



## Creando un auto-keygen para el plugin NeoBookDBPro 1.6a

Fecha	25 de marzo de 2017
Victima	NeoBookDBPro 1.6a
URL de descarga	<a href="http://www.neosoftware.com/software/NeoBookDBPro.exe">www.neosoftware.com/software/NeoBookDBPro.exe</a>
MD5 del instalador	EF1EFC5D2C1F6582B5078392E25C2152
Protección	UPX + registro
Herramientas	Exeinfo PE, OllyDbg, UPX 3.93w
Objetivo	Crear un auto-keygen
Dificultad	Baja/Media
Cracker	Aguml

## Indice

---

1. *Introducción*
2. *Análisis*
3. *Buscando un serial*
4. *Creando el auto-keygen*

# Introducción

---

Este plugin es para el programa NeoBook el cual viene empacado con Armadillo 9.64. El análisis sobre este plugin lo hice sin desempacar el Armadillo y, aunque ya conseguí desempacarlo, voy a explicar cómo hice para analizar el plugin sin desempacar y espero que a alguien le sirva de ayuda para afrontar otros casos similares.

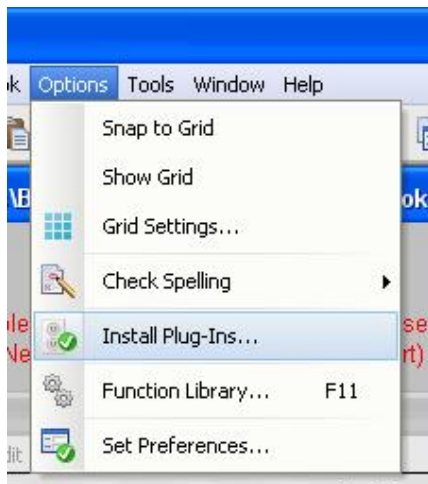
## Análisis

---

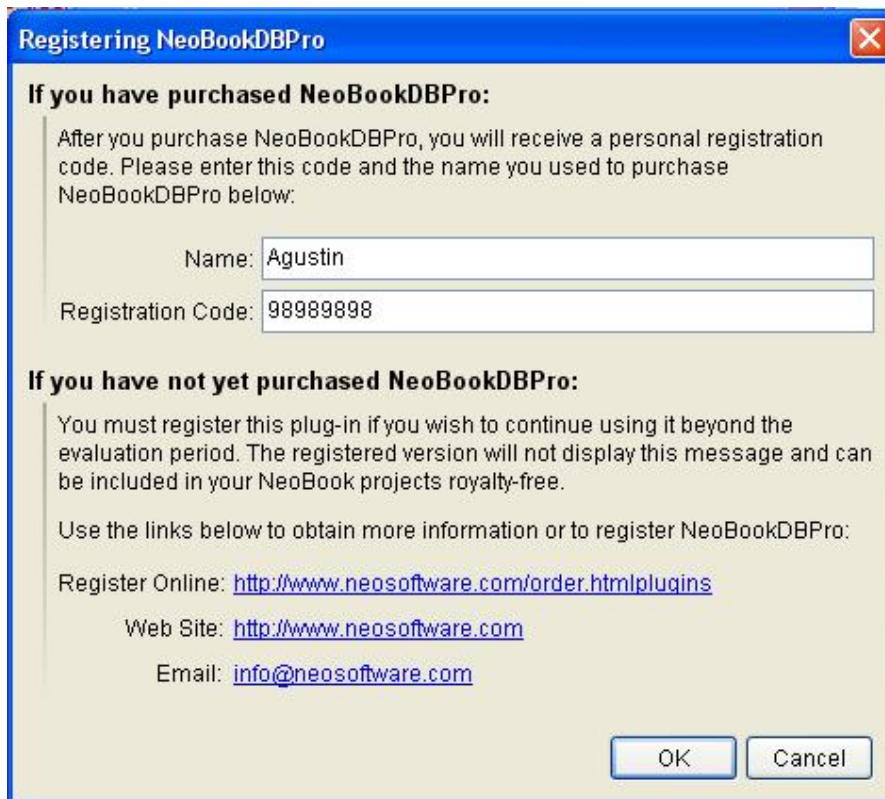
Al examinarlo se ve que está empacado con UPX, nada preocupante:



Intento registrar el plugin:



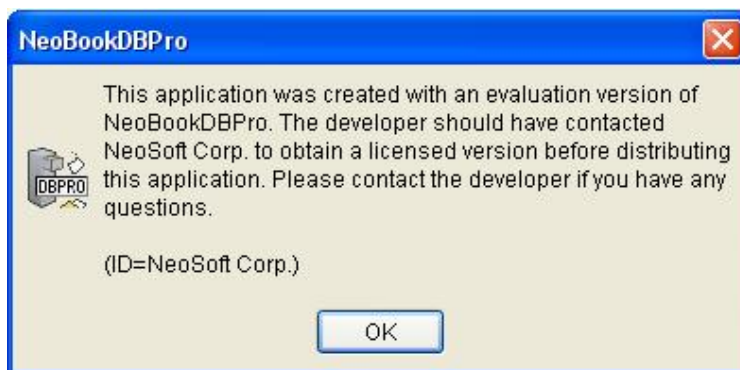
Se puede apreciar que, según la leyenda de la parte inferior de la ventana, el plugin no está registrado así que doy al botón “Register this Plug-in...”:



Y al aceptar:



Si compilo un proyecto de los mismos que trae de ejemplo veo esto al ejecutar el compilado:



Y al cerrar el compilado lo vuelve a mostrar.



# Buscando un serial

Abro NeoBook en Olly y, como sé que este programa tiene Armadillo y una de sus protecciones presentes es Debug-Blocker, doy a F9 para que funcione normalmente. En la CommandBar pongo un BP en WaitForDebugEvent y parará de inmediato así que hago Ctrl+F9 y F7 y caigo aquí:

007FEDC8	8B 8D F8DFFFF	mov	ecx, ss:[ebp-208]	
007FEDD3	51	push	ecx	
007FEDD4	FF 15 5CA08C00	call	ds:[8CA05C]	kernel32.WaitForDebugEvent
007FEDDA	85 C0	test	eax, eax	
007FEDDC	0F 84 89180000	je	0080066B	NeoBook.0080066B
007FEDE2	0FB695 03FEFF	movzx	edx, byte ptr ss:[ebp-1FD]	
007FEDE9	85 D2	test	edx, edx	
007FEDEB	74 12	je	short 007FEDFF	NeoBook.007FEDFF
007FEDED	A1 F4608E00	mov	eax, ds:[8E60F4]	

En Olly doy a Attach:

Select process to attach			
Process	Name	Window	Path
00000670	lsass		C:\WINDOWS\system32\lsass.
000005B4	mDNSRespo		C:\Archivos de programa\Bo
000006C0	MEGAsync	QTrayIconMessageWindow	C:\Documents and Settings\
000003C4	MSCam332		C:\Archivos de programa\Mi
000001FC	NeoBook	About NeoBook	C:\Archivos de programa\Ne
00000C9C	NeoBook	Default IME	C:\Archivos de programa\Ne
00000400	NitroPDF		C:\Archivos de programa\Ni
00000454	nvsvc32	NVSVCPPMWindowClass	C:\WINDOWS\system32\nvsvc3
00000C6C	OSPPSVC		C:\Archivos de programa\Ar
00000320	RTHDCPL	HDMI Settings	C:\WINDOWS\RTHDCPL.EXE
			Attach Cancel

Puedo ver corriendo dos procesos con el mismo nombre aunque el que necesito depurar es el que no está en rojo ya que el rojo es el padre y es el que ya estoy traceando. El otro es el hijo y necesito su PID para un pequeño injerto que queda así:

007FEDC8	8B 8D F8DFFFF	mov	ecx, ss:[ebp-208]	
007FEDD3	51	push	ecx	
007FEDD4	FF 15 5CA08C00	call	ds:[8CA05C]	kernel32.WaitForDebugEvent
007FEDDA	68 FC010000	push	1FC	
007FEDDF	E8 35D3057C	call	7C85C119	kernel32.DebugActiveProcessStop
007FEDE4	90	nop		
007FEDE5	90	nop		
007FEDE6	90	nop		
007FEDE7	90	nop		
007FEDE8	90	nop		
007FEDE9	85 D2	test	edx, edx	
007FEDEB	74 12	je	short 007FEDFF	NeoBook.007FEDFF

Paso esas dos líneas con F8 y abro otra instancia de Olly y atacheo al hijo con ese. No hay que cerrar al padre ni tocarlo más para nada, simplemente hay que dejarlo ahí dormidito.

Una vez estoy ya depurando al hijo, ya nos puedo dedicar plenamente a analizar al plugin.  
Doy a F9 e intento registrar el plugin y, cuando me salga el mensaje de chico malo, pauso el Olly y voy con Ctrl+F9 y F7 hasta que vuelva a tener el control del programa y acepto la ventana de chico malo:

042F7244	E8 1707FBFF	call	042A7960	jmp to USER32.GetActiveWindow
042F7249	3BD8	cmp	ebx, eax	
042F724B	74 05	je	short 042F7252	NeoBookD.042F7252
042F724D	33C0	xor	eax, eax	
042F724F	8945 E4	mov	ss:[ebp-1C], eax	
042F7252	33C0	xor	eax, eax	
042F7254	5A	pop	edx	
042F7255	59	pop	ecx	
042F7256	59	pop	ecx	
042F7257	64:8910	mov	fs:[eax], edx	
042F725A	68 6F722F04	push	42F726F	
042F725F	8B45 FC	mov	eax, ss:[ebp-4]	
042F7262	E8 61FDFFFF	call	042F6FC8	NeoBookD.042F6FC8
042F7267	C3	ret		
042F7268	E9 FFCDFAFF	jmp	042A406C	NeoBookD.042A406C
042F726D	EB F0	jmp	short 042F725F	NeoBookD.042F725F
042F726F	33C0	xor	eax, eax	
042F7271	5A	pop	edx	

Ya estoy en el código del plugin pero este sitio no es interesante para nada así que doy a F7 y voy con Ctrl+F9 y F7 hasta que llego aquí:

043A6698	8B80 FC020000	mov	eax, ds:[eax+2FC]	
043A669E	E8 5928F6FF	call	04308EFC	NeoBookD.04308EFC
043A66A3	A1 20984404	mov	eax, ds:[4449820]	
043A66A8	8B80 00030000	mov	eax, ds:[eax+300]	
043A66AE	33D2	xor	edx, edx	
043A66B0	E8 F72FF6FF	call	043096AC	NeoBookD.043096AC
043A66B5	A1 20984404	mov	eax, ds:[4449820]	
043A66BA	8B80 04030000	mov	eax, ds:[eax+304]	
043A66C0	33D2	xor	edx, edx	
043A66C2	E8 E52FF6FF	call	043096AC	NeoBookD.043096AC
043A66C7	A1 08744404	mov	eax, ds:[4447408]	
043A66CC	8B00	mov	eax, ds:[eax]	
043A66CE	33D2	xor	edx, edx	
043A66D0	E8 131FF5FF	call	042F85E8	NeoBookD.042F85E8
043A66D5	A1 20984404	mov	eax, ds:[4449820]	
043A66DA	8B10	mov	edx, ds:[eax]	
043A66DC	FF92 EC000000	call	ds:[edx+EC]	
043A66E2	66:8945 F6	mov	ss:[ebp-A], ax	
043A66E6	33C0	xor	eax, eax	

Esa zona sigue sin ser de interés ya que no hay ningún salto que lo evite así que sigo con Ctrl+F9 y F7 hasta que llego aquí:

043A6831	B8 66000000	mov	eax, 66	
043A6836	E8 D535F0FF	call	042A9E10	NeoBookD.042A9E10
043A683B	8B4D FC	mov	ecx, ss:[ebp-4]	
043A683E	8BD3	mov	edx, ebx	
043A6840	B8 74683A04	mov	eax, 43A6874	ASCII "NeoBookDBPro"
043A6845	E8 B2F9FFFF	call	043A61FC	NeoBookD.043A61FC
043A684A	33C0	xor	eax, eax	
043A684C	5A	pop	edx	
043A684D	59	pop	ecx	
043A684E	59	pop	ecx	
043A684F	64:8910	mov	fs:[eax], edx	
043A6852	68 67683A04	push	43A6867	ASCII "[Y]Ã"

Apostaría algo a que estoy justo debajo del CALL que muestra el mensaje de chico malo ya que tengo ahí el título del mensaje pero sigue sin haber ningún salto que lo evite así que sigo con Ctrl+F9 y F7 hasta que llego aquí:

04433657	. 8B93 20030000	mov	edx, ds:[ebx+320]	
0443365D	. 8BC3	mov	eax, ebx	
0443365F	. E8 1C1EECFF	call	042F5480	NeoBookD.042F5480
04433664	. 83BB 44030000	cmp	dword ptr ds:[ebx+344], 3	
0443366B	~ 75 21	jnz	short 0443368E	NeoBookD.0443368E
0443366D	. 8D55 E8	lea	edx, [local.6]	
04433670	. B8 B5080000	mov	eax, 8B5	
04433675	. E8 9667E7FF	call	042A9E10	NeoBookD.042A9E10
0443367A	. 8B45 E8	mov	eax, [local.6]	
0443367D	. E8 9231F7FF	call	043A6814	NeoBookD.043A6814
04433682	. C783 4C020000	mov	dword ptr ds:[ebx+24C], 2	
0443368C	~ EB 15	jmp	short 044336A3	NeoBookD.044336A3
0443368E	> 8D55 E4	lea	edx, [local.7]	
04433691	. B8 B6080000	mov	eax, 8B6	
04433696	. E8 7567E7FF	call	042A9E10	NeoBookD.042A9E10
0443369B	. 8B45 E4	mov	eax, [local.7]	
0443369E	. E8 7131F7FF	call	043A6814	NeoBookD.043A6814
044336A3	> 33C0	xor	eax, eax	
044336A5	. 5A	pop	edx	

Aquí sí que hay varios saltos que lo evitan así que pongo un BP en el inicio de la función

044335AB	. C3	retn	
044335AC	. 55	push	ebp
044335AD	. 8BEC	mov	ebp, esp
044335AF	. 33C9	xor	ecx, ecx
044335B1	. 51	push	ecx
044335B2	. 51	push	ecx
044335B3	. 51	push	ecx
044335B4	. 51	push	ecx
044335B5	. 51	push	ecx
044335B6	. 51	push	ecx
044335B7	. 51	push	ecx
044335B8	. 53	push	ebx
044335B9	. 8BD8	mov	ebx, eax

Doy a Ctrl+F9 y F7 hasta que llego aquí:



0430AD51	. C3	retn		
0430AD52	> F643 1C 10	test	byte ptr ds:[ebx+1C], 10	
0430AD56	~ 75 12	jnz	short 0430AD6A	NeoBookD.0430AD6A
0430AD58	. 837B 6C 00	cmp	dword ptr ds:[ebx+6C], 0	
0430AD5C	~ 74 0C	je	short 0430AD6A	NeoBookD.0430AD6A
0430AD5E	. 8BD3	mov	edx, ebx	
0430AD60	. 8B43 6C	mov	eax, ds:[ebx+6C]	
0430AD63	. 8B08	mov	ecx, ds:[eax]	
0430AD65	. FF51 18	call	ds:[ecx+18]	
0430AD68	~ EB 18	jmp	short 0430AD82	NeoBookD.0430AD82
0430AD6A	> 66:83BB 2201	cmp	word ptr ds:[ebx+122], 0	
0430AD72	~ 74 0E	je	short 0430AD82	NeoBookD.0430AD82
0430AD74	. 8BD3	mov	edx, ebx	
0430AD76	. 8B83 24010000	mov	eax, ds:[ebx+124]	
0430AD7C	. FF93 20010000	call	ds:[ebx+120]	
0430AD82	> 5B	pop	ebx	044F77AC
0430AD83	. C3	retn		

Me voy al inicio de la función y pongo un BP en la primera línea:

0430AD16	00	db	00	
0430AD17	00	db	00	
0430AD18	53	push	ebx	
0430AD19	. 8BD8	mov	ebx, eax	
0430AD1B	. 66:83BB 2201	cmp	word ptr ds:[ebx+122], 0	
0430AD23	~ 74 2D	je	short 0430AD52	NeoBookD.0430AD52
0430AD25	. 8BC3	mov	eax, ebx	
0430AD27	. 8B10	mov	edx, ds:[eax]	
0430AD29	. FF52 3C	call	ds:[edx+3C]	
0430AD2C	. 85C0	test	eax, eax	
0430AD2E	~ 74 22	je	short 0430AD52	NeoBookD.0430AD52
0430AD30	. 8BC3	mov	eax, ebx	

Doy a Ctrl+F9 y F7 y caigo aquí:

042E166F	00	db	00	
042E1670	. A0000000	dd	000000A0	
042E1674	. 53	push	ebx	
042E1675	. 8BD8	mov	ebx, eax	
042E1677	. 8BC3	mov	eax, ebx	
042E1679	. E8 66FD0000	call	042F13E4	NeoBookD.042F13E4
042E167E	. 85C0	test	eax, eax	
042E1680	~ 74 0C	je	short 042E168E	NeoBookD.042E168E
042E1682	. 8B93 14020000	mov	edx, ds:[ebx+214]	
042E1688	. 8990 4C020000	mov	ds:[eax+24C], edx	
042E168E	> 8BC3	mov	eax, ebx	
042E1690	. E8 83960200	call	0430AD18	NeoBookD.0430AD18
042E1695	. 5B	pop	ebx	0012E668
042E1696	. C3	retn		
042E1697	90	nop		
042E1698	. 33C0	xor	eax, eax	
042E169A	. C3	retn		
042E169B	90	nop		

Esa zona no tiene interés porque la función es muy pequeña y no hay ningún salto que evite que se ejecute el CALL así que sigo con Ctrl+F9 y F7 y caigo aquí:



042E1757	00	db	00	
042E1758	. 42 55 54 54	ascii	"BUTTON",0	
042E175F	00	db	00	
042E1760	. 53	push	ebx	
042E1761	. 8BD8	mov	ebx, eax	
042E1763	. 8BC3	mov	eax, ebx	
042E1765	. E8 6EB90200	call	0430D0D8	NeoBookD.0430D0D8
042E176A	. 8A83 10020000	mov	al, ds:[ebx+210]	
042E1770	. 8883 12020000	mov	ds:[ebx+212], al	
042E1776	. 5B	pop	ebx	
042E1777	. C3	retn		
042E1778	. 56	push	esi	
042E1779	. 66:837A 06 00	cmp	word ptr ds:[edx+6], 0	
042E177E	75 09	jnz	short 042E1789	NeoBookD.042E1789
042E1780	. 66:BE EBFF	mov	si, 0FFEB	
042E1784	. E8 4323FCFF	call	042A3ACC	NeoBookD.042A3ACC
042E1789	> 5E	pop	esi	044F77AC
042E178A	. C3	retn		
042E178B	. 90	nop		
042E178C	. 53	push	ebx	

La experiencia me dice que aquí no hay mucho que rascar así que doy Ctrl+F9 y F7 y caigo aquí:

0430ABEA	. 8BC6	mov	eax, esi	
0430ABEC	. 66:BE C9FF	mov	si, 0FFC9	
0430ABC0	. E8 078FF9FF	call	042A3ACC	NeoBookD.042A3ACC
0430ABC5	EB 20	jmp	short 0430ABE7	NeoBookD.0430ABE7
0430ABC7	> 3D 0BB00000	cmp	eax, 0B00B	
0430ABCC	75 10	jnz	short 0430ABDE	NeoBookD.0430ABDE
0430ABCE	. 8B53 08	mov	edx, ds:[ebx+8]	
0430AED1	. 52	push	edx	Arg1
0430ABD2	. 8B4B 04	mov	ecx, ds:[ebx+4]	
0430ABD5	. 8BD0	mov	edx, eax	
0430ABD7	. 8BC6	mov	eax, esi	
0430ABD9	. E8 4EE7FFFF	call	0430932C	NeoBookD.0430932C
0430ABDE	> 8BD3	mov	edx, ebx	
0430ABE0	. 8BC6	mov	eax, esi	
0430ABE2	. 8B08	mov	ecx, ds:[eax]	
0430ABE4	. FF51 EC	call	ds:[ecx-14]	
0430ABE7	> 5F	pop	edi	0012E668
0430ABE8	. 5E	pop	esi	
0430ABE9	. 5B	pop	ebx	
0430ABEA	. 8BE5	mov	esp, ebp	
0430ABEC	. 5D	pop	ebp	
0430ABED	. C3	retn		
0430ABEE	. 8BC0	mov	eax, eax	

Si miro más arriba veo esto:

0430AB29	. 48	dec	eax	
0430AB2A	~ 74 17	je	short 0430AB43	NeoBookD.0430AB43
0430AB2C	~ EB 39	jmp	short 0430AB67	NeoBookD.0430AB67
0430AB2E	> 8BCB	mov	ecx, ebx	Case 200 (WM_MOUSEMOVE) of
0430AB30	. A1 AC704404	mov	eax, ds:[44470AC]	
0430AB35	. 8B00	mov	eax, ds:[eax]	
0430AB37	. 8BD6	mov	edx, esi	
0430AB39	. E8 FE05FFFF	call	042FB13C	NeoBookD.042FB13C
0430AB3E	~ E9 9B000000	jmp	0430ABDE	NeoBookD.0430ABDE
0430AB43	> 807E 5D 01	cmp	byte ptr ds:[esi+5D], 1	Cases 201 (WM_LBUTTONDOWN),
0430AB47	~ 75 10	jnz	short 0430AB59	NeoBookD.0430AB59
0430AB49	. 8BC6	mov	eax, esi	
0430AB4B	. 66:BE EDFD	mov	si, OFFED	
0430AB4F	. E8 788FF9FF	call	042A3ACC	NeoBookD.042A3ACC
0430AB54	~ E9 8E000000	jmp	0430ABE7	NeoBookD.0430ABE7
0430AB59	> 66:834E 54 01	or	word ptr ds:[esi+54], 1	
0430AB5E	~ EB 7E	jmp	short 0430ABDE	NeoBookD.0430ABDE
0430AB60	> 66:8366 54 FF	and	word ptr ds:[esi+54], OFFFE	Case 202 (WM_LBUTTONUP) of
0430AB65	~ EB 77	jmp	short 0430ABDE	NeoBookD.0430ABDE
0430AB67	> A1 208B4404	mov	eax, ds:[4448B20]	Default case of switch 0430
0430AB6C	. 8078 20 00	cmp	byte ptr ds:[eax+20], 0	
0430AB70	~ 74 6C	je	short 0430ABDE	NeoBookD.0430ABDE

Es un gestor de eventos y puedo observar como irá a la zona donde estoy parado con el evento WM\_LBUTTONDOWN.

Creo que ya me pasé así que doy a F9 y vuelvo a intentar registrarme y para en el último BP que puse y desde ahí voy traceando con F8 observando bien la pila y los registros por si veo algo sospechoso pero acabo cayendo en el siguiente BP que está en 044335AC sin ver nada extraño.

Sigo con F8 hasta que veo esto:

044335BD	. 55	push	ebp	
044335BE	. 68 CB364304	push	44336CB	
044335C3	. 64:FF30	push	dword ptr fs:[eax]	
044335C6	. 64:8920	mov	fs:[eax], esp	
044335C9	. 8D55 FC	lea	edx, [local.1]	
044335CC	. 8B83 20030000	mov	eax, ds:[ebx+320]	
044335D2	. E8 B561EDFF	call	0430978C	NeoBookD.0430978C
044335D7	. 837D FC 00	cmp	[local.1], 0	
044335DB	~ 0F86 C2000000	jbe	044336A3	NeoBookD.044336A3

Stack ss:[0012E4E8]=044F8D74, (ASCII "98989898")

Sigo traceando con F8 y veo esto:

044335DB	~ 0F86 C2000000	jbe	044336A3	NeoBookD.044336A3
044335E1	. 8D55 F8	lea	edx, [local.2]	
044335E4	. 8B83 0C030000	mov	eax, ds:[ebx+30C]	
044335EA	. E8 9D61EDFF	call	0430978C	NeoBookD.0430978C
044335EF	. 837D F8 00	cmp	[local.2], 0	
044335F3	~ 0F86 AA000000	jbe	044336A3	NeoBookD.044336A3
044335F9	. 8D55 F4	lea	edx, [local.3]	

Stack ss:[0012E4E4]=044FD4C4, (ASCII "Agustin")

Sigo traceando con F8:



044335F9	. 8D55 F4	lea	edx, [local.3]	
044335FC	. 8B83 20030000	mov	eax, ds:[ebx+320]	
04433602	. E8 8561EDFF	call	0430978C	NeoBookD.0430978C
04433607	. 8B45 F4	mov	eax, [local.3]	
0443360A	. 50	push	eax	

Stack ss:[0012E4E0]=044F8D8C, (ASCII "98989898")  
 eax=00000008

Sigo con F8 y veo esto:

0443360E	. 8B83 0C030000	mov	eax, ds:[ebx+30C]	
04433614	. E8 7361EDFF	call	0430978C	NeoBookD.0430978C
04433619	. 8B45 F0	mov	eax, [local.4]	
0443361C	. B1 01	mov	cl, 1	
0443361E	. 5A	pop	edx	
0443361F	. E8 C45EF7FF	call	043A94E8	NeoBookD.043A94E8
04433624	. 84C0	test	al, al	
04433626	. 74 29	je	short 04433651	NeoBookD.04433651
04433628	. A1 A06B4404	mov	eax, ds:[4446BA0]	
0443362D	. C600 01	mov	byte ptr ds:[eax], 1	
04433630	. 8D55 EC	lea	edx, [local.5]	
04433633	. B8 B4080000	mov	eax, 8B4	
04433638	. E8 D367E7FF	call	042A9E10	NeoBookD.042A9E10
0443363D	. 8B45 FC	mov	eax, [local.5]	

Stack ss:[0012E4DC]=044FD0E4, (ASCII "Agustin")  
 eax=00000007

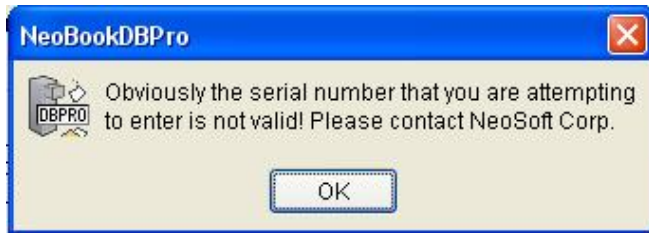
Se puede observar que cada vez que llama a esa función se retorna un puntero a una cadena y en EAX obtengo el largo de la cadena.

Sigo traceando y llego aquí:

0443365F	. E8 1C1EECFF	call	042F5480	NeoBookD.042F5480
04433664	. 83BB 44030000	cmp	dword ptr ds:[ebx+344], 3	
0443366B	. 75 21	jnz	short 0443368E	NeoBookD.0443368E
0443366D	. 8D55 E8	lea	edx, [local.6]	
04433670	. B8 B5080000	mov	eax, 8B5	
04433675	. E8 9667E7FF	call	042A9E10	NeoBookD.042A9E10
0443367A	. 8B45 E8	mov	eax, [local.6]	
0443367D	. E8 9231F7FF	call	043A6814	NeoBookD.043A6814
04433682	. C783 4C020000	mov	dword ptr ds:[ebx+24C], 2	
0443368C	. EB 15	jmp	short 044336A3	NeoBookD.044336A3
0443368E	. 8D55 E4	lea	edx, [local.7]	
04433691	. B8 B6080000	mov	eax, 8B6	
04433696	. E8 7567E7FF	call	042A9E10	NeoBookD.042A9E10
0443369B	. 8B45 E4	mov	eax, [local.7]	
0443369E	. E8 7131F7FF	call	043A6814	NeoBookD.043A6814
044336A3	. 33C0	xor	eax, eax	

Stack ss:[0012E4D0]=044F8DA4, (ASCII "The serial number that you entered is not valid!!Please che  
 eax=0012E4A4

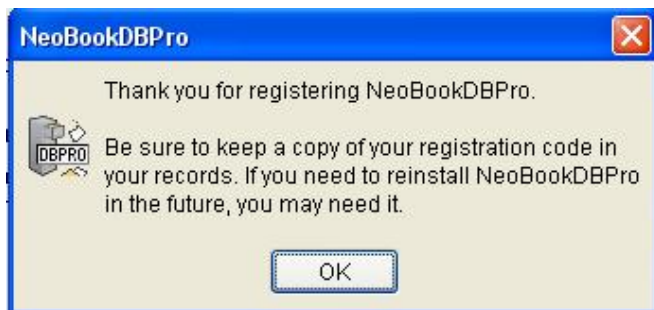
Pues me he pasado. Pongo un BP en el salto condicional que hay más arriba y vuelvo a intentarlo y cuando pare en el salto lo invierto para ver qué pasa y obtengo esto:



Ese salto no nos sirve así que subo un poco más y pongo un BP en él:

0443361C	. B1 01	mov	cl, 1	
0443361E	. 5A	pop	edx	
0443361F	. E8 C45EF7FF	call	043A94E8	NeoBookD.043A94E8
04433624	. 84C0	test	al, al	
04433626	~ 74 29	je	short 04433651	NeoBookD.04433651
04433628	. A1 A06B4404	mov	eax, ds:[4446BA0]	
0443362D	. C600 01	mov	byte ptr ds:[eax], 1	
04433630	. 8D55 EC	lea	edx, [local.5]	
04433633	. B8 B4080000	mov	eax, 8B4	
04433638	. E8 D367E7FF	call	042A9E10	NeoBookD.042A9E10
0443363D	. 8B45 EC	mov	eax, [local.5]	
04433640	. E8 CF31F7FF	call	043A6814	NeoBookD.043A6814
04433645	. C783 4C020000	mov	dword ptr ds:[ebx+24C], 1	
0443364F	~ EB 52	jmp	short 044336A3	NeoBookD.044336A3
04433651	. FF00 44000000	jmp	dword ptr ds:[ebx+244]	

Cuando pare lo invierto y veo esto:



Pues me da que el CALL de arriba tiene algo que ver así que pongo un BP en el CALL, desinstalo el plugin desde la misma ventana del programa dando al botón “Remove” y vuelvo a instalarlo dando en el botón “Install” y vuelvo a intentar registrarlo y, cuando pare, entro en él. Sigo traceando con F8 hasta que llego aquí:



```

05569509 55          push     ebp
0556950A 68 20985605 push     5569820
0556950F 64:FF30     push     dword ptr fs:[eax]
05569512 64:8920     mov      fs:[eax], esp
05569515 C645 F7 00  mov      byte ptr ss:[ebp-9], 0
05569519 8B45 F8     mov      eax, ss:[ebp-8]
0556951C E8 B7B5EFFF call     05464AD8
05569521 83F8 22     cmp      eax, 22
05569524 0F85 0C020000 jnz      05569736
0556952A 8B45 FC     mov      eax, ss:[ebp-4]
0556952D E8 A6B5EFFF call     05464AD8

```

eax=00000008

Al entrar a ese CALL tenía en EAX el puntero al serial mío y salgo con el largo de este y justo debajo una comparación con 0x22 que no va a pasar así que voy hasta el salto y hago que no salte y sigo traceando hasta que llego aquí:

```

05569521 83F8 22     cmp      eax, 22
05569524 0F85 0C020000 jnz      05569736
0556952A 8B45 FC     mov      eax, ss:[ebp-4]
0556952D E8 A6B5EFFF call     05464AD8
05569532 83F8 03     cmp      eax, 3
05569535 0F8C FB010000 jl       05569736
0556953B 84DB       test     bl, bl
0556953D 0F85 5E010000 jnz      055696A1

```

eax=00000007

Hace lo mismo con el nombre comprobando que el nombre tenga al menos 3 caracteres. Como mi nombre tiene más de 3 caracteres no me preocupa así que sigo traceando con F8 y voy viendo que hace operaciones con mi serial y mi nombre hasta que llego aquí:

```

05569707 8D4D F0     lea      ecx, ss:[ebp-10]
0556970A 8BD3       mov      edx, ebx
0556970C 8B45 FC     mov      eax, ss:[ebp-4]
0556970F E8 00FCFFFF call     05569314
05569714 84C0       test     al, al
05569716 0F84 E1000000 je       055697FD
0556971C 8B45 F0     mov      eax, ss:[ebp-10]
0556971F 8B55 F8     mov      edx, ss:[ebp-8]
05569722 E8 FDB4EFFF call     05464C24
05569727 0F85 D0000000 jnz      055697FD
0556972D C645 F7 01  mov      byte ptr ss:[ebp-9], 1
05569731 E8 C7B5EFFF call     05464AD8

```

NeoBookD.05569314  
NeoBookD.055697FD  
NeoBookD.05464C24  
NeoBookD.055697FD  
NeoBookD.055697FD

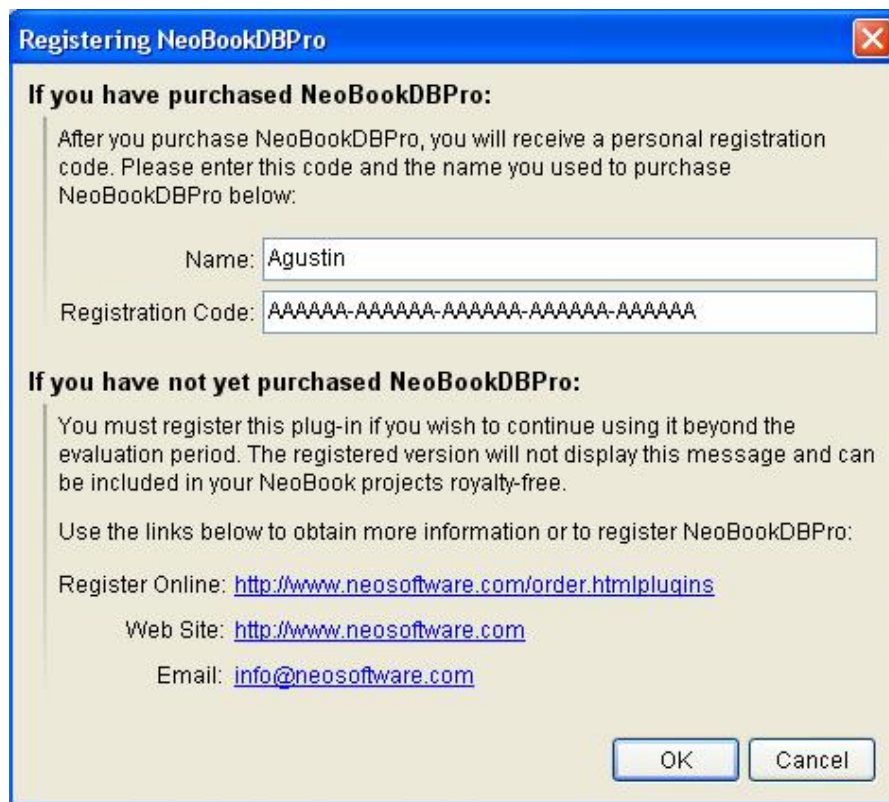
```

Registers (FPU)
EAX 0522ECEC ASCII "K57FCC-202615-3E5C09-72F989-DC2"
ECX 0012E414
EDX 0522E9A8 ASCII "98989898"
EBX 00000000
ESP 0012E410

```

Se ve mi serial y lo que parece un serial bueno. Si paso el CALL me devuelve en EAX el valor 0x17 que es justo el largo del serial que se ve en EAX menos el largo de mi serial. El serial que se muestra en EAX tiene un largo de 0x1F y como vi que se comparaba mi serial con 0x22 doy por hecho que ese serial tampoco es válido. De todos

modos, una vez que pase el CALL, invierto el salto y sigo traceando hasta que veo que me muestra la ventana de chico bueno. Estoy muy cerca así que pongo un BP en ese CALL y ahora intentaré registrarme con un serial de 0x22 caracteres con el formato que se muestra arriba:



**Registering NeoBookDBPro**

**If you have purchased NeoBookDBPro:**

After you purchase NeoBookDBPro, you will receive a personal registration code. Please enter this code and the name you used to purchase NeoBookDBPro below:

Name:

Registration Code:

**If you have not yet purchased NeoBookDBPro:**

You must register this plug-in if you wish to continue using it beyond the evaluation period. The registered version will not display this message and can be included in your NeoBook projects royalty-free.

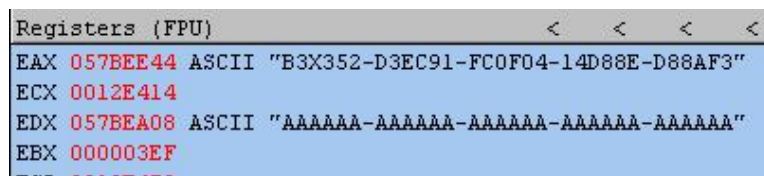
Use the links below to obtain more information or to register NeoBookDBPro:

Register Online: <http://www.neosoftware.com/order.htmlplugins>

Web Site: <http://www.neosoftware.com>

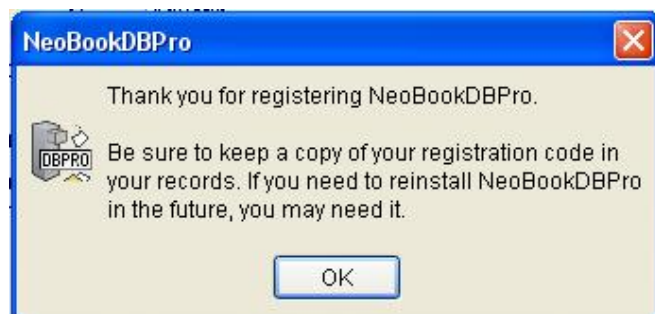
Email: [info@neosoftware.com](mailto:info@neosoftware.com)

Y al parar en el CALL veo esto:




Registers (FPU)	
EAX	057BEE44 ASCII "B3X352-D3EC91-FC0F04-14D88E-D88AF3"
ECX	0012E414
EDX	057BEA08 ASCII "AAAAAA-AAAAAA-AAAAAA-AAAAAA-AAAAAA"
EBX	000003EF

Ese serial parece tener un formato correcto así que lo copio e intento registrarme con él y:



**NeoBookDBPro**

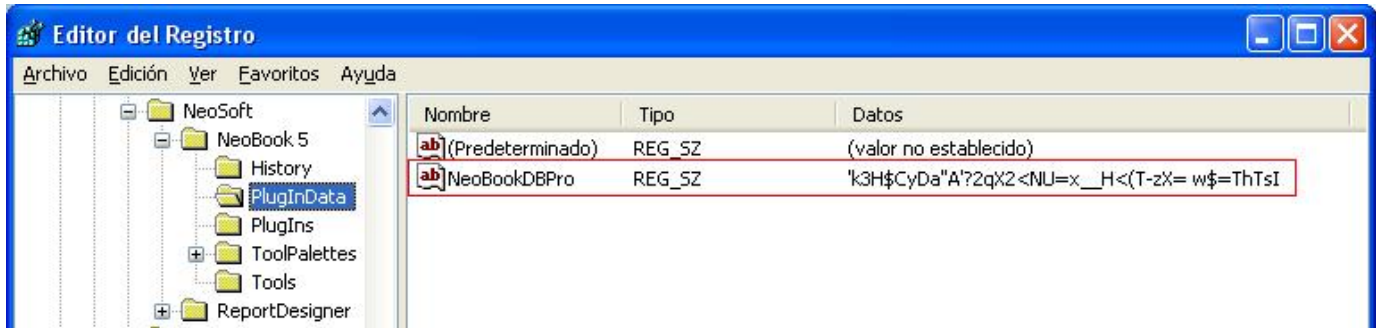
Thank you for registering NeoBookDBPro.

 Be sure to keep a copy of your registration code in your records. If you need to reinstall NeoBookDBPro in the future, you may need it.

Si cierro el programa y vuelvo a abrirlo sigo estando registrado y cuando compilo ya no muestra ningún mensaje molesto con lo que el serial sí que es bueno jejeje.

# Creando el auto-keygen

Como ya tengo un lugar donde se muestra el serial ¿Por qué no intentar crear un auto-keygen?  
Para ello primero tengo que eliminar la entrada del registro para poder seguir trasteando:



La ruta completa es “HKEY\_CURRENT\_USER\Software\NeoSoft\NeoBook 5\PlugInData”.

Elimino esa clave, desinstalo el plugin dando al botón “Remove”.

Desempaco el plugin para poder injertar lo que quiera y vuelvo a instalarlo dando al botón “Install” y ya puedo seguir jugando con el plugin descriptado.

Pongo un BP en el CALL que muestra el serial e intento registrarme con el serial “AAAAAA-AAAAAA-AAAAAA-AAAAAA-AAAAAA” y cuando pare cambio el CALL por el salto a mi injerto que irá en una zona vacía al final de la sección:

0550970F	E8 00FCFFFF	call	05509314	NeoBookD.05509314
05509714	84C0	test	al, al	
05509716	0F84 E1000000	je	055097FD	NeoBookD.055097FD
0550971C	8B45 F0	mov	eax, ss:[ebp-10]	
0550971F	8B55 F8	mov	edx, ss:[ebp-8]	
05509722	E9 77170900	jmp	0559AE9E	NeoBookD.0559AE9E
05509727	0F85 D0000000	jnz	055097FD	NeoBookD.055097FD
0550972D	C645 F7 01	mov	byte ptr ss:[ebp-9], 1	
05509731	E9 C7000000	jmp	055097FD	NeoBookD.055097FD
05509736	8B45 F8	mov	eax, ss:[ebp-8]	
05509739	E8 9AB3EFFF	call	05404AD8	NeoBookD.05404AD8

Busco una zona vacía al final de la sección donde escribiré mi injerto que queda así:

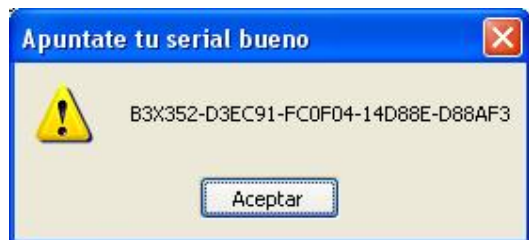
0559AE98	0000	add	ds:[eax], al	
0559AE9A	0000	add	ds:[eax], al	
0559AE9C	0000	add	ds:[eax], al	
0559AE9E	60	pushad		
0559AE9F	68 30200000	push	2030	
0559AEA4	8B4C24 28	mov	ecx, ss:[esp+28]	
0559AEA8	81C1 60160900	add	ecx, 91660	
0559AEAE	51	push	ecx	
0559AEAF	50	push	eax	
0559AEB0	6A 00	push	0	
0559AEB2	E8 9964E6FF	call	05401350	<jmp.<user32.MessageBoxA>
0559AEB7	61	popad		
0559AEB8	E8 679DE6FF	call	05404C24	NeoBookD.05404C24
0559AEBD	E9 65E8F6FF	jmp	05509727	NeoBookD.05509727
0559AEC2	0000	add	ds:[eax], al	
0559AEC4	0000	add	ds:[eax], al	

Y para la cadena que usaré para el título del mensaje:

Address	Hex dump	ASCII
0559AE80	41 70 75 6E 74 61 74 65 20 74 75 20 73 65 72 69	Apuntate tu seri
0559AE90	61 6C 20 62 75 65 6E 6F 00 00 00 00 00 00 60 68	al bueno.....`h

Lo que tengo es un PUSHAD para guardar los registros, un MessageBoxA donde mostraré el serial y cuyo título será el que se ve en el Dump, después uso POPAD para restaurar los registros, ejecuto la línea que me cargo con el salto y por ultimo retorno a la línea por la que debería seguir ejecutándose.

Si doy a F9 veo esto:



Guardo todos los cambios y ya tengo un auto-keygen que me mostrará el serial correcto para el nombre deseado. Solo hay una pega y es que a esa zona entra siempre que verifica el serial y por lo tanto nos mostrará el serial bueno incluso aunque esté ya registrados e incluso al iniciar NeoBook con lo que una vez conseguido el serial bueno es mejor remover el parcheado dando al botón “Remove” e instalar el original pulsando en el botón “Install” y registrarlo con el serial obtenido y listo.