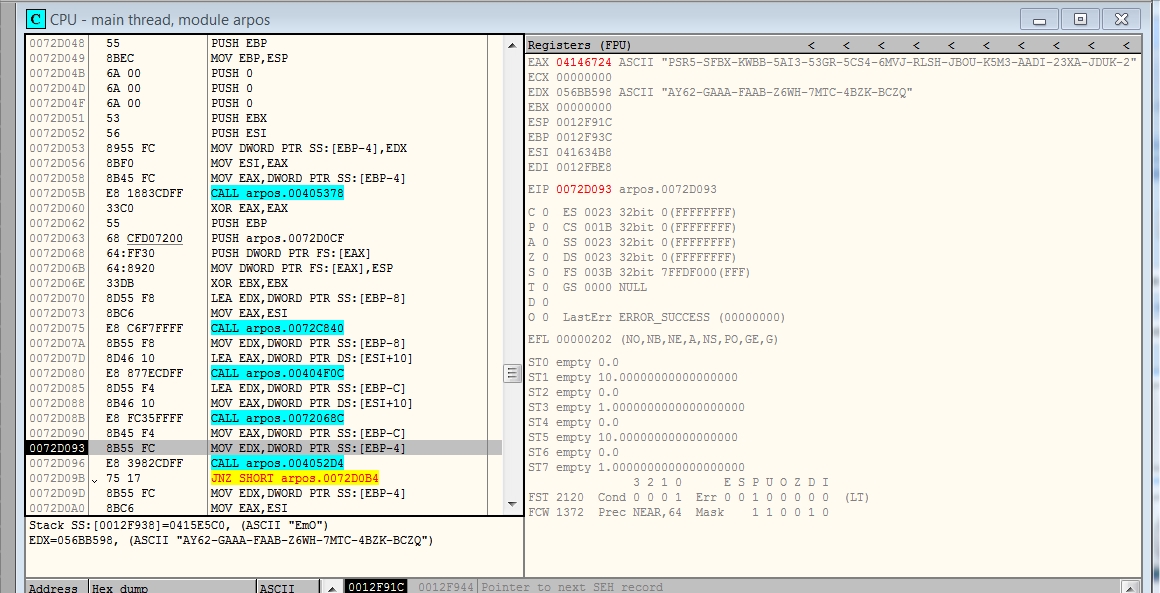
Meto un nombre y doy a Activate,me tira Error …



Aqui la idea seria saltarse también esta nag y llegar directamente al programa,podríamos buscar en las string la frase Your Activation …. Y la encontramos 

Si le damos 2click llegamos en esta seccion

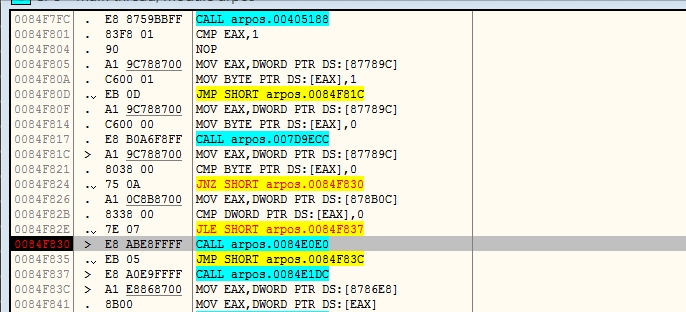
Y en esta call,si reiniciamos y pones un BP,entrando con f7 y traceando con f8 ,podremos ver el código de activación correcto para nuestra maquina



Pero mi idea es saltar todas estas comprobaciones y que el programa quede registrado sin pasar por estas complicaciones,además el programa cuenta también con deactivacion por cambio de hardware y seria complicado llegar aquí cada vez que lo reinstalamos en una maquina diferente.

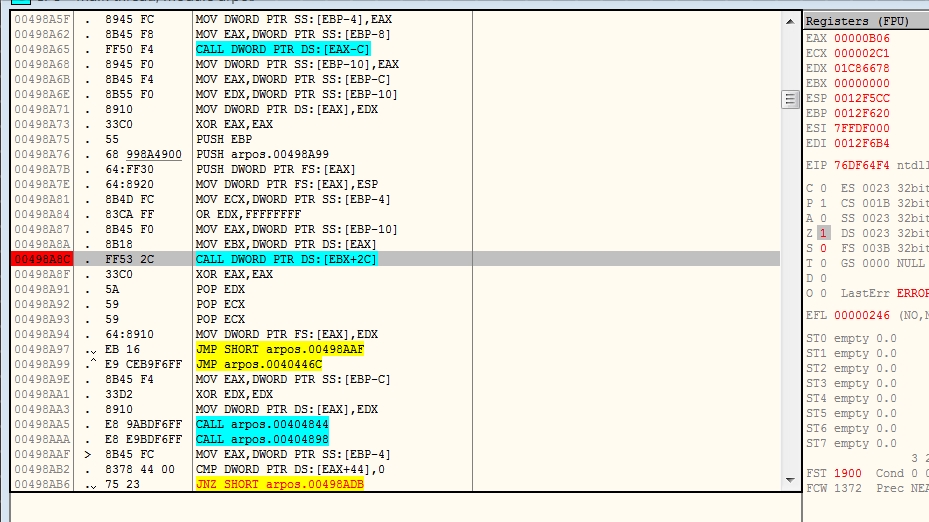
Entonces reiniciamos …

Cargamos otra vez el exe ,modificamos la instrucción test eax,eax por cmp eax,1 en 84f801 y paramos en la nag de login en 84f830



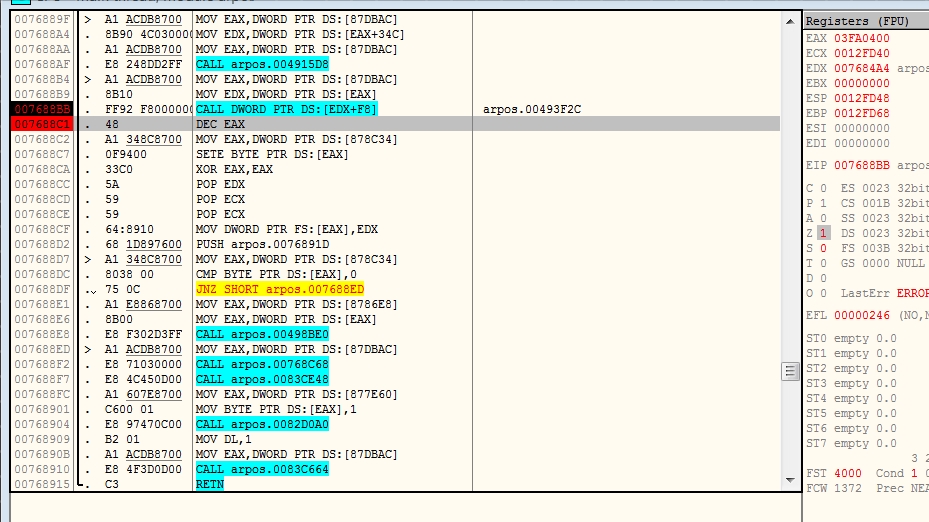
Ahora traceamos en la call con f7 y vemos q en 84e10b abre la nag login (nidificado),reiniciamos y metemos bp aquí.

El olly para y si entramos con f7 y traceamos con f8 podemos encontrar donde abre la nag login (mas nidificado)



Metemos bp y reiniciamos…Seguimos traceando adentro de esta ultima call con f7 y otra vez la nag de login aquí en 7688bb,esta vez ponemos un bp aquí y uno a la salida de la call,suponiendo sea la ultima y que el exe salga a la próxima instrucción después del login

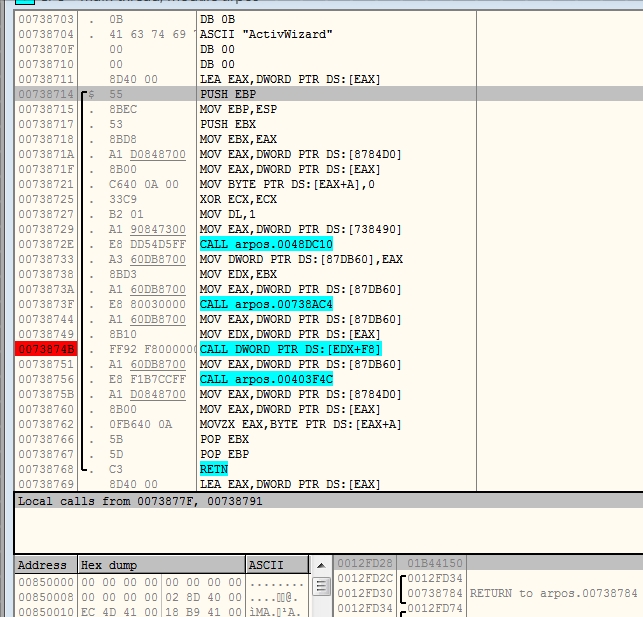
Reiniciamos y para en dicha call



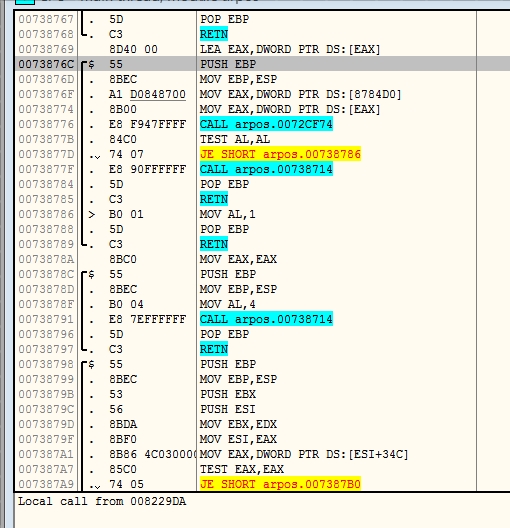
Damos f9 y para aquí,otra vez f9 y abre la nag login,introducimos la contraseña y damos a ok,el programa para en la siguiente instrucción en 7688c1,ahora nos toca tracear con f8 hasta la nag de la activación….

Aquí abre la nag activación 

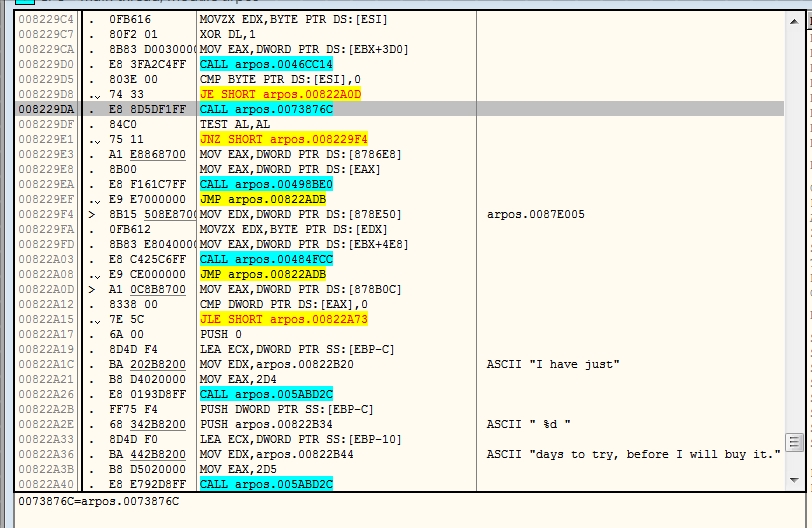
Y si vemos donde empieza la rutina el olly nos dice desde donde a sido llamada….



Buscamos en 73877f y seguimos traceando para atrás



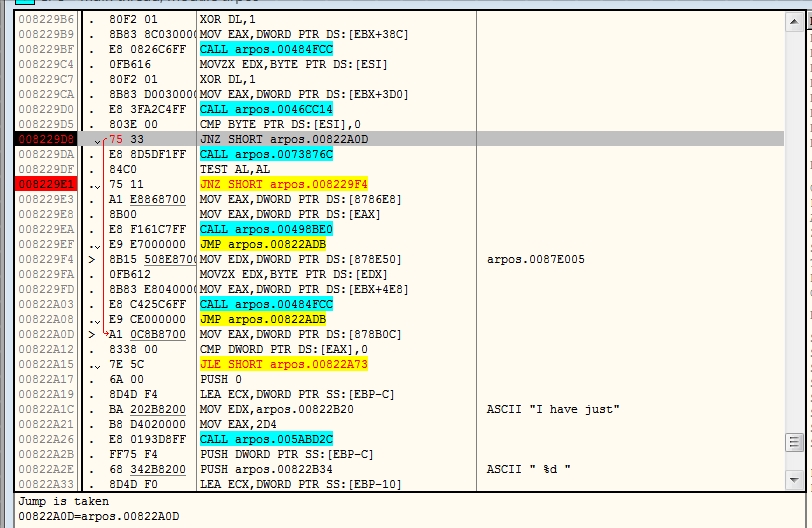
Local call from 8229da



Esta sección esta muy interesante,podemos ver varios saltos que nos mandan a la limitación de tiempo y justo arriba de esta ultima call un salto JE en 8229d8,será el salto de la activación…

Metemos un bp aquí en el salto y reiniciamos…

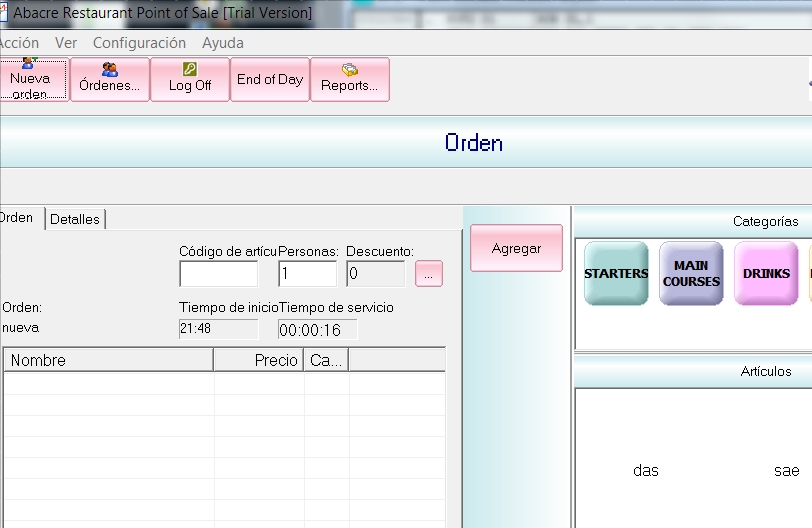
Para en el salto y seguiría a la call de la activación ,invertimos el salto para ver que pasaría



Seguramente en la call anteriores al salto viene la comprobación de la activación…

Bueno,el programa salta una vez y también en 822a15 salta ,el programa abre ¡!!

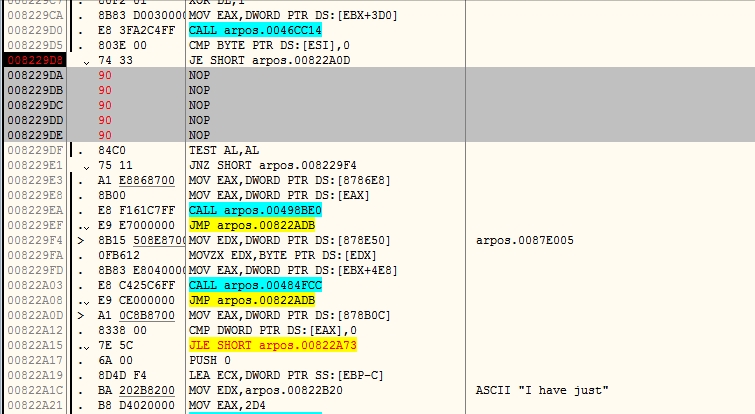
Pero arriba leo un trial versión muy molesto….



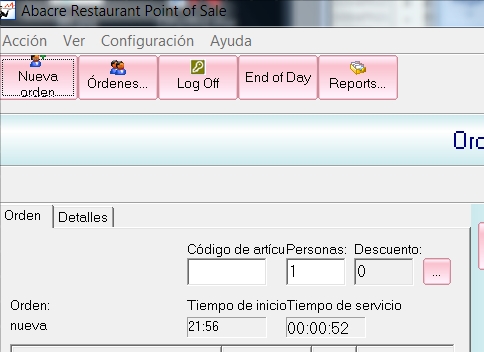
Reiniciamos con un bp en 8229d8 y para .

Para saltarnos esta molestia deberíamos caer el el jump en 8229ef o en 822ª08…

Entonces en lugar de cambiar el salto,noppamos la call de la activación….



Salta a jump en 822ª08 y evita la TRIAL VERSION,arranca el exe sin problemas…



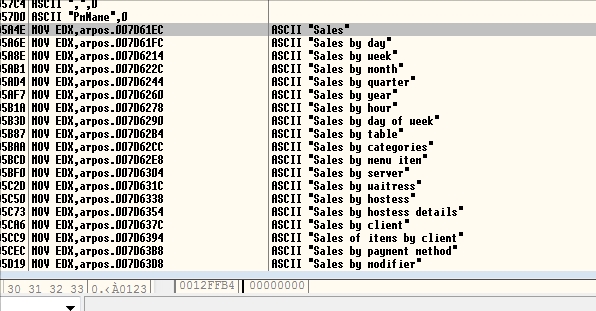
Hasta aquí todo bien parece…

Si nos fijamos en el programa y vamos a ayuda ,sobre,aparece registrado a lblregiter y License type sin ningún valor,esto significa que deberemos obligarlo a registrarse versión profesional para tener todas las funciones del programa activadas.

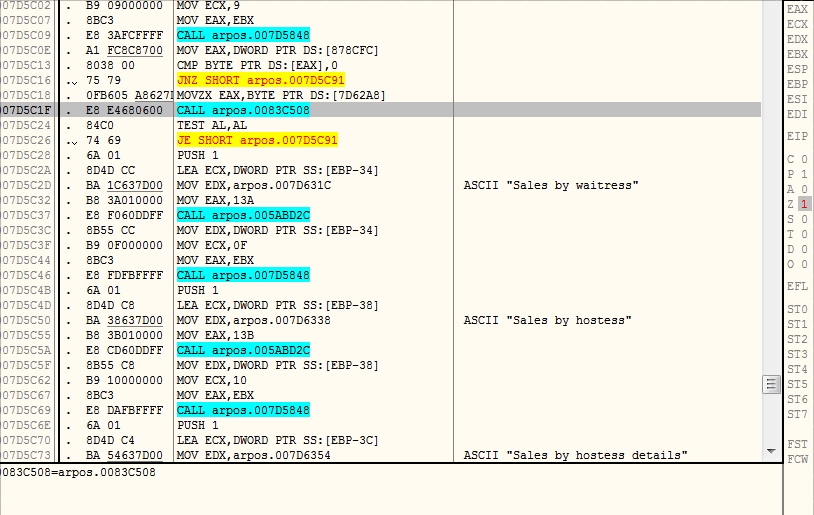
Si se han fijado bien,cuando se prueba el programa en versión trial,aparecen mas botones y opciones,la versión demo esta profesional,mientras que esta esta Lite.

Por ejemplo en la sección REPORTS,muchas opciones no están activadas,como el report Sales by Waitress o el margin profit….

Existen varias maneras de atacar este problema,yo voy a buscar en las string las Sales by y encuentro esto

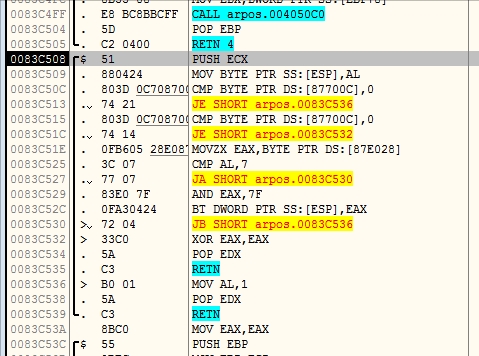


Le doy a cualquiera y llego aquí…

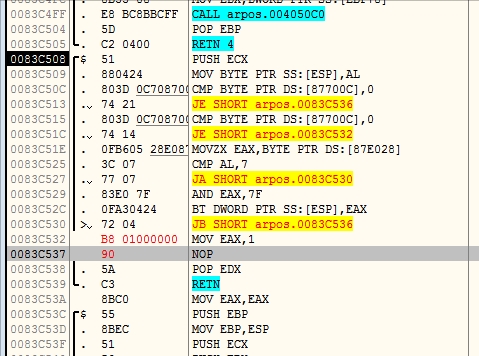


En esta Seccion ahí que tener un poco de buen ojo,notar que para algunas categorías de sales,existe un salto antes de la rutina ,como por ejemplo aquí en 7d5c26 y una CALL que se repite en varias secciones de Sales ,la CALL arpos.00835c08.

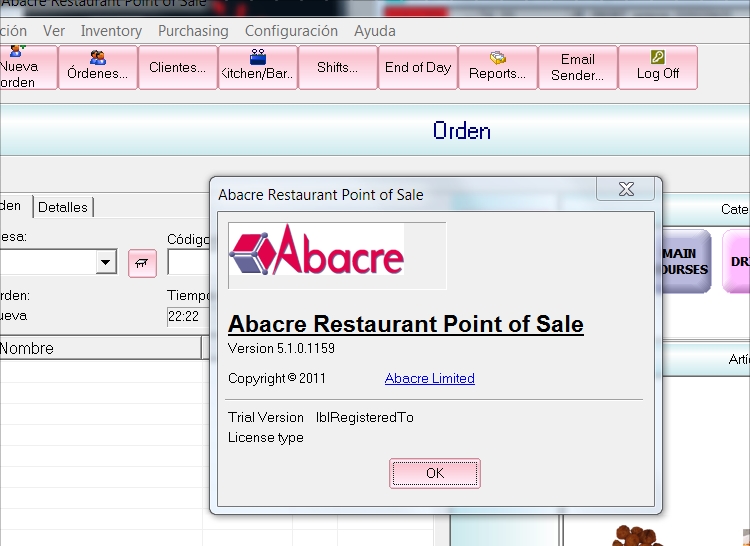
Me imagino sea una rutina de comprobación del tipo de licencia,lite,profesional etc etc

Si analizamos,estos saltos son decisivos para que algunas opciones del programa estén disponibles. A la salida de la call EAX==0 Entro a la call con Enter (follow) y veo que en ultima istancia xorea eax

Voy a cambiar esta instrucción para que salga siempre EAX==1

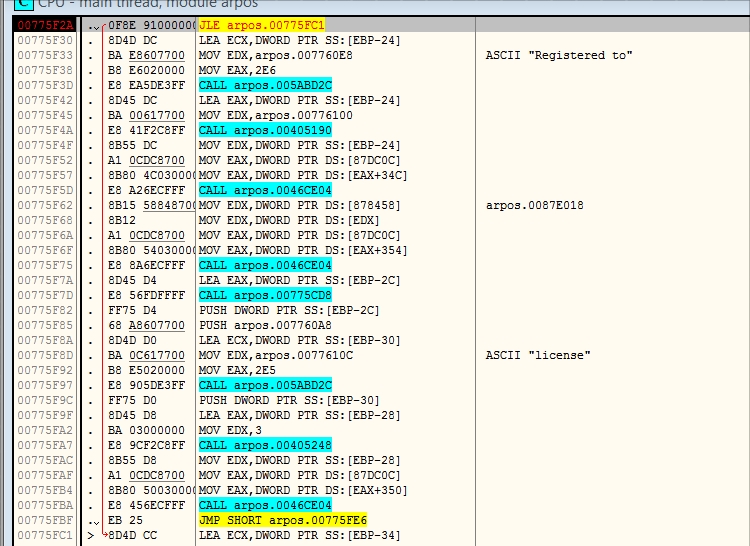


Doy f9 y ya con todas las modificacione echas el programa arranca…



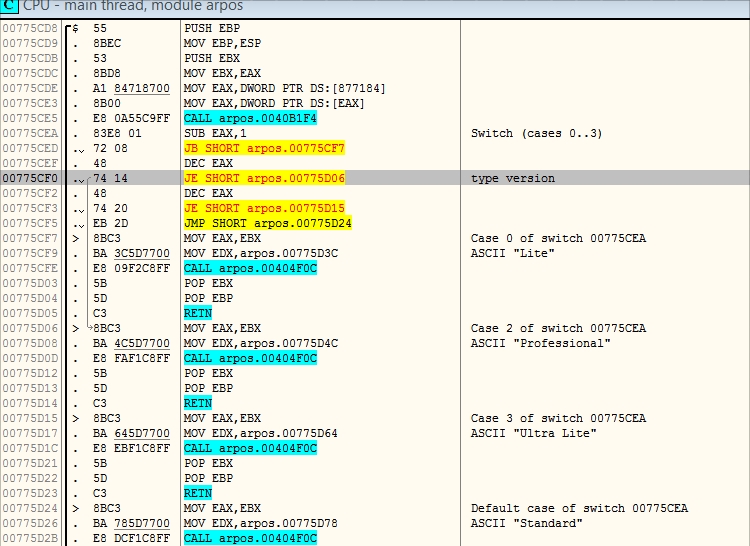
Todas las funciones están activadas,si queremos faltaría ,en Sobre,anadir profesional a license type,aunque no haga falta,pero como es teoría,lo haremos…

Buscamos “license” en strings y caemos aquí,claramente un salto nos impide llegar a “versión”



Invertimos este salto ,abrimos ayuda,metemo en pausa f12 y le damos a Sobre ,para justo aquí.

Traceamos con f8 hasta la Call antes del texto “license” y aquí traceamos con f7,caemos en esta zona



Obligamos en 775cf0 a saltar a “profesional” invirtiendo el salto ….

Ya queda license Type “profesional”

Esto es todo,agradezco a Narvaja y Indulgeo,todos los de crackslatinos

EmO\_11