



# funsoundplayer

By Apuromafo

Un mini tute, una app con EC(execryptor)

**casa**

**Escrito por: Apuromafo**

***DESCARGO LEGAL***

**DOCUMENTO ESCRITO PARA FINES DE  
*EDUCACION/iNVESTiGACION***

Fecha: 28/06/08  
Revisión: 17/6/11

Pido disculpas de las posibles faltas de ortografía y marcas de agua, pero prefiero a que se publique a que quede guardado en un lugar sin mover

Todo comenzó por aquí:

[http://foro.elhacker.net/ingenieria\\_inversa/que\\_piensan\\_del\\_flashwamp-t202073.0.html](http://foro.elhacker.net/ingenieria_inversa/que_piensan_del_flashwamp-t202073.0.html)

luego analizando mas tenemos esto:

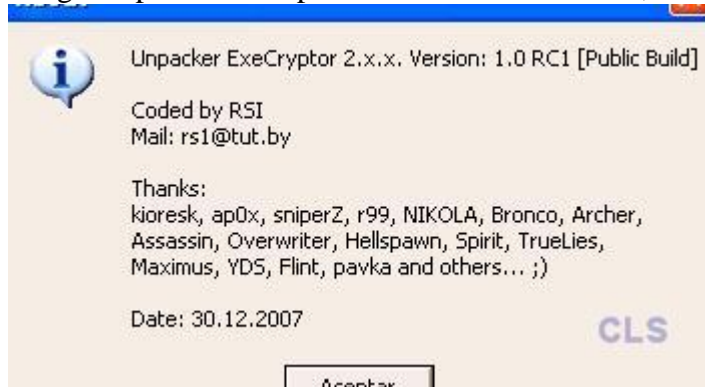
Flash WAMP transforma cualquier piel original de Winamp para Flash basado en el reproductor de música de Internet. Dan vida a su sitio web con un reproductor de Flash de sonido elegante y dar a sus visitantes la posibilidad de jugar o dejar de hacer clic en el sonido de encendido / apagado de un jugador en el estilo de Winamp directamente en una página web.

No necesita experiencia en Flash o conocimientos de programación para integrar Flash player de audio en su sitio.

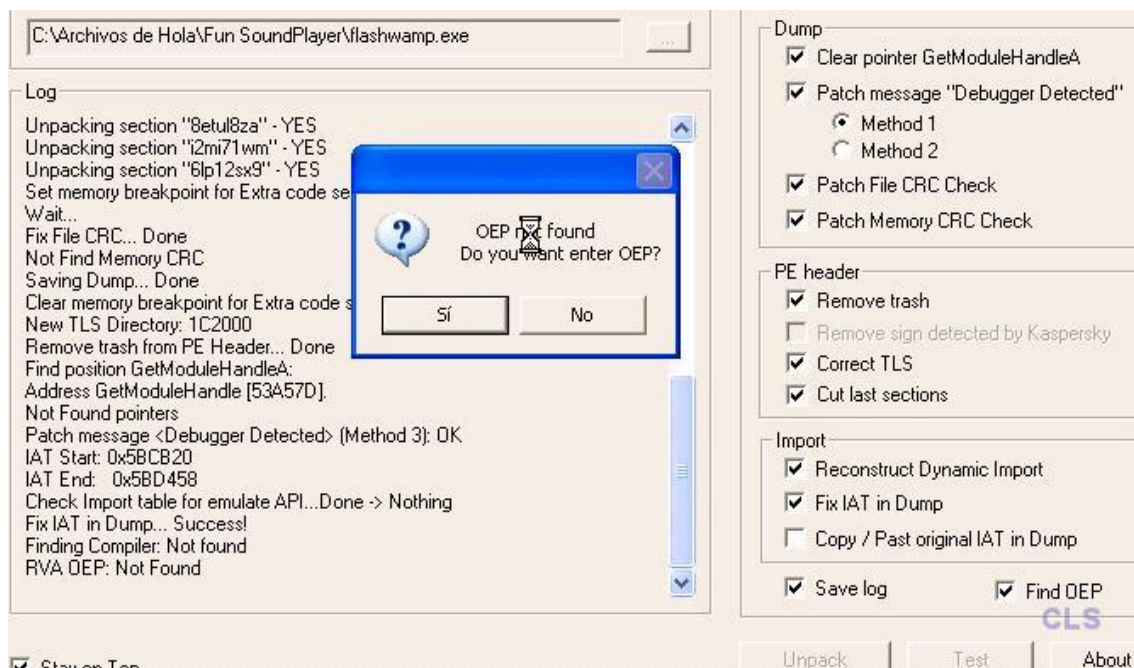
Vamos a Flash WAMP hacer eso por usted.

FlashWamp también contiene SWFObject 2.0 - un pequeño archivo JavaScript que evita que Internet Explorer bloquee las páginas web con el objeto Flash.

Luego de probar el Unpacker de Rsi versión RC1, no encontraba el oep



Y termino con un donde esta el oep..

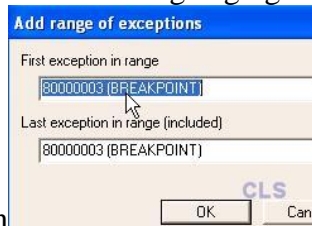




Ejecuto el script



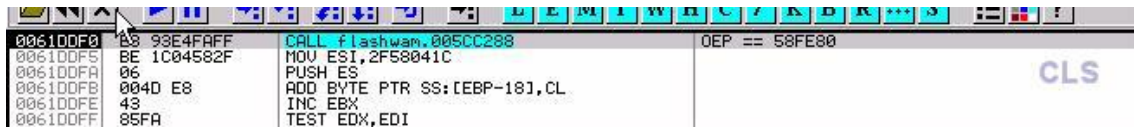
luego agrego algunas excepciones que se me



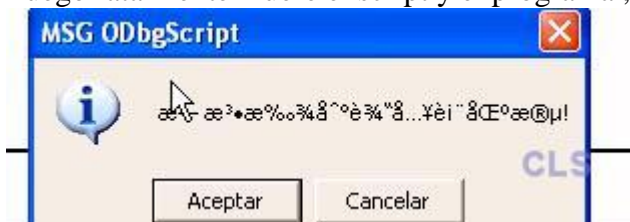
olvidaban

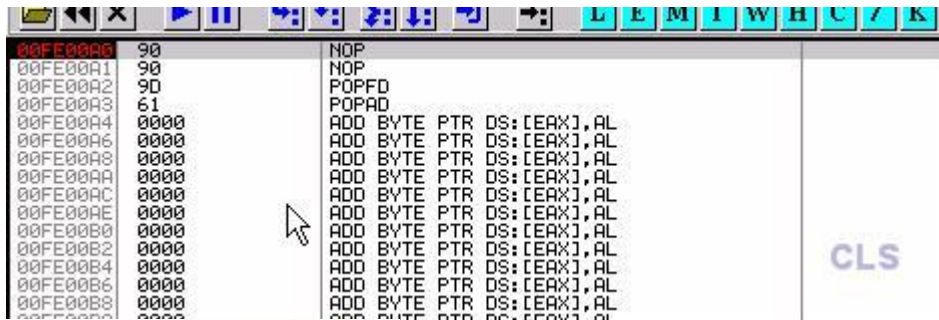


Y me sale el mensaje del oep



Luego fatalmente muere el script y el programa , o sea solo me sirvio de darme el oep





Muere con el mensaje error

Pero bien muerto o no, tengo el oep, sin haber traceado ni 2 minutos

oep = 58FE80>rva 18fe80

\*nota, el oep, puede que no sea el oep real, pues este seria como el oep falso que contenia el execryptor, pero igual me servira para super alterarlo

\*quizas en un proximo escrito saldria un inline ☺

vuelvo al unpacker de RSI release 1 (~~el 2 es privado aun~~)



ingresado el oep, presiono



Y dice



, por lo tanto debemos corregir el crc  
(dicen que la version 2 encuentra este crc)

Según mis apuntes que aprendi

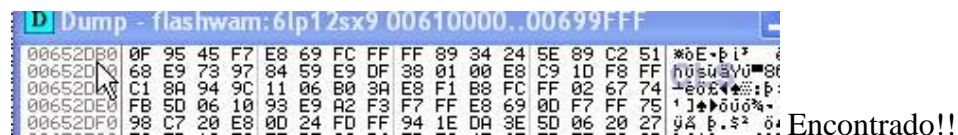
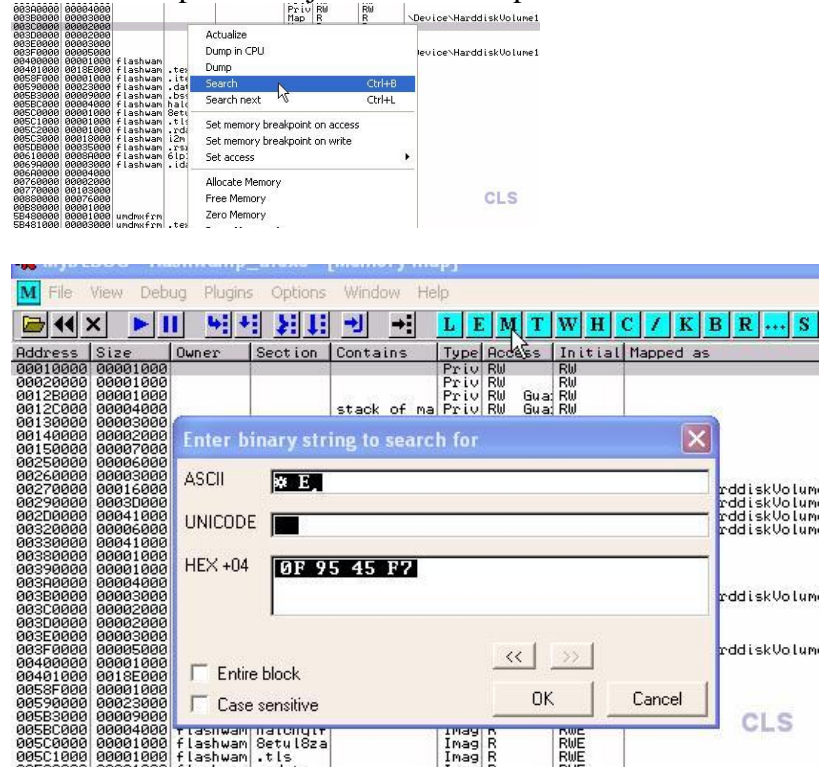
Existen 2 tipos de crc en execryptor

0F 95 45 FB

0F 95 45 F7

Las 2 pueden ser parchadas sin mayor problema

Presiono alt+M o presiono la letra M y coloco binary search ctr+B en una parte levemente superior al ejecutable desempacado



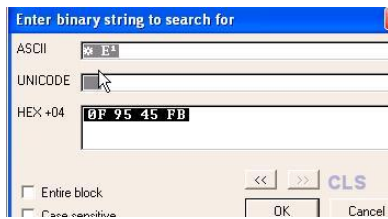
Como se cambia ese CRC?

00652DB0 C645 F7 00 MOV BYTE PTR SS:[EBP-9],0

00652DB4 E8 69FCFFFF CALL flashwam.00652A22  
00652DB9 893424 MOV DWORD PTR SS:[ESP],ESI  
00652DBC 5E POP ESI

Guardo los cambios (save changes) y comienzo para el próximo (osea reinicio, porque el unpacked no acepta save all changes porque esta un poco packed)

Y en este reinicio de olly vamos por el otro chequeo de crc



Encontrandolo esos bytes caracteristicos vencemos esa comparacion



Ahora como se vence?

Cambiandolo para que sea siempre 0

```
00441EDC  C645 FB 00  MOV BYTE PTR SS:[EBP-5],0
00441EE0  |. 807D FB 00  CMP BYTE PTR SS:[EBP-5],0
00441EE4  |. 0F84 2D010000 JE flashwam.00442017
```

Y este escrito y el cracked fue enviado para testing a Rsi :

```
2008/5/9 <rs1@tut.by> <"?????????>:
Hi!

Sorry for my bad english...

I'm testing this program on unpacker version RC2 => unpacked sucessfully ;)

Thanks is bug reports. ))

P.S. If enterest, Unpacker Log attached...
```

Luego de guardados los cambios, ya no molesta el crc  
Por lo tanto, el **programa esta unpacked**



Analizando:

Luego en la ventana, esta unregistred!!

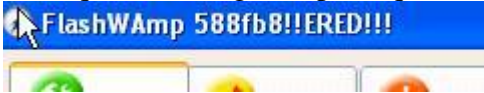


Busco la referencia

Y modifico con un metodo no muy conocido y espero sirva :0

Llamado "con el espacio alcanzo a colocar la direccion"

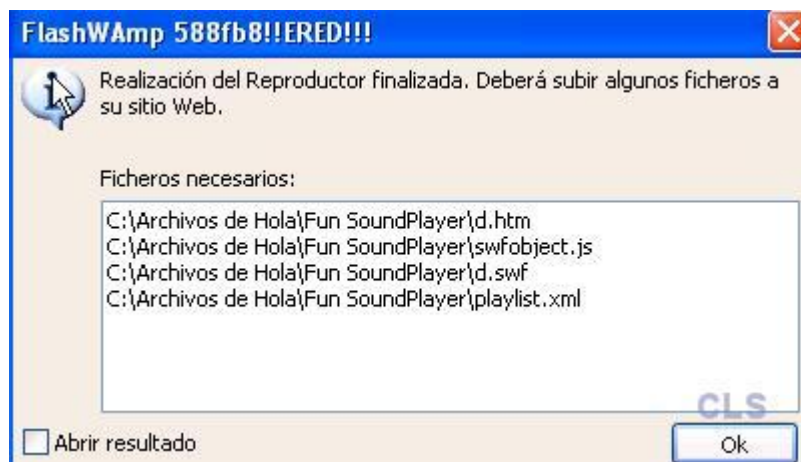
Creo que esta imagen explica que se hizo



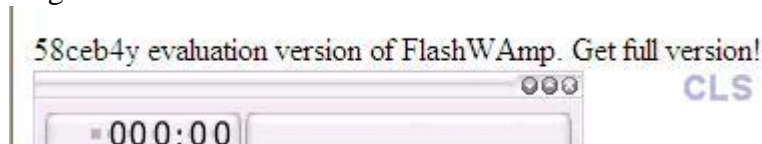
Luego de ello claramente verifico que la referencia era la correcta ☺

\*nota: para quienes no saben que hice, pues busque la referencia, luego altere los datos en binario y queda la direccion de forma que cuando se abra el programa o realice las rutinas, se explore que cosas va a realizar, y sobre todo en que dirección  
Esto es usado solo cuando no sabes cual referencia va a tomar y en que lugar

Explicado el pequeño metodo, queda hacer el trabajo de tantear el terreno

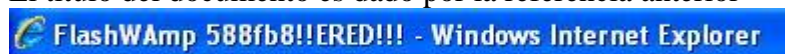


luego



El mensaje de evaluacion del htm esta en 58ceb4

El titulo del documento es dado por la referencia anterior





Y el mensaje dentro de la reproducción esta en 58b000



Muchos cambios que hacer y muy poco tiempo para explicar ni mostrar

Asi que comenzamos la batalla

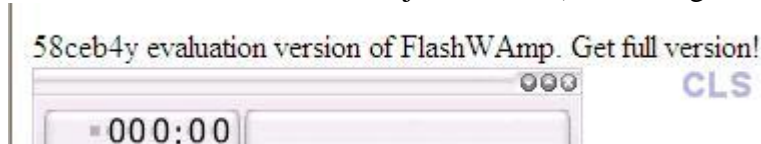


588fb8 le colocamos un 00 para que no indexe ninguna palabra post flashWamp  
00588FB8 00 4C 69 63 65 6E 73 65 .

Quedando claramente mucho mas presentable



el de html lo encuentro con object classid (en el codigo de fuente)



luego de modificado el html en olly no aparecera mas la referencia  
(pensando como poder alterar el mensaje )

```
0058CEAC FF FF FF FF 3E 00 00 00     >...
0058CEB4 3C 62 72 3E 20 20 20 20 <br>
0058CEBC 20 20 20 20 20 20 20 20
0058CEC4 20 20 20 20 20 20 20 20
0058CECC 20 20 20 20 20 20 20 20
0058CED4 20 20 20 20 20 20 20 20
0058CEDC 20 20 20 20 20 20 20 20
0058CEE4 20 20 20 20 20 20 20 20
0058CEEC 20 20 3C 62 72 3E 00 00 <br>..
0058CEF4 FF FF FF FF 9E 01 00 00         ..
0058CEFC 3C 6F 62 6A 65 63 74 20 <object
0058CF04 63 6C 61 73 73 69 classi
```

Obviamente deje los br para guiarme , pero tambien pueden ser 2020 como el anterior  
Luego me enfurezco buscando la nag que aparece sutilmente , asi que no le doy mas guerra y altero algo que no queria tocar



0053A97F	833D D4A35B00 0	CMP DWORD PTR DS:[5BA3D4],0	
0053A986	74 1C	JE SHORT flashwam.0053A9A4	
0053A988	6A 00	PUSH 0	
0053A98A	B9 88A35B00	MOV ECX,flashwam.005BA3B8	
0053A98F	8B15 D4A35B00	MOV EDX,DWORD PTR DS:[5BA3D4]	
0053A995	A1 D0A35B00	MOV EAX,DWORD PTR DS:[5BA3D0]	
0053A99A	E8 B5F8FFFF	CALL flashwam.0053A254	
0053A99F	3C 03	CMP AL,3	
0053A9A1	0F94C3	SETB BL	
0053A9A4	E9 DCE41200	JMP flashwam.00668E85	

En 53A9a1 posee un sete bl, hay que cambiarlo a setne bl

Para quitar la nag

Alguno dira como llegaste a eso?

Pues les comento algo que casi nadie comenta de los execrypteds  
Las referencias de unregistered, que le agrega o las rutinas de donde esta el lugar especial , justo esta ofuscado

Buscando algo tipico, pues llegue por ahi

0053A9EC	FF	DB FF	
0053A9ED	FF	DB FF	
0053A9EE	FF	DB FF	
0053A9EF	FF	DB FF	
0053A9F0	. 15 00000055	ADC EAX,55000000	
0053A9F5	: 4E	DEC ESI	
0053A912	. C3	RETN	
0053A913	. 00	DB 00	
0053A914	. FFFFFFFF	DD FFFFFFFF	
0053A918	. 24000000	DD 00000024	
0053A91C	. 53 4F 46 54 5	ASCII "SOFTWARE\Feather"	
0053A920	. 79 53 6F 66 7	ASCII "ySoft\FunSoundPl"	
0053A93C	. 61 79 65 72 0	ASCII "ayer",0	
0053A941	. 00	DB 00	
0053A942	. 00	DB 00	
0053A943	. 00	DB 00	
0053A944	. 90	NOP	
0053A945	. 90	NOP	
0053A946	. 90	NOP	
0053A947	. 90	NOP	
0053A948	. 90	NOP	
0053A949	. 90	NOP	
0053A94A	. 90	NOP	
0053A94B	. 90	NOP	
0053A94C	. 55 4E 52 45 4	ASCII "UNREGISTERED VER"	
0053A95C	. 53 49 4F 4E 2	ASCII "SION!",0	
0053A962	. 00	DB 00	
0053A963	. 00	DB 00	
0053A964	. \$ 55	PUSH EBP	
0053A965	. 8BEC	MOV EBP,ESP	
0053A967	. 53	PUSH EBX	
0053A968	. 33C0	XOR EAX,EAX	
0053A96A	. 55	PUSH EBP	

Y claramente al analizar hubiese sido mucho mas facil ver lo que muestra

0053A941	. 00	DB 00	
0053A942	. 00	DB 00	
0053A943	. 00	DB 00	
0053A944	. 90	NOP	
0053A945	. 90	NOP	
0053A946	. 90	NOP	
0053A947	. 90	NOP	
0053A948	. 90	NOP	
0053A949	. 90	NOP	
0053A94A	. 90	NOP	
0053A94B	. 90	NOP	
0053A94C	. 55 4E 52 45 4	ASCII "UNREGISTERED VER"	
0053A95C	. 53 49 4F 4E 2	ASCII "SION!",0	
0053A962	. 00	DB 00	
0053A963	. 00	DB 00	
0053A964	. \$ 55	PUSH EBP	
0053A965	. 8BEC	MOV EBP,ESP	
0053A967	. 53	PUSH EBX	
0053A968	. 33C0	XOR EAX,EAX	
0053A96A	. 55	PUSH EBP	

Si analizo la rutina  
Luego

00589DF8	. 8B F8	Mov EDI, EHX	
00589DFD	. B2 07	Mov DL, 7	
00589DFE	. 8B C7	Mov EAX, EDI	
00589E01	. E8 CE32F5FF	CALL 3.00400004	
00589E06	. 807D A3 00	CMP BYTE PTR SS:[EBP-5D], 0	
00589E09	. 0F84 7F020000	JE 3.0058A08F	
00589E10	. E8 4F0BF8FF	CALL 3.0058A964	
00589E13	. 84 C0	TEST AL, AL	salto unregistered version
00589E17	. 74 0E	JE SHORT 3.00589E27	
00589E19	. A1 88295B00	Mov EAX, DWORD PTR DS:[5B2988]	
00589E1E	. 3338 00	CMP DWORD PTR DS:[EAX], 0	
00589E21	. 0F85 68020000	JNZ 3.0058A08F	
00589E27	. E8 C896E7FF	CALL 3.004034F4	
00589E2C	. B8 0F270000	Mov EAX, 270F	
00589E31	. E8 E696E7FF	CALL 3.0040351C	
00589E36	. 8D95 74FFFFFF	LEA EDX, DWORD PTR SS:[EBP-8C]	
00589E3C	. E8 6B13E8FF	CALL 3.0040B1AC	
00589E41	. 8B95 74FFFFFF	Mov EDX, DWORD PTR SS:[EBP-8C]	
00589E47	. 8B C7	Mov EAX, EDI	
00589E49	. E8 4EDAFFFF	CALL 3.0058789C	
00589E4E	. 66:C747 64 10	Mov WORD PTR DS:[EDI+64], 2710	
00589E54	. A1 44295B00	Mov EAX, DWORD PTR DS:[5B2944]	
00589E59	. 8B 00	Mov EAX, DWORD PTR DS:[EAX]	
00589E5B	. B2 D0	Mov DL, 00	
00589E5D	. E8 7ABDEFFF	CALL 3.00485BDC	
00589E62	. 50	PUSH EAX	
00589E63	. 68 13010000	PUSH 113	Arg2 = 00000113
00589E68	. 6A 12	PUSH 12	Arg1 = 00000012
00589E6A	. 33C9	XOR ECX, ECX	
00589E6C	. 33D2	XOR EDX, EDX	
00589E6E	. 8B C7	Mov EAX, EDI	
00589E70	. E8 13A8FFFF	CALL 3.00584688	3.00584688
00589E75	. 5A	POP EDX	
00589E76	. E8 998BFEFF	CALL 3.00572A14	
00589E7B	. 8B45 AC	Mov EAX, DWORD PTR SS:[EBP-54]	
00589E7E	. 8B50 68	Mov EDX, DWORD PTR DS:[EAX+68]	
00589E81	. 33C9	XOR ECX, ECX	
00589E83	. 8B C7	Mov EAX, EDI	
00589E85	. E8 7EA5FFFF	CALL 3.00584408	
00589E8A	. 50	PUSH EAX	
00589E8B	. 8D8D 6CFFFFFF	LEA ECX, DWORD PTR SS:[EBP-94]	
00589E91	. 33D2	XOR EDX, EDX	
00589E93	. 33C0	XOR EAX, EAX	
00589E95	. E8 E629E9FF	CALL 3.0041C800	
00589E9A	. 8D85 6CFFFFFF	LEA EAX, DWORD PTR SS:[EBP-94]	
00589EA0	. 50	PUSH EAX	
00589EA1	. 6A 00	PUSH 0	
00589EA3	. 68 FF000000	PUSH 0FF	Arg1 = 000000FF
00589EA8	. B1 FF	Mov CL, 0FF	
00589EAA	. B2 33	Mov DL, 33	
00589EAC	. B0 33	Mov AL, 33	
00589EAE	. E8 B1BCEFFF	CALL 3.00485B64	3.00485B64
00589EB3	. 8B C8	Mov ECX, EAX	
00589EB5	. BA 00B05B00	Mov EDX, 3.0058B000	
00589EB8	. 8B C7	Mov EAX, EDI	
00589EBC	. E8 FFA9FFFF	CALL 3.005848C0	
00589EC1	. 33D2	XOR EDX, EDX	ASCII "Made by evaluation version of FL: 0.6

Si vemos hay unos saltos, abajo se ve el made by evaluation (el de la referencia de 58b000)

Hay una comparación y los saltos al parecer deben saltar a otra cosa

Como se que el primero al cambiarle el bl saca la nag, el segundo pues se encargara del mensaje y el alterado no habra nag ni mensaje

Por eso cambio el segundo, para no dejarlo tan facil

Que facil salio? al made by evaluation (solo estoy probando si resulta)



Y claramente resulta

```

00589E01 . E8 CE32F5FF CALL 3.0040D004
00589E06 . 807D A3 00 CMP BYTE PTR SS:[EBP-5D],0
00589E0B . 0F84 7F020000 JE 3.0058A08F
00589E10 . E8 4F08FBFF CALL 3.0053A964
00589E15 . 84C0 TEST AL,AL
00589E17 . 74 0E JE SHORT 3.00589E27
00589E19 . A1 88295B00 MOV EAX,DWORD PTR DS:[5B2988]
00589E1E . 8338 00 CMP DWORD PTR DS:[EAX],0
00589E21 . E9 69020000 JMP 3.0058A08F
00589E26 . 90 NOP
00589E27 . E8 C896E7FF CALL 3.004034F4
00589E2C . B8 0F270000 MOV EAX,270F
00589E31 . E8 E696E7FF CALL 3.00403510
00589E36 . 8D95 74FFFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00589E3B . 8B 2A 000000 MOV EBX,DWORD PTR DS:[EBP-2A]

```

589e21

Solo faltaria un repaso para ver si falta algo

Luego de alterar ese mensaje titulo588FB8 a 00

No hay escrito en el flash 00589E21 jmp

No hay escrito unregistred

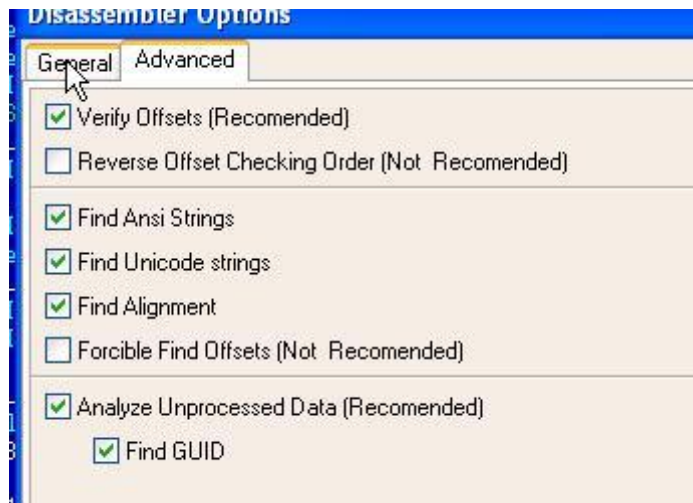
Falta reconocer el escrito rojo, quien use IDA , fácilmente lo encontrará

Pero prefiero en este caso mostrar algo similar, y que quizás sea útil para quienes no saben encontrar referencias en los ofuscados por execryptor

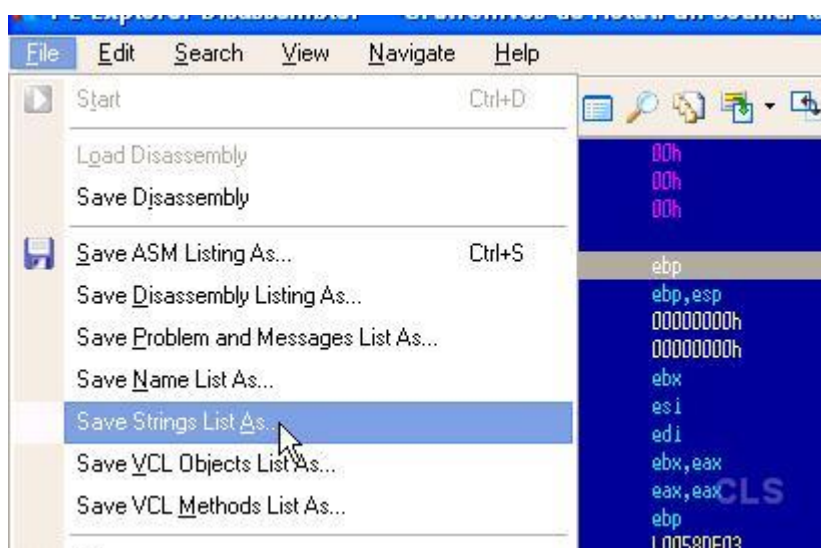
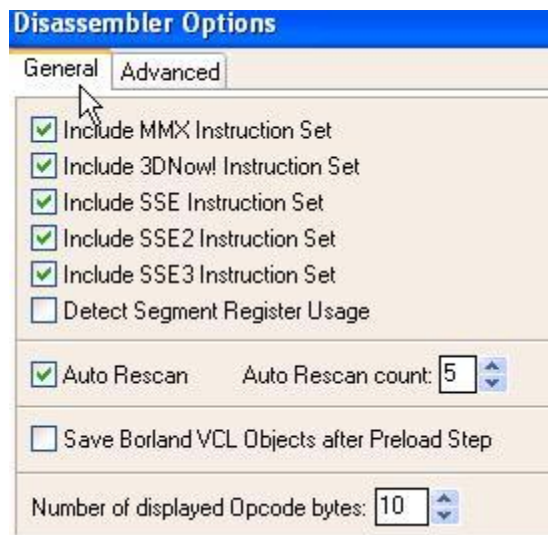
Antes no lo usaba, hoy en día lo uso pero hasta por ahí no mas



Uso el dissasemble de pexplorer







```

0053967C: \
005396A0: 'FileVersion'
0053A91C: 'SOFTWARE\FeatherySoft\FunSoundPlayer'
0053A94C: 'UNREGISTERED VERSION!'
0053A9F4: 'UNREGISTERED VERSION!'
0053D45C: 'OLE control activation failed'
0053D710: 'Could not obtain OLE control window har

00588F90: 'English'
00588FA0: 'WAPlayerView'
00588FCC: 'You are using the unregistered version of the program!',0Dh,'Please register it!',0
00589020: 'LicenseTo'
00589034: 0Dh
00589280: 'SOFTWARE\FeatherySoft\FunSoundPlayer'

```

Y claramente tiene todas las referencias que teníamos anteriormente en olly

Pero queda un detalle

Estando mas o menos aquí

Teniamos el mensaje del unregistred

(no mostre foto en vista previa, pero )  
Normalmente se ve algo asi



UNREGISTRED en rojo

Observen bien, porque alterando el 58b314 a 00FF

55B826C0	•	FFFFFFFF	DD	FFFFFFFF	
55B826C0	•	67000000	DD	00000067	
55B82700	•	40 61 64 65 21	ASCII	"Made by  Flash"	
55B82800	•	57 41 60 70 31	ASCII	"Wamp ca h"	
55B82900	•	72 65 66 30 21	ASCII	"ref=http://flas"	
55B82A00	•	68 77 61 60 71	ASCII	"wamp.com" targ"	
55B82B00	•	74 30 22 5F 61	ASCII	"=blank"><u>w"	
55B82C00	•	77 28 46 5C 61	ASCII	"FlashWamp.com<"	
55B82D00	•	2F 75 3E 3C 21	ASCII	"u</>"/>0	
55B82D08	•	0000	ADD BYTE PTR DS:[EAX],AL		
55B82DA0	•	0000	ADD BYTE PTR DS:[EAX],AL		
55B82DC0	•	0000	ADD BYTE PTR DS:[EAX],AL		
55B82DE0	•	00	DB 00		
55B82DF0	•	00	DB 00		
55B82E00	•	3C 62 72 3E 31	ASCII	" <font color="	
55B82F00	•	22 23 46 46 31	ASCII	"#FF0000">58b2FA"	
55B83000	•	53 54 45 52 41	ASCII	"STERED!!!!<font>"	
55B83100	•	00	DB 00		
55B83110	•	00	DB 00		
55B83120	•	00	DB 00		
55B83130	•	00	DB 00		
55B83140	•	59 6F 75 20 61	ASCII	"You are using th"	
55B83240	•	65 20 75 6E 71	ASCII	"e unregistered v"	
55B83340	•	65 72 73 69 61	ASCII	"ersion of the pr"	
55B83440	•	6F 67 72 61 61	ASCII	"ogram!Please re"	
55B83540	•	67 69 73 74 61	ASCII	"gister it"/>0	
55B835F0	•	00	DB 00		
55B83600	•	FFFFFFFF	DD	FFFFFFFF	
55B83640	•	80000000	DD	00000080	
55B83680	•	41 62 6F 75 71	ASCII	"AboutStr"/>0	
55B83710	•	00	DB 00		
55B83720	•	00	DB 00		
55B83730	•	00	DB 00		

Queda como



o sea echamos a perder el mensaje

0058B2E0	00FF	ADD BH, BH
0058B2F2	90	NOP

## Pero si hacemos otra historia

## Como analizar

Veamos el primer mensaje, dice made by..etc

	. FFFFFFFF	DD FFFFFFFF
-4	: 67000000	DD 00000067
+0	: 4D 61 64 65 20 62 79 20 3C 62 3E	ASCII "Made by <b>Flash"
+10	: 57 41 6D 70 3C 2F 62 3E 3C 62 72	ASCII "&lt;/> <a "
+20	: 72 65 66 3D 2C 22 68 74 7A 70 3A 2F	ASCII "ref=http://flas
+30	: 68 77 61 6D 70 2E 63 6F 6D 22 20	ASCII "hw&amp;.com" targ
+40	: 74 3D 22 5F 62 6C 61 6E 68 22 3E	ASCII "t= blank"><u>ww
+50	: 77 2E 46 6C 61 73 68 57 41 6D 70	ASCII "w.Flash&amp;.com<
+60	: 2F 75 3E 3C 2F 61 3E 00	ASCII "/u></a>",0
+68	FF	DB FF
+69	FF	DB FF
+6A	FF	DB FF
+6B	FF	DB FF

Arriba dice 67

Y claramente donde cuento tengo 67 remarcado

00000000	. FFFFFFFF	DD FFFFFFFF
00000001	. 67000000	DD 00000067
00000002	. 4D 61 64 65 20 62 79 20 3C 62 3E	ASCII "Made by <b>Flash"
00000003	. 57 41 6D 70 3C 2F 62 3E 3C 62 72	ASCII "Wamp</b> <a h"
00000004	. 72 65 66 3D 22 68 74 74 70 3A 2F	ASCII "ref="http://flas"
00000005	. 68 77 61 6D 70 2E 63 6F 6D 22 20	ASCII "hwamp.com" targe"
00000006	. 74 3D 22 5F 62 6C 61 6E 68 22 3E	ASCII "t="blank"><u>ww"
00000007	. 77 2E 46 6C 61 73 68 57 41 6D 70	ASCII "w.FlashWamp.com<"
00000008	. 2F 75 3E 3C 2F 61 3E 00	ASCII "</u></a>",<0
00000009	. FF	DB FF

Ahora bien, mas abajo en el de unregistered dice 30

00000000	. 30	DB 30
00000001	. 00	DB 00

Y ahora bien como se entiende la idea (que esos 30 bytes es de la palabra unregistered)

Pues me despido de ese mensaje

Modificandolo a 0

0058B208	. FF
0058B209	. 0000
0058B20A	. 00
0058B20B	. 00
0058B20C	. 00FF



Ahora bien, antes habiamos alterado uno similar . solo con nops

0058CEAB	. 00	DB 00
0058CEAC	. FFFFFFFF	DD FFFFFFFF
0058CEAD	. 3E000000	DD 0000003E
0058CEAE	. 4D 61 64 65 20	ASCII "Made by evaluati"
0058CEAF	. 6F 6E 20 76 61	ASCII "on version of Fl"
0058CEB0	. 61 73 68 57 4	ASCII "ashWamp. Get ful"
0058CEB1	. 6C 20 76 65 7	ASCII "l version! ",<0
0058CEB2	. 00	DB 00
0058CEB3	. 00	DB 00

Ahora como estamos claramente modificando esos mensajes

Podemos hacerlo elegantemente

0058CEAB	. FFFFFFFF	DD FFFFFFFF
0058CEAC	. 3E000000	DD 0000003E
0058CEAD	. 4D 61 64 65 20	ASCII "Made by evaluati"
0058CEAE	. 6F 6E 20 76 61	ASCII "on version of Fl"
0058CEAF	. 61 73 68 57 4	ASCII "ashWamp. Get ful"
0058CEB0	. 6C 20 76 65 7	ASCII "l version! ",<0
0058CEB1	. 00	DB 00
0058CEB2	. FFFFFFFF	DD FFFFFFFF
0058CEB3	. 00000000	DD 00000000

58cEb0 -> alterando a 3E a 0

0058CEAC	. FFFFFFFF	DD FFFFFFFF
0058CEAD	. 0000	ADD BYTE PTR DS:[EAX],AL
0058CEAE	. 0000	ADD BYTE PTR DS:[EAX],AL
0058CEAF	. 4D 61 64 65 20	ASCII "Made by evaluati"
0058CEB0	. 6F 6E 20 76 61	ASCII "on version of Fl"
0058CEB1	. 61 73 68 57 4	ASCII "ashWamp. Get ful"
0058CEB2	. 6C 20 76 65 7	ASCII "l version! ",<0
0058CEB3	. 00	DB 00

Teniendo listo el mensaje que mostrara en el html

Ahora listo ese problema

Vamos al proximo

recordemos que aparece un mensaje en la parte superior , con la mismo metodo alterandolo a 0 queda como en pantalla

00588FB4	. 00	DB 00
00588FB5	. 00	DB 00
00588FB6	. 00	DB 00
00588FB7	. 00	DB 00
00588FB8	. 00	DB 00
00588FB9	. 35 38 38 66 6	ASCII "588fb8!ERED!!",0
00588FBA	. 00	DB 00
00588FBB	. 00	DB 00



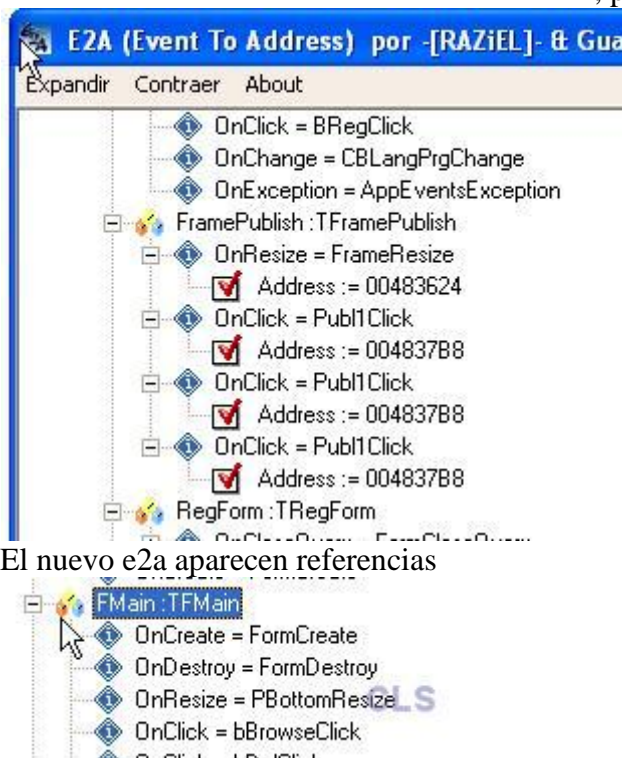
Tendriamos todo mas o menos listo  
Veo en ejecución si es delphi



El unpacked



, pero el script no contiene nada ☺



El nuevo e2a aparecen referencias

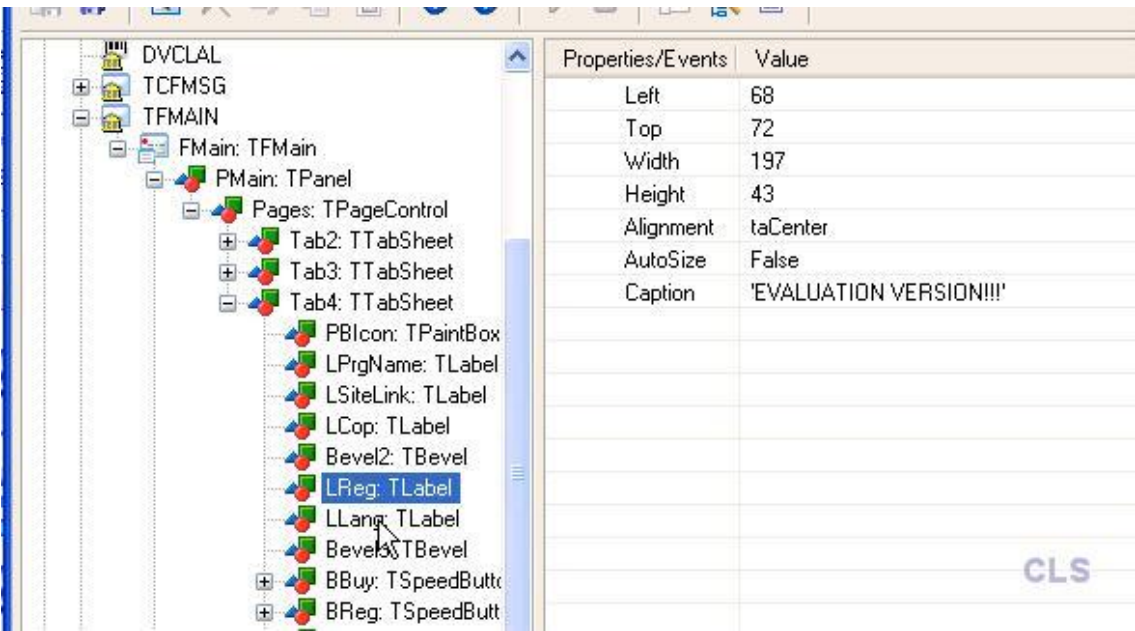
Pero al main nada(solo algunos toma y otros no..Eso pasa a los execrypteds)

Destruye demasiado el ejecutable haciendo pensar que no es delphi.

Bien queda lo ultimo a modificar



EN4BLER DE AT4RE DICE QUE ES PARTE DE INFO

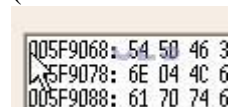


PEXPLOER LO ENCUENTRO EN MAIN  
(PERO POR ESTAR UNPACKED Y SIN RESTAURAR, DEJARA LA ESCOBA  
ASI QUE SOLO CON MAIN, ME QUEDO Y DE AHÍ LO BUSCO

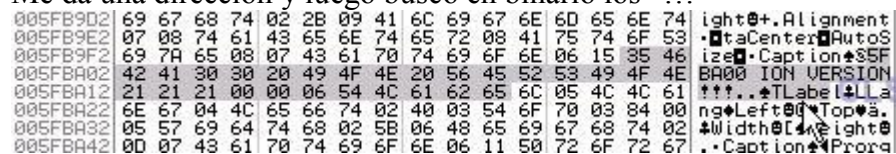
Luego de encontrado uso el



(TAMBIEN SERVIAN LAS REFERENCIAS, PERO ASI ES MAS BONITO

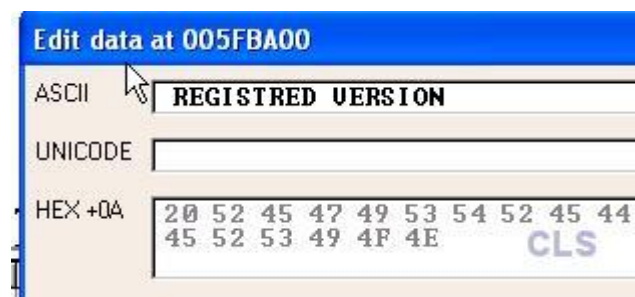


Me da una direccion y luego busco en binario los “!!!”



Y con el metodo comprobado

Puede cambiarse a



Pero como no queremos dejarlo así



Coloco VERSION APUROMAFO



FlashWamp (1.1.0.0)

www.FlashWamp.com

Copyright (c) 2005-2008 FeatherySoft

VERSION APUROMAFO !!!

Y LOS BOTONES, pues pueden dejar para cancelar el programa y aportar a este programa que me ha dado un momento de practicar ☺ y conocer un poquito mas de execryptor+delphi

### Conclusiones

Quien pilla las referencias encuentra todo

Pero con esto que escribo solo muestro un 10% de el total que he descubierto

\*sobre todo los bytes ofuscados que ayudan en gran parte a encontrar las referencias para poder registrarlo (aun no lo demuestro en todo, por eso dejare hasta aquí)

Pero no es todo eso

Guardo los cambios y se me ocurre instalar el otro programa de la web

[http://www.funsoundplayer.com/download/sp\\_setup.exe](http://www.funsoundplayer.com/download/sp_setup.exe)

y aparece



Ups aun me queda un detalle, ya lo borraremos después, me concentrare en el nuevo

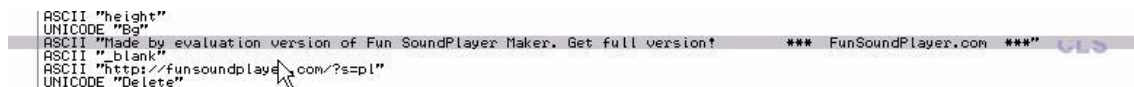
Lo abro y sale **Wa REGISTRED???**



Pero voy al nuevo instalado y dice license to : ssss  
Mas de alguno dira, y como lo hiciste apuromafo  
recuerdo haber hecho algo

Desempaco (no mostrare)

Pero realmente no es que venga registrado, pues tiene todo lo anterior para que sea trial

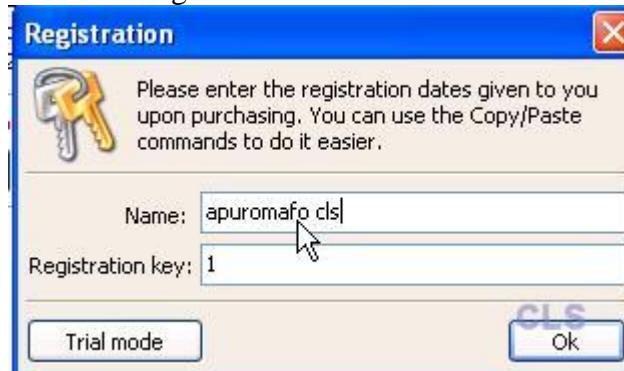


Claramente existe la evaluation version de fun sound player maker

Pero

Como anexo en mi fun sound player

Coloco en registrar



Al pulsar ok, me aparece bien y desaparece esa ventana



pero el programa sigue trial (eso creia)

Y ahora voy al otro programa luego del ok que fue aceptado

Y vemos que el maker, que posee mas características que el que estaba registrando aparece



Chachan ;) toma el registro del otro  
Saludos Apuromafo

Pd: este fun sound player maker, tambien esta packed con execryptor  
Pero no puedo dejar que les diga la nag que estan usando la version no registrada

Porque o no estaria full cracked

0064C56C	890424	MOV DWORD PTR SS:[ESP],EAX
0064C56F	68 CC8F5800	PUSH 1.00588FCC
0064C571	87C3	XCHG EBX,EAX
0064C576	8BD8	MOV EBX,EAX
0064C578	E8 E3CDE1FF	CALL 1.00469360
0064C57D	68 CF411DB9	PUSH B91D41CF
0064C582	890424	MOV DWORD PTR SS:[ESP],EAX
0064C585	9C	PUSHFD

La nag aparecia con esta direccion

Encontrarla no fue tan difícil

(busque el push 588fcc)

Se puede cambiar a otro mensaje o sea aparecera la nag con otro mensaje

0064C56C	890424	MOV DWORD PTR SS:[ESP],EAX	
0064C56F	68 2A905800	PUSH nop_call.00589020	ASCII "LicenseTo"
0064C574	87C3	XCHG EBX,EAX	
0064C576	8BD8	MOV EBX,EAX	
0064C578	90	NOP	
0064C579	90	NOP	

Luego dije, noo, mejor que no aparezca el mensaje



Anule el call nopeandolo

0064C578	90	NOP
0064C579	90	NOP
0064C57A	90	NOP
0064C57B	90	NOP
0064C57C	90	NOP
0064C57D	68 CF411DB9	PUSH_B91D41CF

Con esto estaria full cracked y nada de nag tal como un registred

Y por ultimo recordemos que este exe registraria el otro programa de forma extraña ☺

Saludos Cordiales Apuromafo

Luego de esto logramos 1 cracked 1 registred sin crackear ni tocar un byte

Creo que servirá para alguno, que investigue mas del tema o simplemente se sorprenda de execryptor que nos regale un programa mas

Que mas queremos , estan full los 2 ☺

Ahora adiós al programa

### **CONCLUSION**

descargaR este programa

[http://www.funsoundplayer.com/download/fwa\\_setup.exe](http://www.funsoundplayer.com/download/fwa_setup.exe)

y en registrar coloca

nombre:apuromafo CLS

contraseña:1

luego de aceptarlo ve y descarga este

[http://www.funsoundplayer.com/download/sp\\_setup.exe](http://www.funsoundplayer.com/download/sp_setup.exe)

luego al iniciar deberia (en mi casa ocurre eso)

iniciar registrado a "apuromafo CLS"

saludos

Apuromafo

SALUDOS apuromafo

\*ahora bien pueden borrar el programa para que no le hagan problema al autor ☺

Por algo sirve el nuevo ☺

Jiji saludos a toda la Lista de Cracklatinos