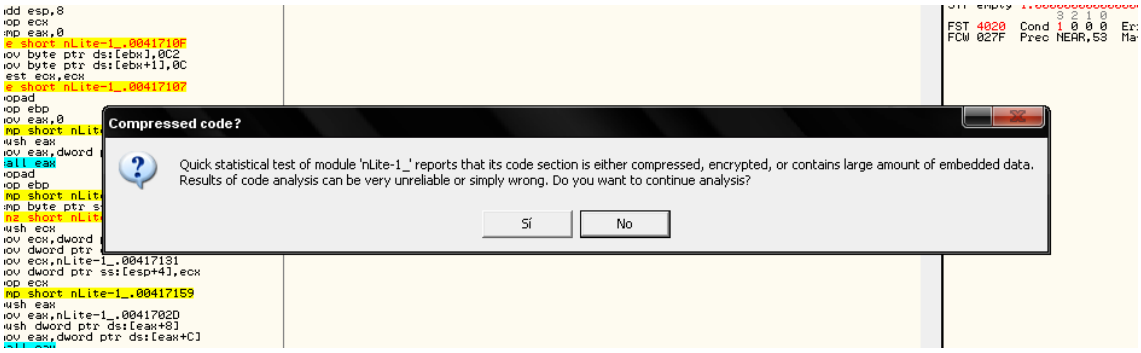
Programa	Instalador creado con installshield 2008 Professional.
Versión	Installshield 2008 Professional DEMO
Herramientas	Ollydbg
Compilador	¿¿¿¿¿¿?????????
Objetivos	Saltarnos la protección del número de serie
Cracker	**Noukeys**

Renuncia: Este tutorial es educativo y no persigue ningún tipo de lucro. El autor no se hace responsable del uso que se pueda hacer del mismo. Recuerdo que liberar cracks o cualquier software destinado a anular una protección es un delito.

Bueno, espero que este pequeño tutorial le sirva a mucha gente. Os expongo los antecedentes.

He descargado la ultima versión de installshield de la página oficial, después he utilizado su sistema de claves para proteger una instalación y tener algo con lo que jugar ☺. El resultado es los sorprendentemente fácil que resulta crackear este tipo de protección. Pero bueno, manos a la obra, que esto esta cracked en menos de 5 min.

Lo primero que hacemos, como siempre, es cargar nuestra víctima en Olly.



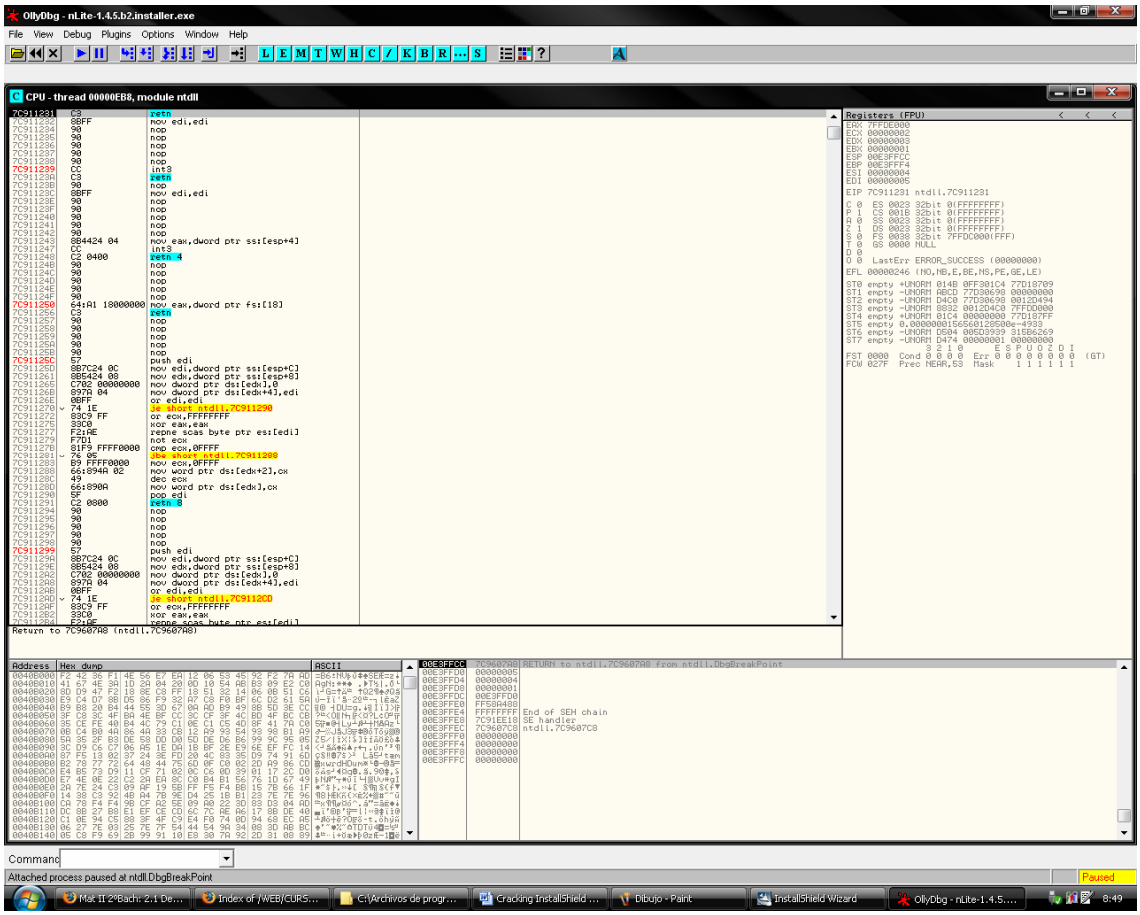
Mmm, empacado, vemos a ver si podemos continuar y convivir con el packer, es más fácil que centrarse en quitarlo ☺

Murió el proceso ☹

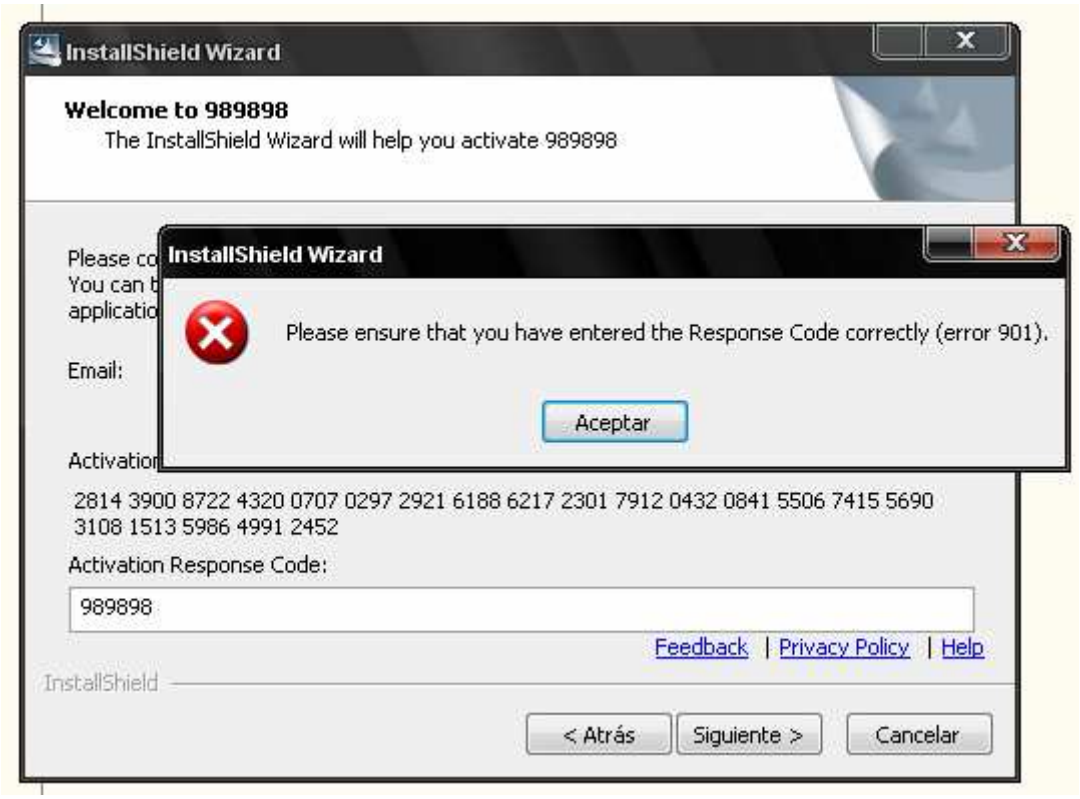
Bueno, ¿desde cuando ha sido esto motivo de preocupación? Jejeje, desde nunca ☺. Pues nada, a utilizar la opción de atach que trae nuestro maravilloso Olly.

Nota: *Antes de continuar, un recordatorio para los que lo sepáis, aclaración para los que no; installshield por defecto intenta activar los programas a través de Internet, por lo que vamos a desconectar nuestra conexión, para que cuando esto falle nos brinde la opción de activar a través del email.*

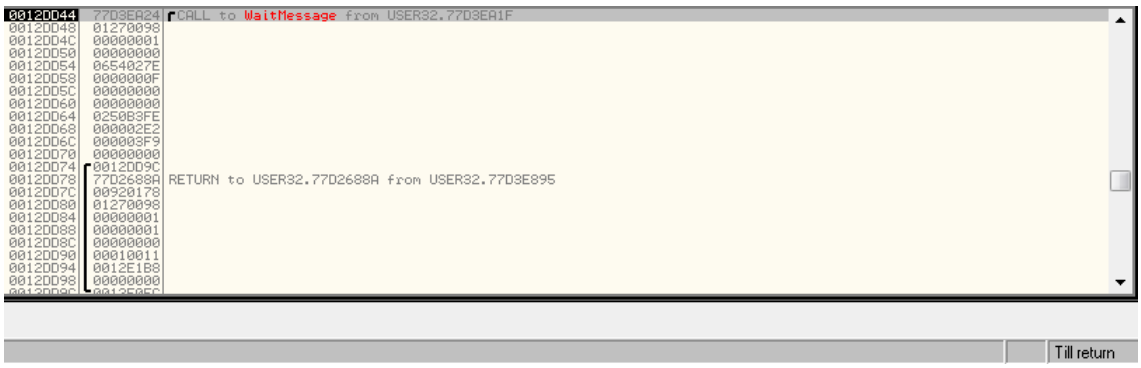
Bueno, en este punto del tutorial, todos tenemos nuestro Olly con el proceso atacheado y parado, como en la siguiente imagen:



Pulsamos [F9] para que continúe el proceso, y vamos a meter un número de serie, por ejemplo 989898 (… que original …) a ver que nos dice.

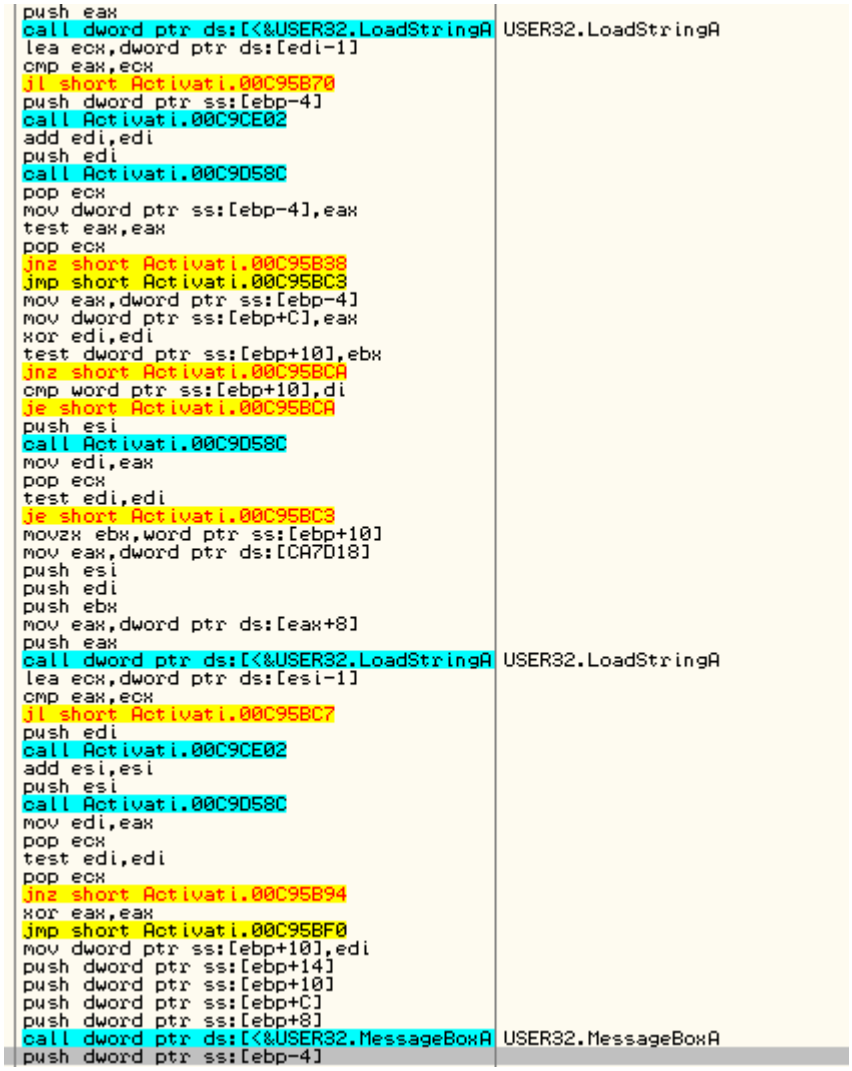


Bueno, parece que este número de serie no le ha gustado al programa, y nos ha devuelto un mensaje de error. Bueno, ahora llegar a la zona caliente es muy muy fácil. Simplemente, pausamos el programa [F12] y luego [Ctrl. + F9] hasta que veamos Hill Return como en la imagen

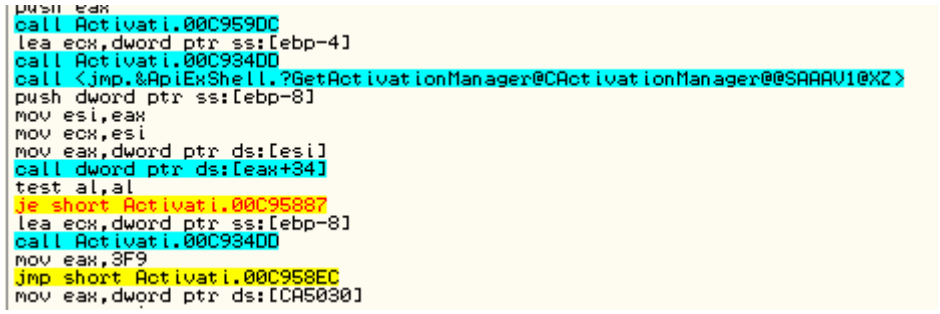


Si nos fijamos en la pila, el proceso está en “WaitMessage”. ☺ digamos que esta esperando una acción para procesarla. Pues esa acción va a ser la pulsación del botón aceptar. Una vez pulsado vemos que estamos parados en User32.

Vamos a llegar a la zona caliente mediante los returns, es decir [Ctrl. + F9] y si lo hacemos bien vemos que llegamos a esta zona, dentro del módulo principal del programa

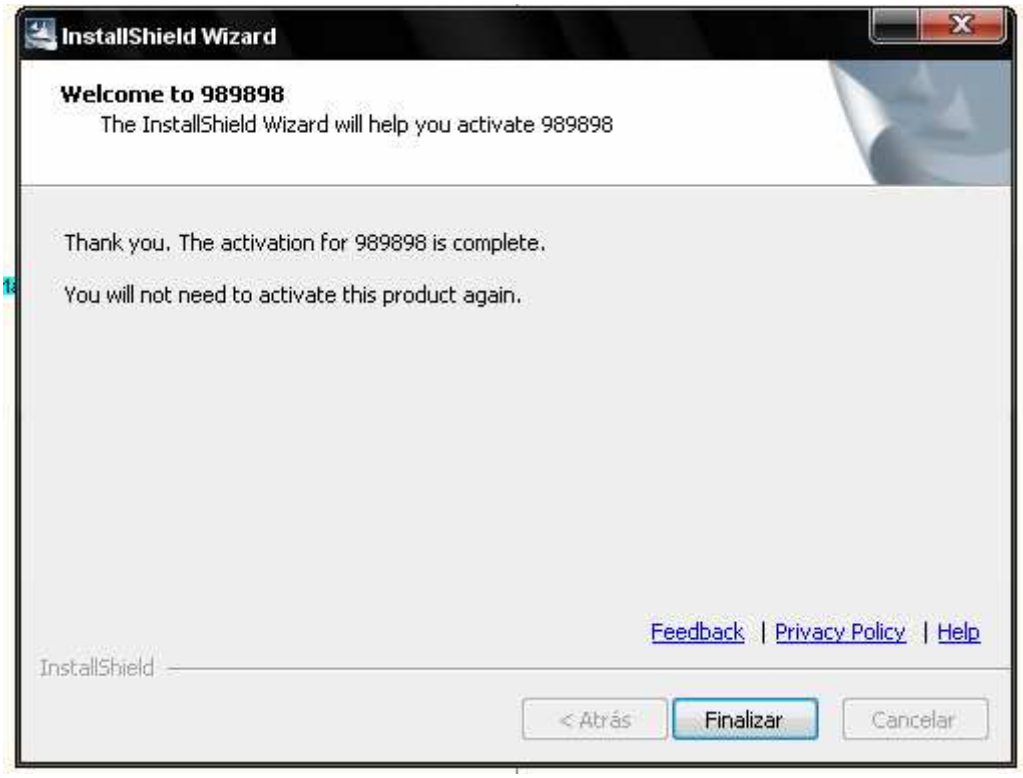


Bueno, cualquiera que lleve 5 min. depurando, sabe que es esto, la carga y posterior muestra del mensaje, pues un poco antes, vamos a llegar al salto mágico del instalador, ejecutamos el ret y… un poquito más arriba…



Mmmm, GetActivationManager …. un call y un salto ¿??? Mmm, que pasa si forzamos la cosa un poco¿?¿?¿?

Paramos en el jnz, cambiamos la flan Z, y el salto no se ejecuta, luego [F9] y….



OOooo, siiii, la pantalla de que somos unos campeones ☺. Espero que os sea de mucha utilidad y le saquéis partido.

Un abrazo de vuestro amigo noukeys

Noukeys 2.008