

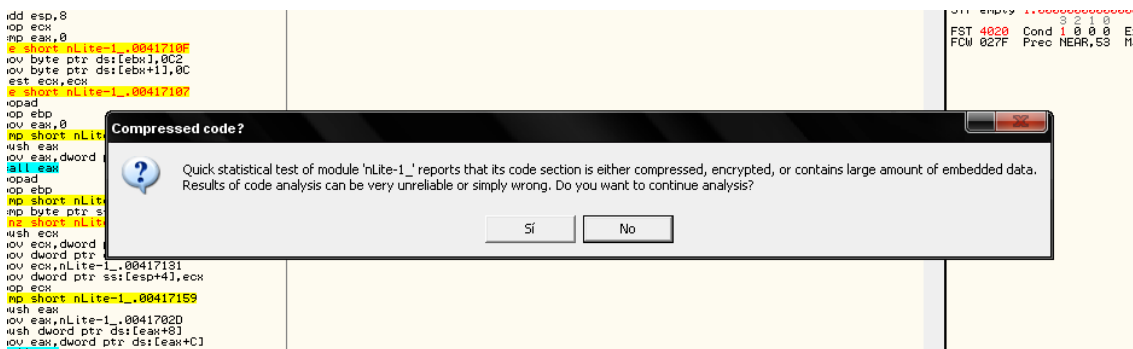
➤ Programa	Instalador creado con installshield 2008 Professional.
➤ Versión	Installshield 2008 Professional DEMO
➤ Herramientas	Ollydbg
➤ Compilador	????????????
➤ Objetivos	Saltarnos la protección del número de serie
➤ Cracker	Noukeys

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 última 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 😊

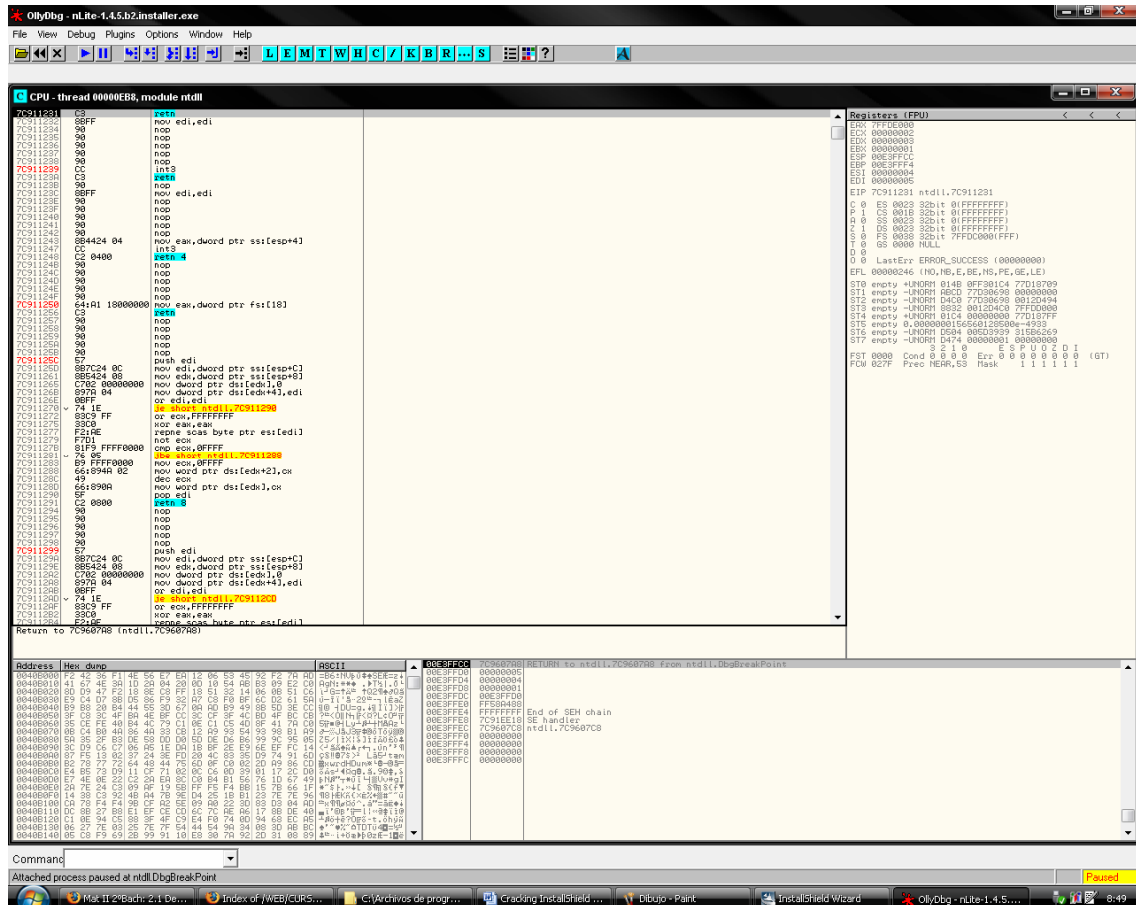


Murió el proceso 😊

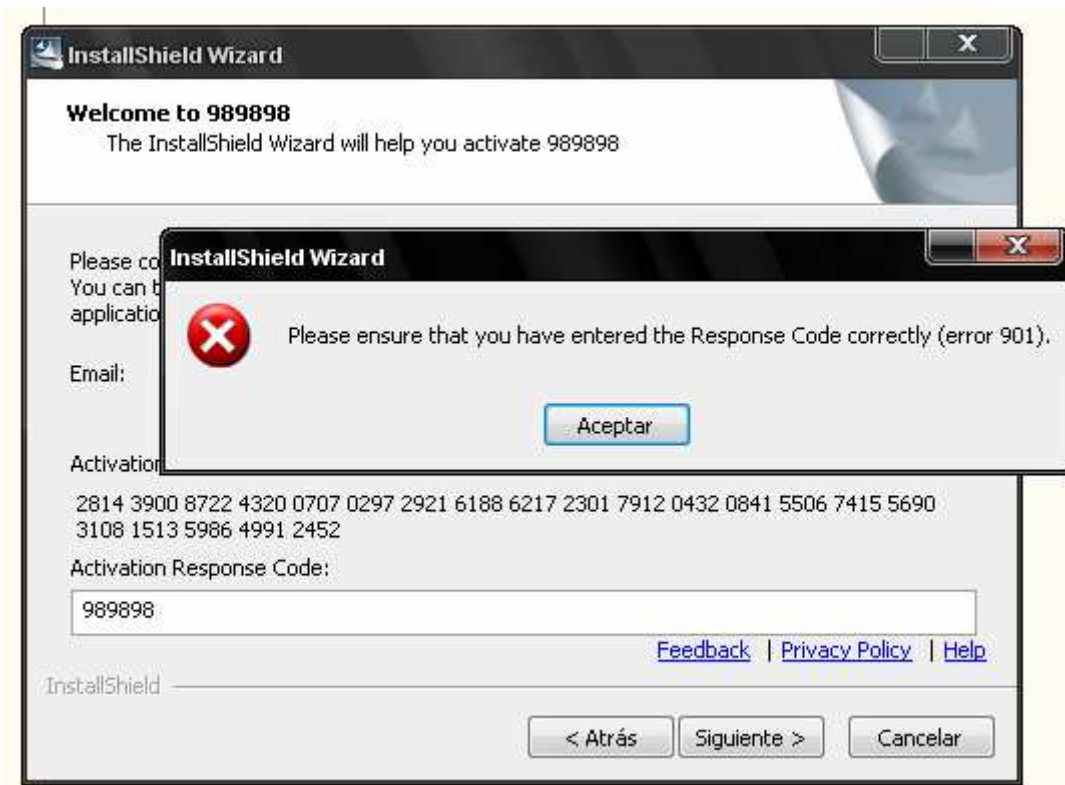
Bueno, ¿desde cuando ha sido esto motivo de preocupación? Jejeje, desde nunca ☺. Pues nada, a utilizar la opción de attach que trae nuestro maravilloso Olly.

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.

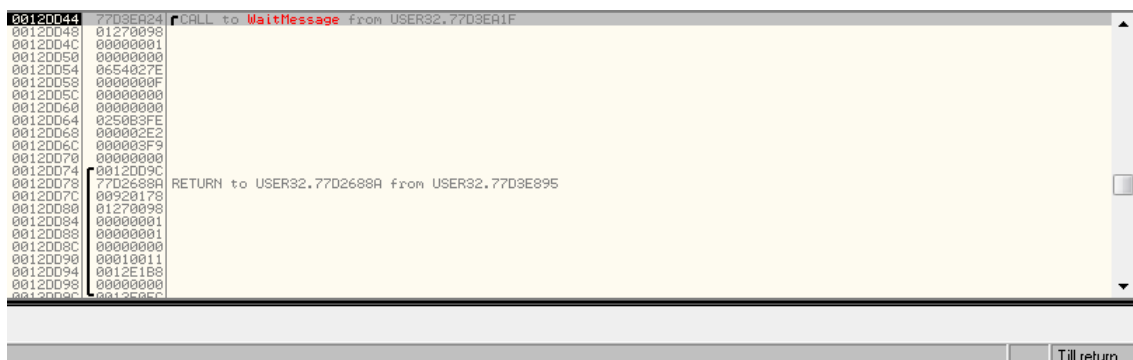
Bueno, en este punto del tutorial, todos tenemos nuestro Olly con el proceso atachado y parado, como en la siguiente imagen:



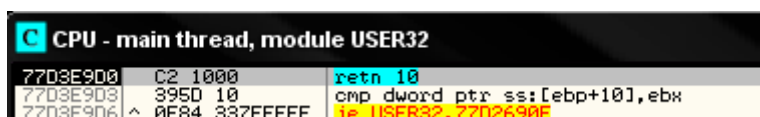
Pulsamos [F9] para que continúe el proceso, y vamos a meter un número de serie, por ejemplo 989898 (... que original ...) a ver que nos dice.



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

```

push eax
call dword ptr ds:[<&USER32.LoadStringA USER32.LoadStringA
lea ecx,dword ptr ds:[edi-1]
cmp eax,ecx
jl short Activati.00C95B70
push dword ptr ss:[ebp-4]
call Activati.00C9CE02
add edi,edi
push edi
call Activati.00C9D58C
pop ecx
mov dword ptr ss:[ebp-4],eax
test eax,eax
pop ecx
jnz short Activati.00C95B38
jmp short Activati.00C95BC3
mov eax,dword ptr ss:[ebp-4]
mov dword ptr ss:[ebp+C],eax
xor edi,edi
test dword ptr ss:[ebp+10],ebx
jnz short Activati.00C95BCA
cmp word ptr ss:[ebp+10],di
je short Activati.00C95BCA
push esi
call Activati.00C9D58C
mov edi,eax
pop ecx
test edi,edi
je short Activati.00C95BC3
movzx ebx,word ptr ss:[ebp+10]
mov eax,dword ptr ds:[CA7D18]
push esi
push edi
push ebx
mov eax,dword ptr ds:[eax+8]
push eax
call dword ptr ds:[<&USER32.LoadStringA USER32.LoadStringA
lea ecx,dword ptr ds:[esi-1]
cmp eax,ecx
jl short Activati.00C95BC7
push edi
call Activati.00C9CE02
add esi,esi
push esi
call Activati.00C9D58C
mov edi,eax
pop ecx
test edi,edi
pop ecx
jnz short Activati.00C95B94
xor eax,eax
jmp short Activati.00C95BF0
mov dword ptr ss:[ebp+10],edi
push dword ptr ss:[ebp+14]
push dword ptr ss:[ebp+10]
push dword ptr ss:[ebp+C]
push dword ptr ss:[ebp+8]
call dword ptr ds:[<&USER32.MessageBoxA USER32.MessageBoxA
push dword ptr ss:[ebp-4]

```

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...

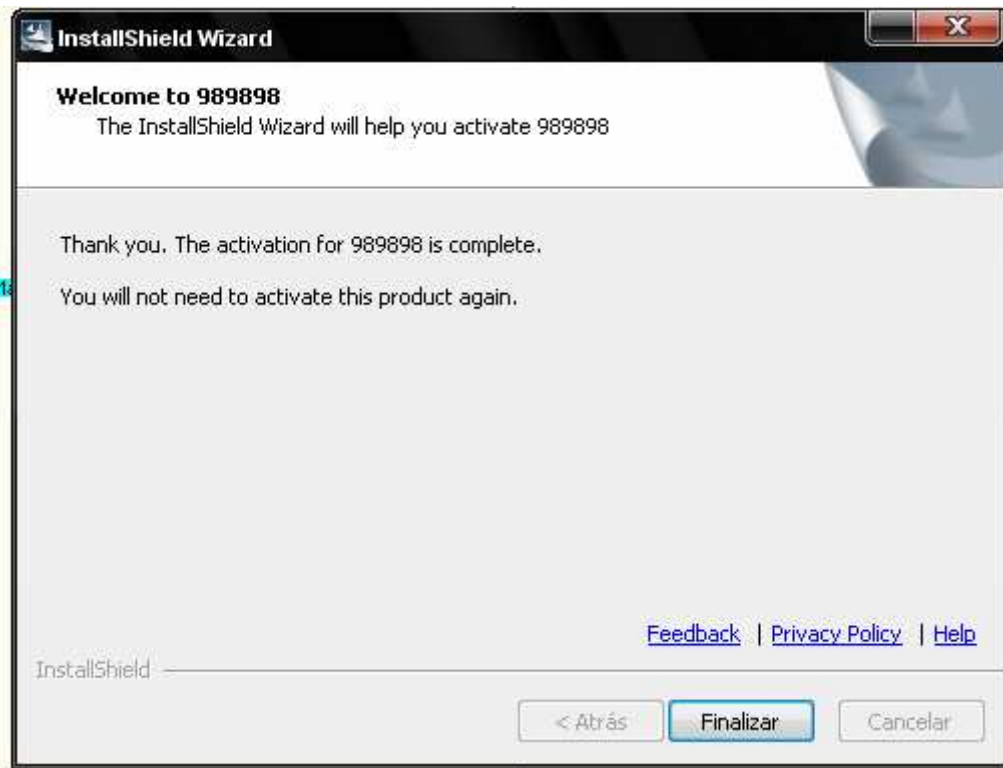
```

push eax
call Activati.00C959DC
lea ecx,dword ptr ss:[ebp-4]
call Activati.00C934D0
call <Jmp.&ApiExShell. ?GetActivationManager@CActivationManager@@SAAAU1@XZ>
push dword ptr ss:[ebp-8]
mov esi,eax
mov ecx,esi
mov eax,dword ptr ds:[esi]
call dword ptr ds:[eax+34]
test al,al
je short Activati.00C95887
lea ecx,dword ptr ss:[ebp-8]
call Activati.00C934D0
mov eax,3F9
jmp short Activati.00C958EC
mov eax,dword ptr ds:[CA5030]

```

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, siiiii, 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