Programa	Privacy Dummy! 1.1		
Protección	------		
Descripción	Un programa		
Dificultad	baja		
DownLoad	http://www.dummysoftware.com/		
Herramienta	Olly		
Cracker	La Calavera	**Fecha**	

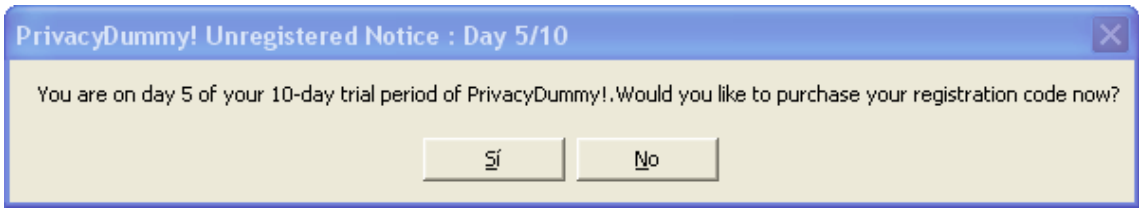
INTRODUCCION

Bueno aquí aburrido jejeje me puse a ver varios programas para exploit pero como no encontré algún bug pues me decidí a crackear este programa en un principio no iba a hacer tute ya que parecía muy sencillo pero me salio con un CRC y bueno aquí esta.

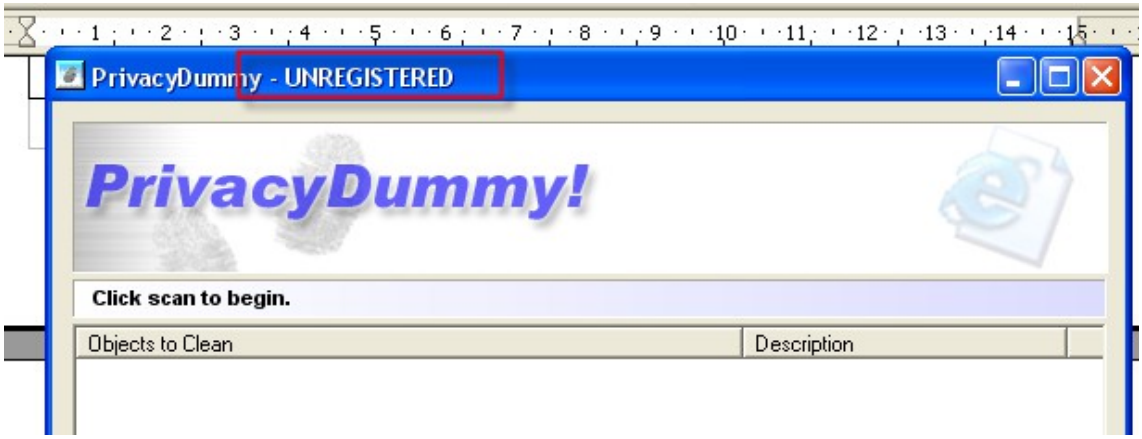
AL ATAKE

Bueno comenzando.

Como ya hace días lo tengo instalado me sale este cartelito

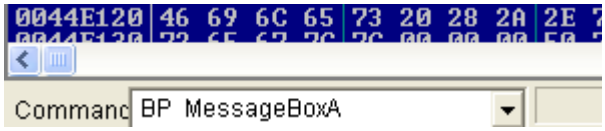


Como verán 5 de 10 días de uso o algo así mi ingles es muy malo :-P le doy a no y arranca el programa

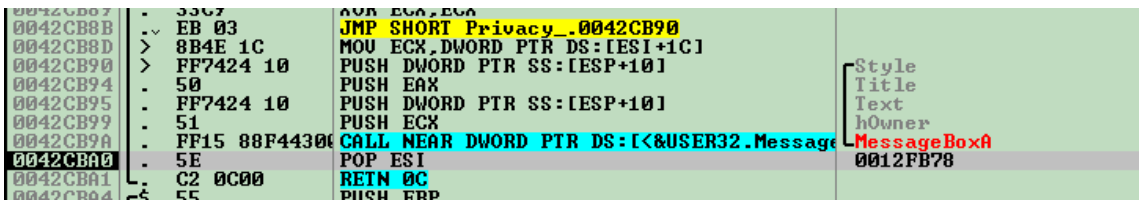


como ven nos pone un lindo UNREGISTERED pero si busco entre las string no hay nada (las string están bastante bien ocultas las mayoría claro) así que como no me quise romper la cabeza me decidí a atacar por el mensaje inicial ya que un MessageBoxA y así buscar un indicio de por donde saltarnos la registracion

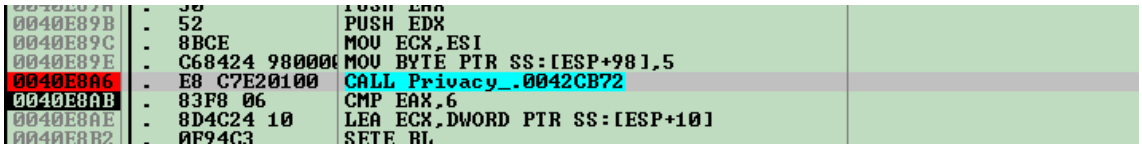
bueno lo cargamos en el Olly y ponemos un BP en MessageBoxA



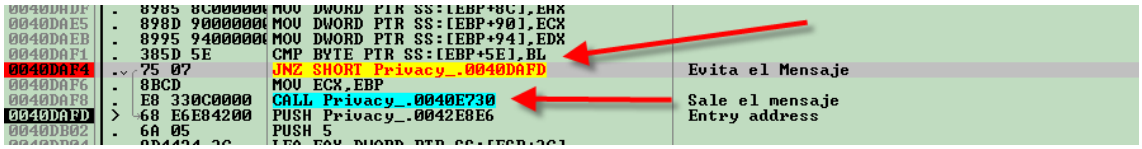
Y le damos a F9 y cuando para aceptamos el mensaje y comenzamos a tracear hasta llegar al programa en si



como ven ahí tenemos la llama a la API así que seguimos traceando para ver desde donde es llamada

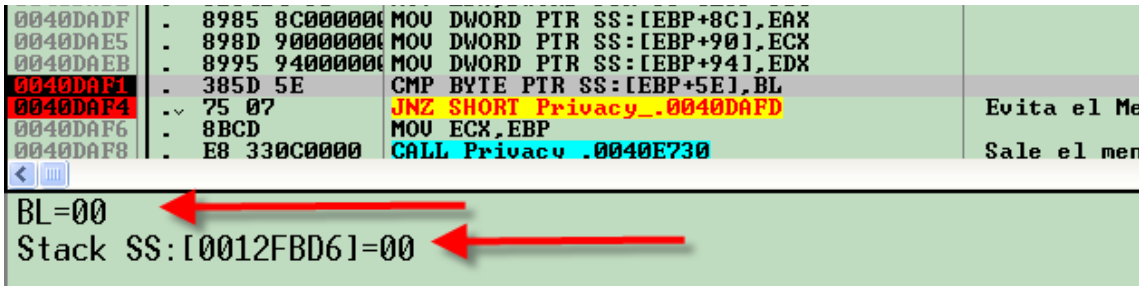


Ese es el CALL que llama al mensaje y si subimos vemos que estamos dentro de otro call así que traceamos hasta el final y vemos

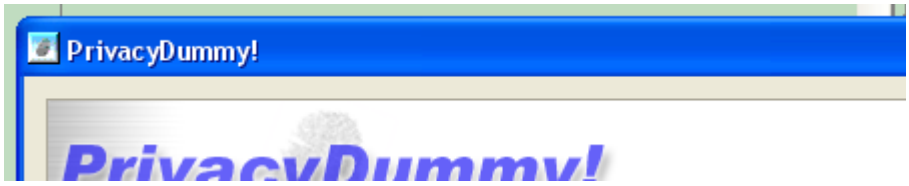


Bueno como ven justo por encima tenemos el salto que evita el mensaje así que ponemos un BP en el mensaje y reiniciamos y cuando para cambiamos el FLAG y arranca el programa sin el mensaje inicial o sea que ya evitamos que caduque pero ….

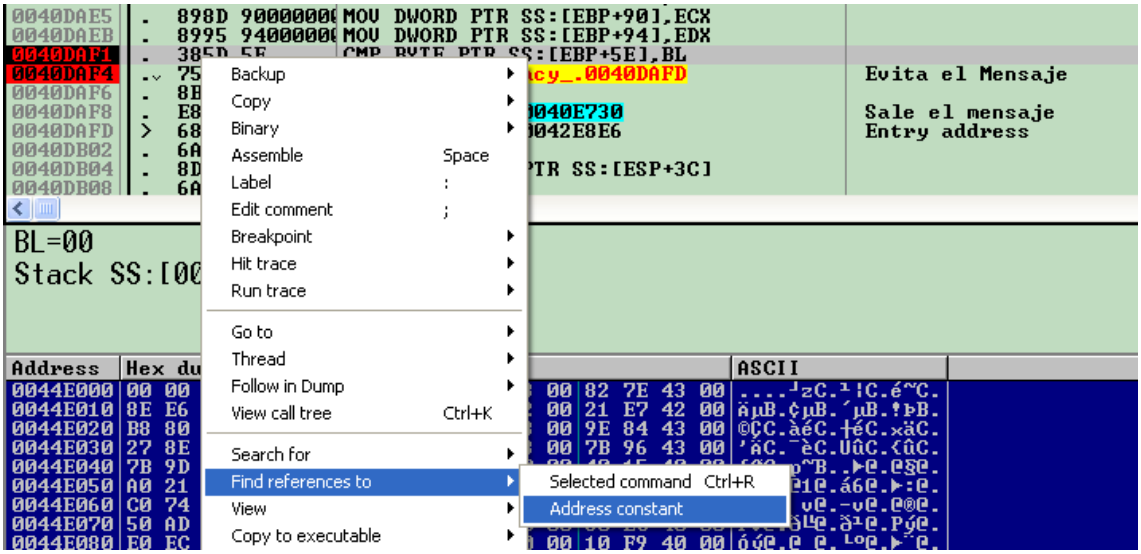
Como ven sigue diciendo UNREGISTERED y eso es feo jejeje ahora bien como se ve por encima del salto hay una direccion que se compara con BL así que ponemos un BP en la comparación y reiniciamos nuevamente

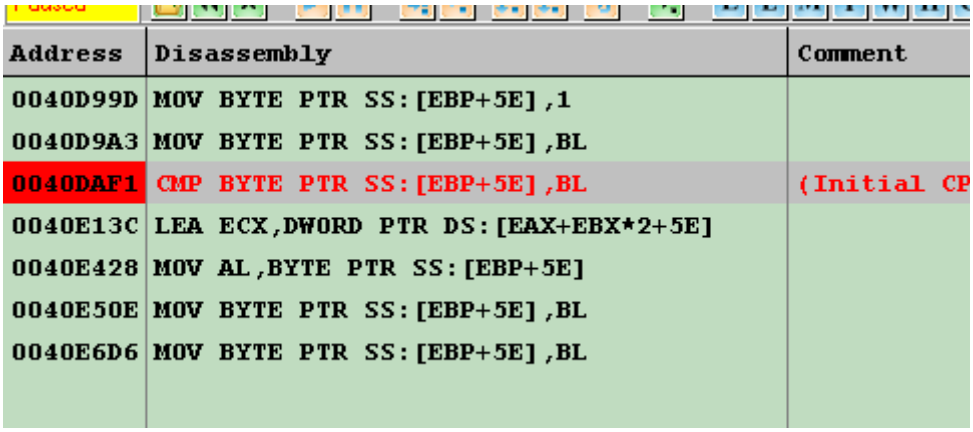


Como ven ambas valen 0 así que cambiamos el 0 de 12fbd6 (ojo esa direccion es en mi caso ya que es un valor de la pila) lo cambio a 1 y le doy a F9

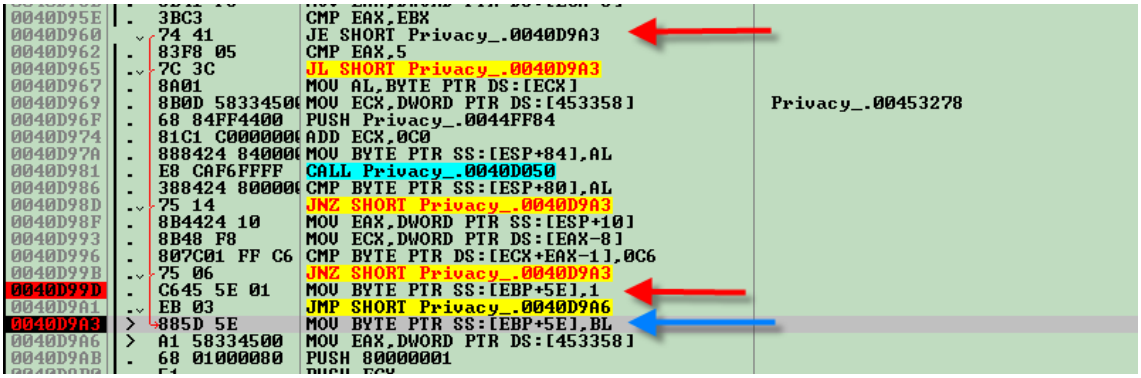


Como ven arranca el programa y registrado bien ahora hay que buscar meter un 1 en esa direccion y para ello vamos a buscarlo





ese es el listado esta vez son pocos así que le vamos a poner un BP en cada uno a ver en cual para reiniciamos



Como vemos en la imagen para en 40D9A3 y justo por encima tenemos el mov 1 a esa direccion y un poco mas arriba tenemos un salto al BP que estamos así que cambiamos

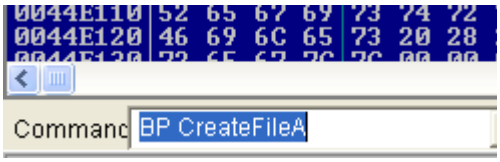
ese salto por un JMP 40D99D y siempre esa direccion valdrá 1 con lo cual estaremos registrados.

Bueno guardamos los cambios con algún otro nombre y vamos a ver como nuestro programa quedo crackeado lo cargo desde fuera del Olly y.... el programa no arranca ???? bueno como dije antes el muy condenado tiene un CRC (o sea que comprueba que todos sus byte estén correcto sin modificación).

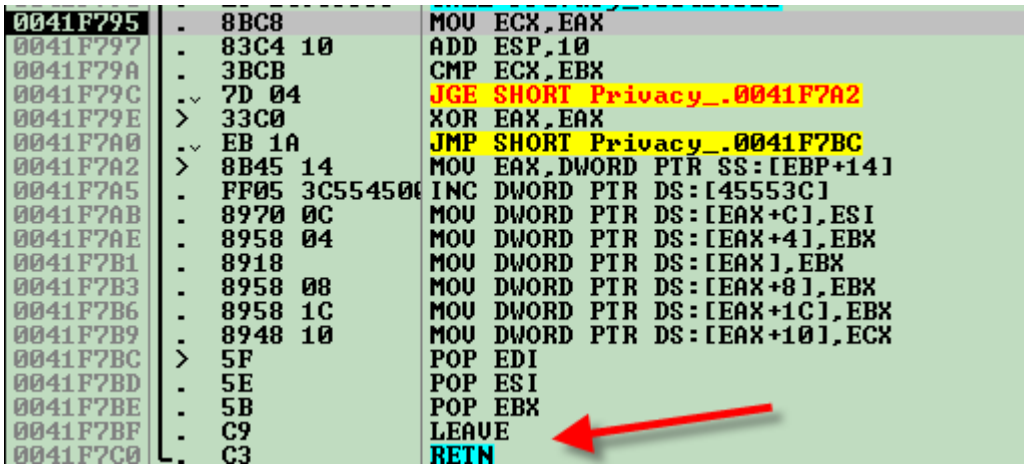
Bueno cargamos el programa modificado dentro del Olly y lo primero que intente fue ver si lee en la memoria los byte que hay en la sección de registro (antes funcionaba jejejeje) y nada se cierra sin leer un solo byte hmmmmm

Bueno como ya dije antes estuve mirándolo para ver si encontraba algún bug para exploit y lo primero que mire fue ver que archivos cargaba y el primero que carga es el ejecutable, entonce veamos que hace.

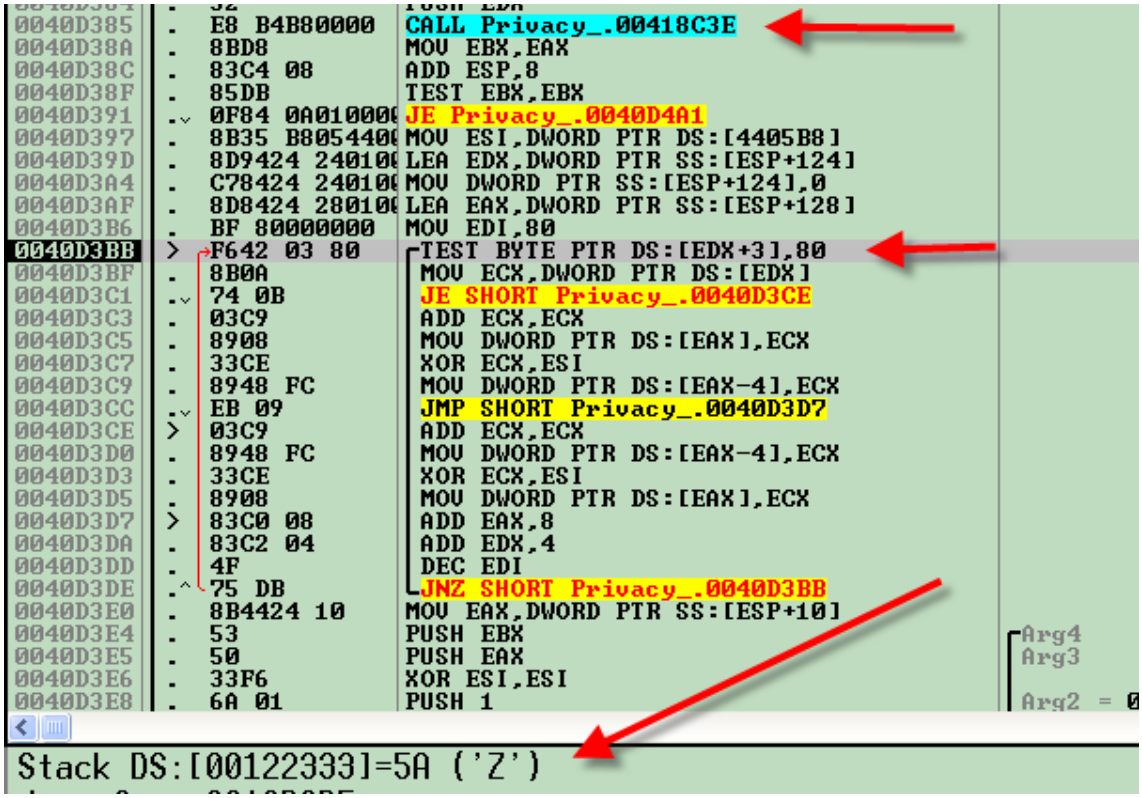
Cargamos el modificado y ponemos un BP en CreateFileA



y le damos a F9, una vez que para traceamos para salir de la API hasta el programa y continuamos traceando hasta salir del CALL

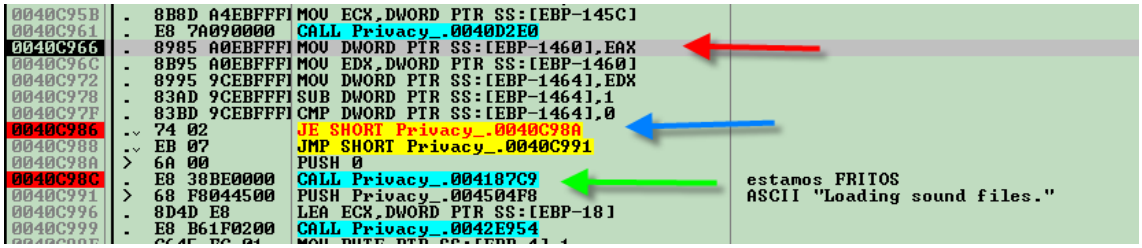


Como vemos no hay nada así que seguimos hasta el retn y así vamos saliendo de los distintos CALL hasta llegar a esta parte

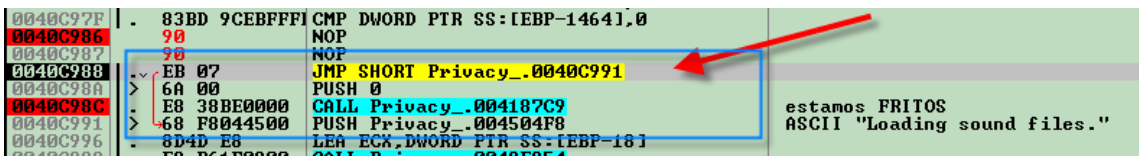


Bueno cuando salimos del CALL vemos que en 40D385 esta el CALL que llama a la API y un poco mas abajo hay un bucle que empieza a tomar valores y comienza a hacer una series de operaciones y como verán unos de los valores es la “Z” que es la cabecera del binario.

Bueno vamos por buen camino jejeje, seguimos traceando y encontramos otro bucle seguimos hasta el retn y salimos del call



Bueno como verán en la imagen tenemos con la flecha roja donde salimos en la flecha verde el call que si pasamos en el chau programa se cierra y justo por encima un JE y un JMP si JE salta nos manda directo al CALL así que nopeamos el JE y comenzamos a tracear



Como vemos el JMP evita el call le damos a F9 y.....

El programa arranca sin ningún problema guardamos los cambios y lo probamos fuera del olly y el programa arranca sin ningún problema y registrado.

Bueno eso es todos ya saben dudas solo pregunten.

Saludos a toda la lista.

Daniel –La Calavera -