funsoundplayer

By Apuromafo

Un mini tute, una app con EC(execryptor)

casa

Escrito por: Apuromafo

DESCARGO LEGAL

DOCUMENTO ESCRiTO PARA FiNES DE *EDUCACiON/iNVESTiGACION*

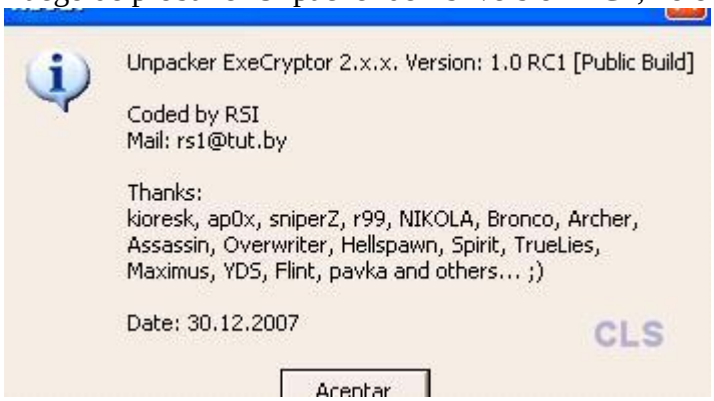
Fecha: 28/06/08
Revisión: 17/6/11

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
luego analizando mas tenemos esto:

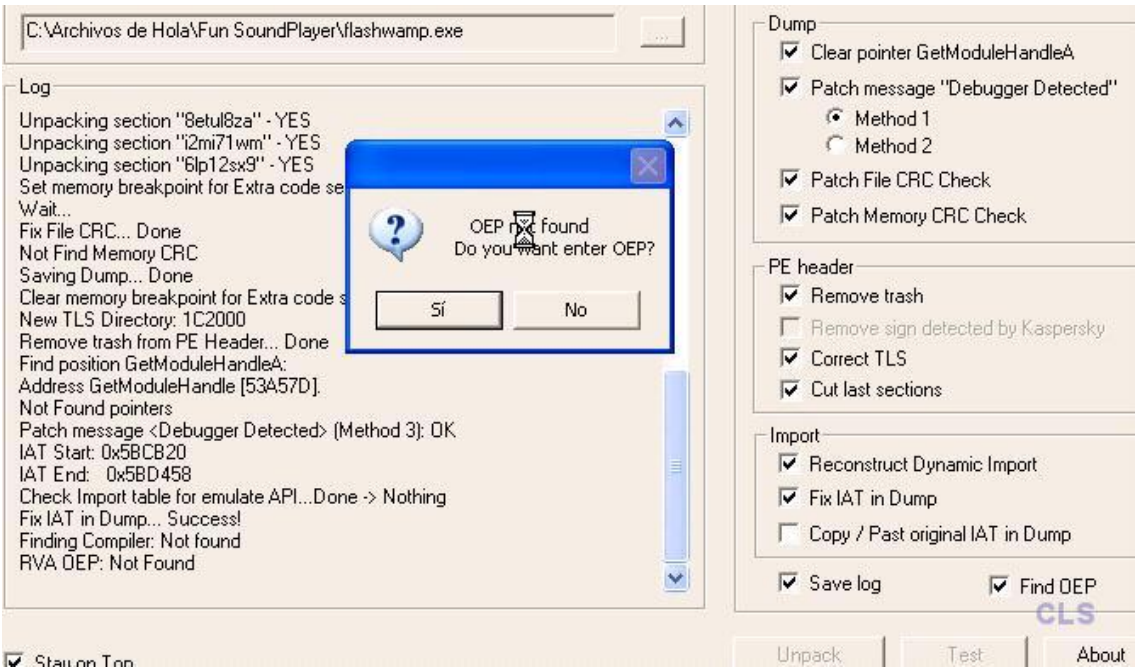
Flash WAMP transforma cualquier piel original de Winamp para Flash basado en el reproductor de música de Internet. Dan vida a su sitio web con un reproductor de Flash de sonido elegante y dar a sus visitantes la posibilidad de jugar o dejar de hacer clic en el sonido de encendido / apagado de un jugador 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 bloquea las páginas web con el objeto Flash.
Luego de probar el Unpacker de Rsi versión RC1, no encontraba el oep

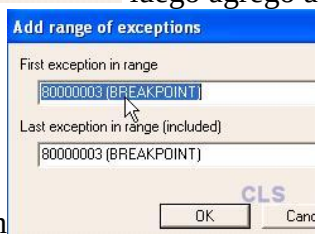


Y termino con un donde esta el oep..



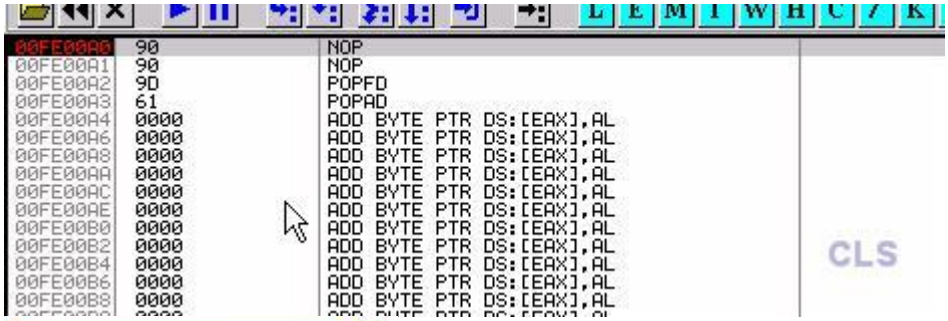
Ejecuto el script

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

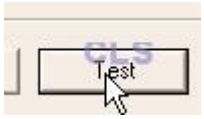


Muere con el mensaje error

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

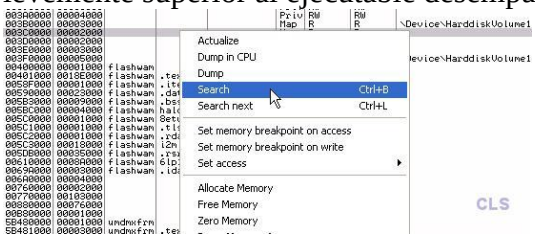


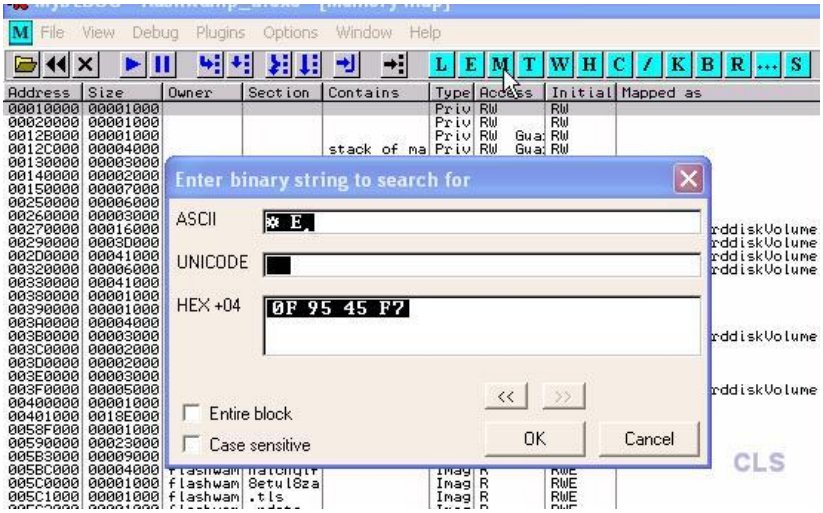
Y dice

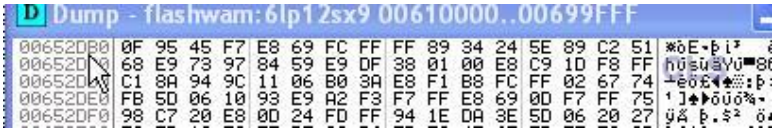
, por lo tanto debemos corregir el crc
(dicen que la version 2 encuentra este crc)

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







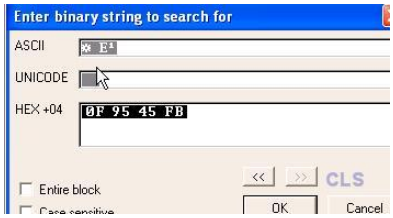
Encontrado!!

Como se cambia ese CRC?

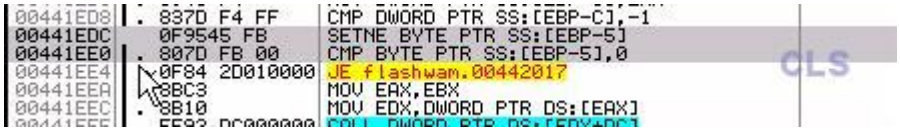
00652DB0 C645 F7 00 MOV BYTE PTR SS:[EBP-9],0

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> <"?????????>:

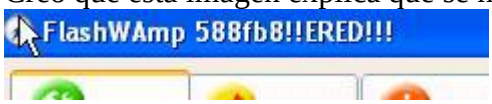
> Hi!
>
> Sorry for my bad english...
>
> I'm testing this program on unpacker version RC2 => unpacked sucessfully ;)
>
> Thanks is bug reports.))
>
> P.S. If enterest, Unpacker Log attached...

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

Analizando:

Luego en la ventana, esta unregistred!!

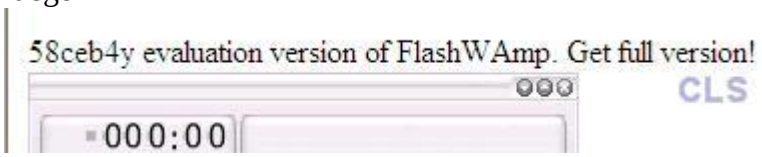
Busco la referencia
Y modifico con un metodo no muy conocido y espero sirva :0
Llamado “con el espacio alcanzo a colocar la direccion”
Creo que esta imagen explica que se hizo



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

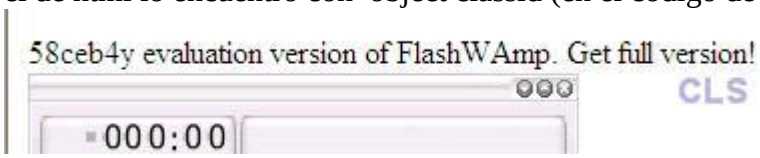
Muchos cambios que hacer y muy poco tiempo para explicar ni mostrar

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 ÿÿÿÿ>...
0058CEB4 3C 62 72 3E 20 20 20 20
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
..
0058CEF4 FF FF FF FF 9E 01 00 00 ÿÿÿÿž□ ..
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

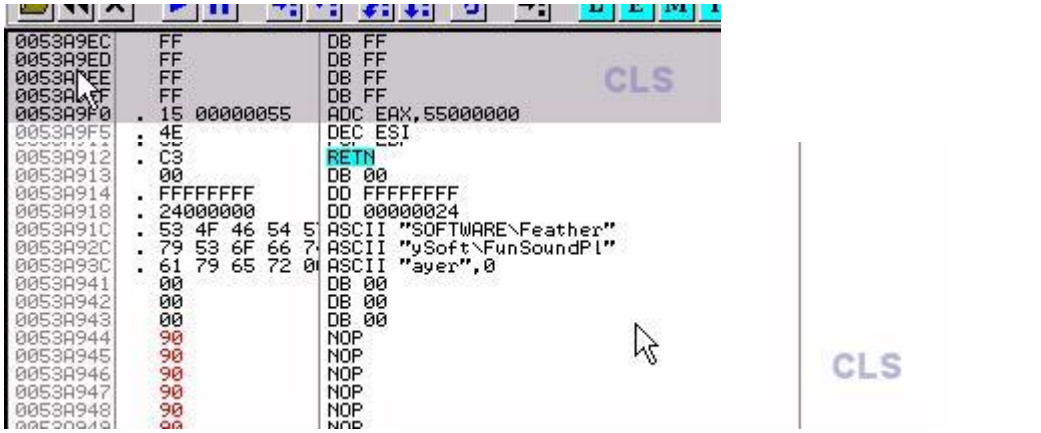
En 53A9a1 posee un sete bl, hay que cambiarlo a setne bl

Para quitar la nag

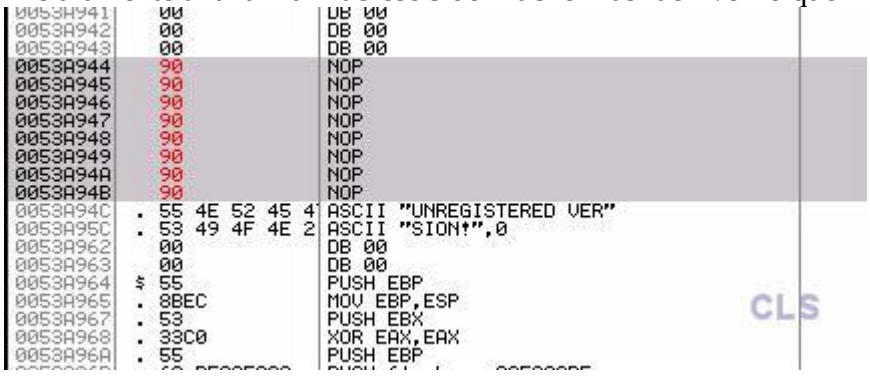
Alguno dira como llegaste a eso?

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

Buscando algo tipico, pues llegue por ahi



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

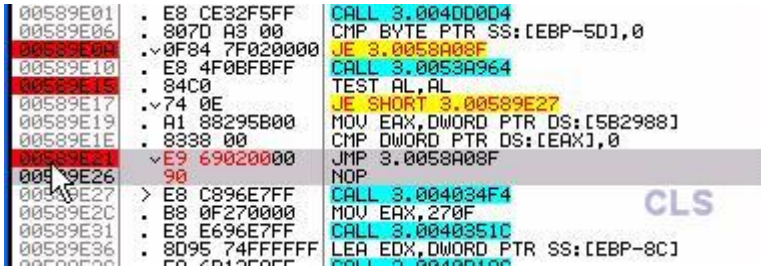


Si analizo la rutina
Luego

```
00589DFB  . 8BF8          MOV EDI,EAX
00589DFD  . B2 07         MOV DL,7
00589DFF  . 8BC7          MOV EAX,EDI
00589E01  . E8 CE32F5FF   CALL 3.004DD0D4
00589E06  . 807D A3 00    CMP BYTE PTR SS:[EBP-5D],0
00589E0A  .v0F84 7F020000 JE 3.0058A08F
00589E10  . E8 4F0BFBFF   CALL 3.0053A964                  salto unregistred version
00589E15  . 84C0          TEST AL,AL
00589E17  .v74 0E         JE SHORT 3.00589E27
00589E19  . A1 88295B00   MOV EAX,DWORD PTR DS:[5B2988]
00589E1E  . 8338 00       CMP DWORD PTR DS:[EAX],0
00589E21  .v0F85 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  . 8BC7          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  . 8B00          MOV EAX,DWORD PTR DS:[EAX]
00589E5B  . B2 D0         MOV DL,0D0
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  . 8BC7          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  . 8BC7          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 3.0041C880
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  . 8BC8          MOV ECX,EAX
00589EB5  . BA 00B05800   MOV EDX,3.0058B000               ASCII "Made by evaluation version of Fl
00589EBA  . 8BC7          MOV EAX,EDI
00589EBC  . E8 FFA9FFFF   CALL 3.005848C0
00589EC1  . 33D2          XOR EDX,EDX
```

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



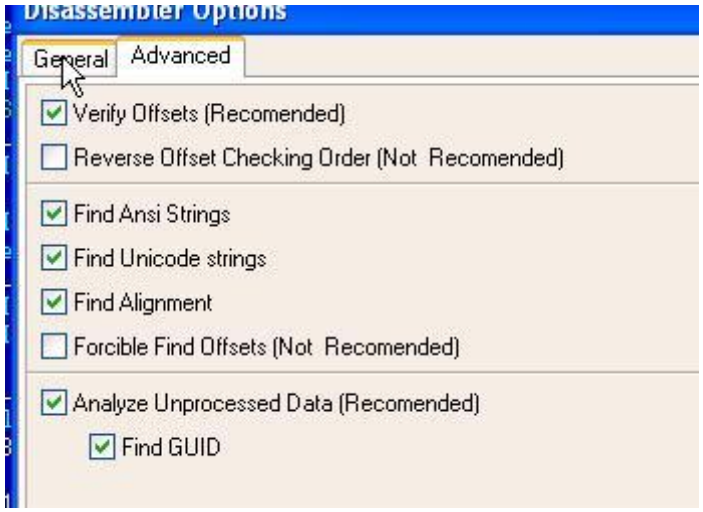
589e21
Solo faltaria un repaso para ver si falta algo

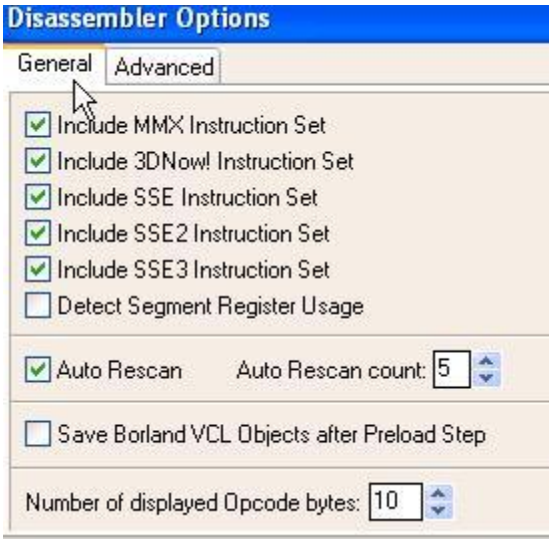
Luego de alterar ese mensaje titulo588FB8 a 00
No hay escrito en el flash 00589E21 jmp

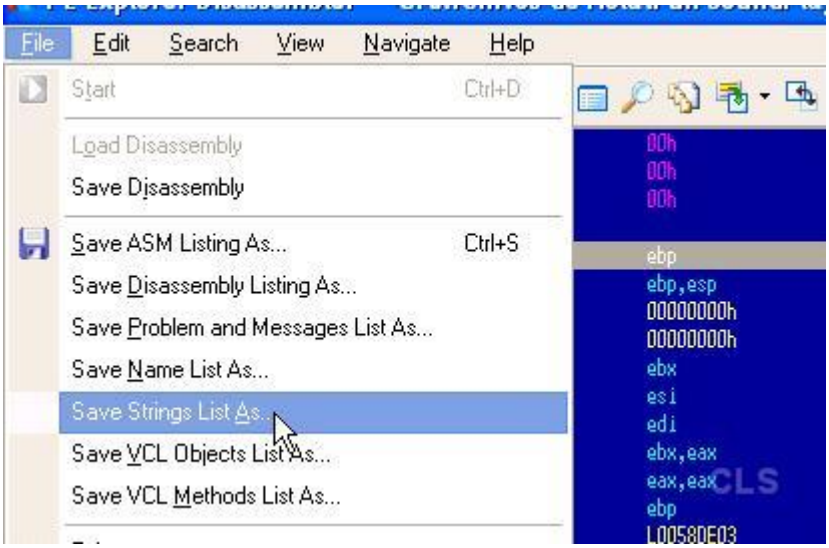
No hay escrito unregistred
Falta reconocer el escrito rojo, quien use IDA , fácilmente lo encontrará
Pero prefiero en este caso mostrar algo similar, y que quizas sea util para quienes no saben encontrar referencias en los ofuscados por execryptor

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

Uso el dissasemble de pexplorer







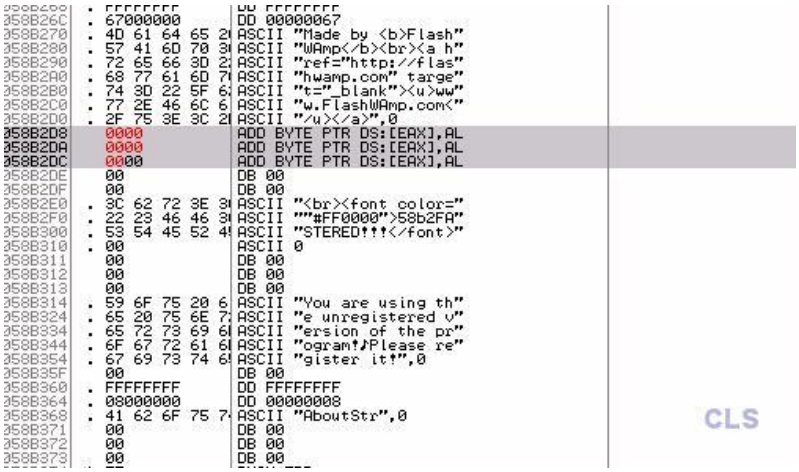

```
005396A0: 'FileVersion'
0053A91C: 'SOFTWARE\FeatherySoft\FunSoundPlayer'
0053A94C: 'UNREGISTERED VERSION!'
0053A9F4: 'UNREGISTERED VERSION!'
0053D45C: 'OLE control activation failed'
0053D710: 'Could not obtain OLE control window har
```

```
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

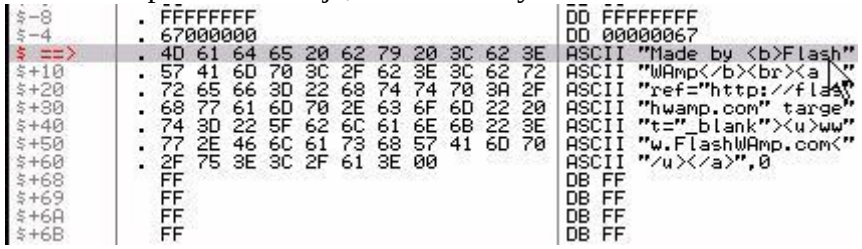


Queda como

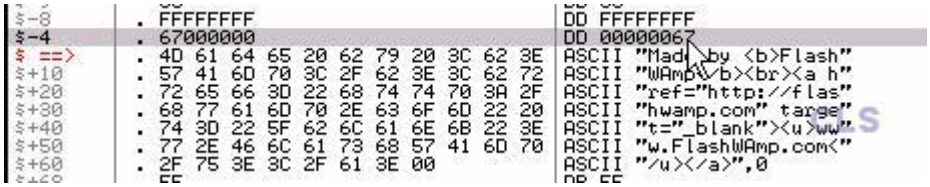
o sea echamos a perder el mensaje

Pero si hacemos otra historia

Como analizar
Veamos el primer mensaje, dice made by..etc



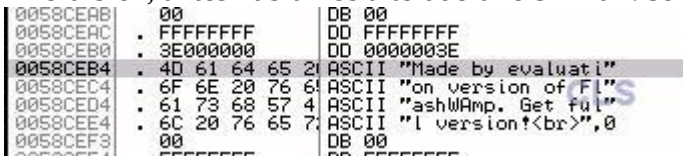
Arriba dice 67
Y claramente donde cuento tengo 67 remarcado



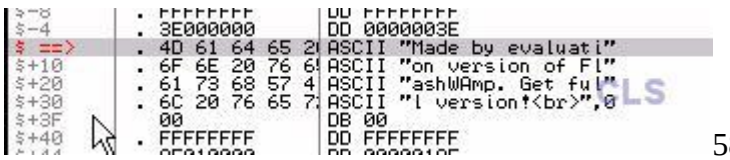
Ahora bien, mas abajo en el de unregistred dice 30

Y ahora bien como se entiende la idea (que esos 30 bytes es de la palabra unregistred)
Pues me despido de ese mensaje
Modificandolo a 0

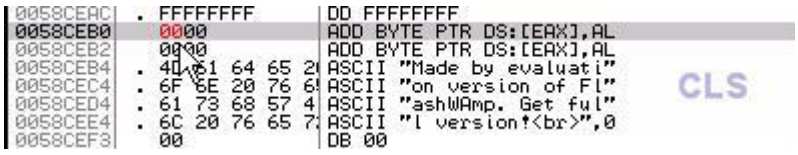
Ahora bien, antes habiamos alterado uno similar . solo con nops



Ahora como estamos claramente modificando esos mensajes
Podemos hacerlo elegantemente

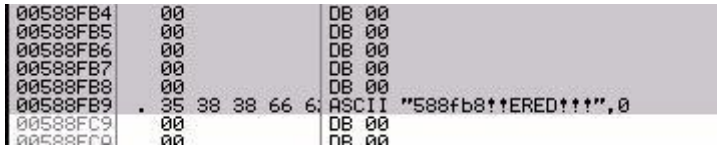


58cEb0 -> alterando a 3E a 0



Teniendo listo el mensaje que mostrara en el html
Ahora listo ese problema
Vamos al proximo

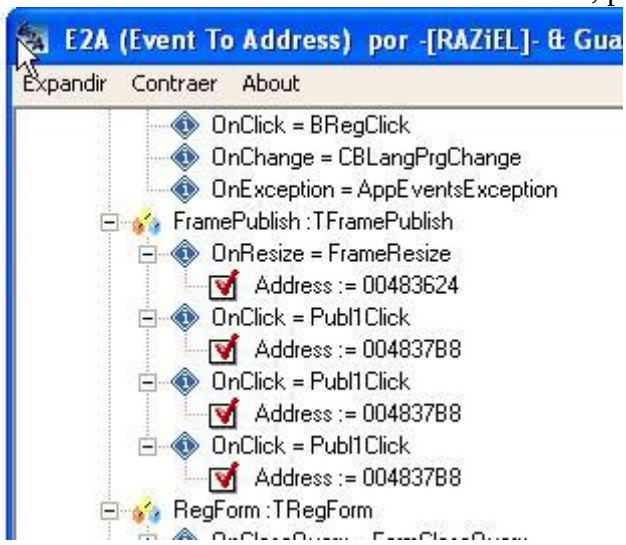
recordemos que aparece un mensaje en la parte superior , con la mismo metodo alterandolo a 0 queda como en pantalla



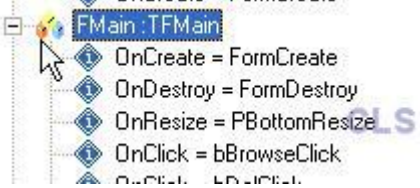
Tendriamos todo mas o menos listo
Veo en ejecución si es delphi

El unpacked

, pero el script no contiene nada ☺



El nuevo e2a aparecen referencias

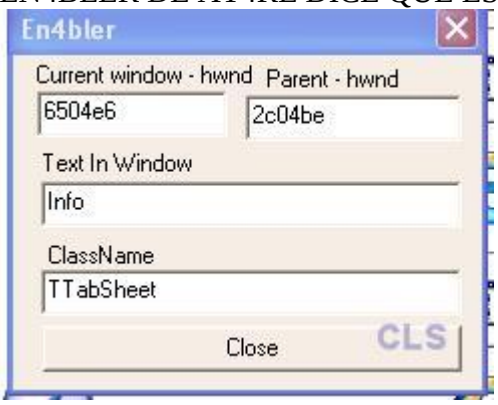


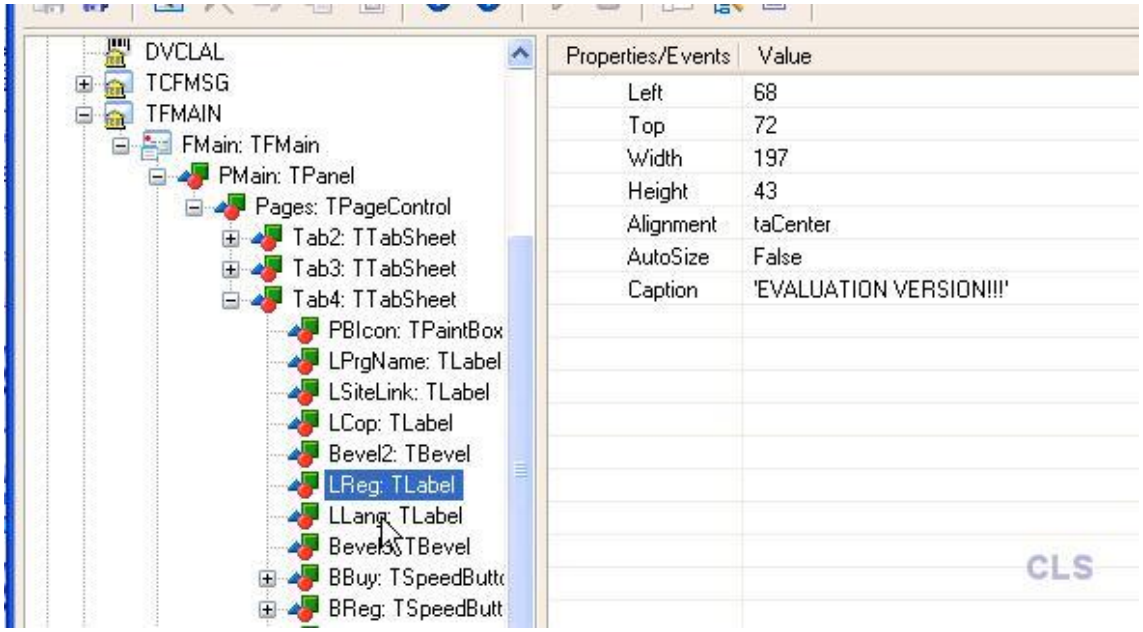
Pero al main nada(solo algunos toma y otros no..Eso pasa a los execrypteds)

Destruye demasiado el ejecutable haciendo pensar que no es delphi.

Bien queda lo ultimo a modificar

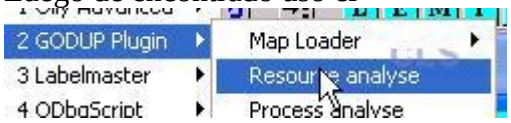
EN4BLER DE AT4RE DICE QUE ES PARTE DE INFO

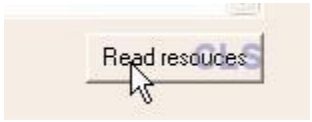




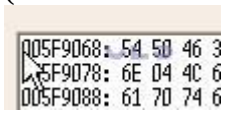
PEXPLORER LO ENCUENTRO EN MAIN
(PERO POR ESTAR UNPACKED Y SIN RESTAURAR, DEJARA LA ESCOBA
ASI QUE SOLO CON MAIN, ME QUEDO Y DE AHÍ LO BUSCO

Luego de encontrado uso el

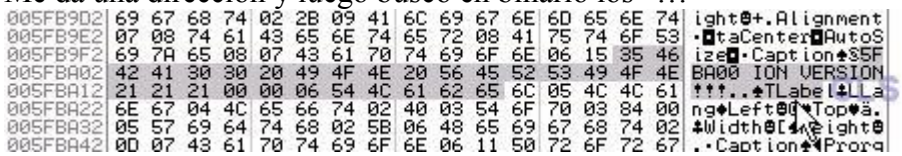




(TAMBIEN SERVIAN LAS REFERENCIAS, PERO ASI ES MAS BONITO

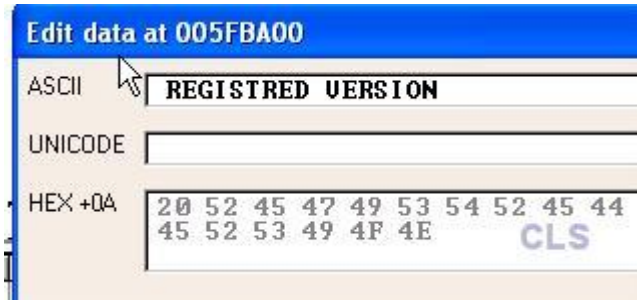


Me da una direccion y luego busco en binario los “!!!”



Y con el metodo comprobado

Puede cambiarse a



Pero como no queremos dejarlo así

Coloco VERSION APUROMAFO

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)

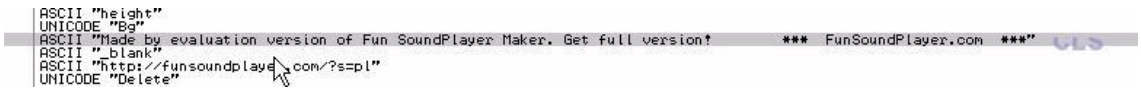
Pero no es todo eso
Guardo los cambios y se me ocurre instalar el otro programa de la web
http://www.funsoundplayer.com/download/sp_setup.exe
y aparece

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

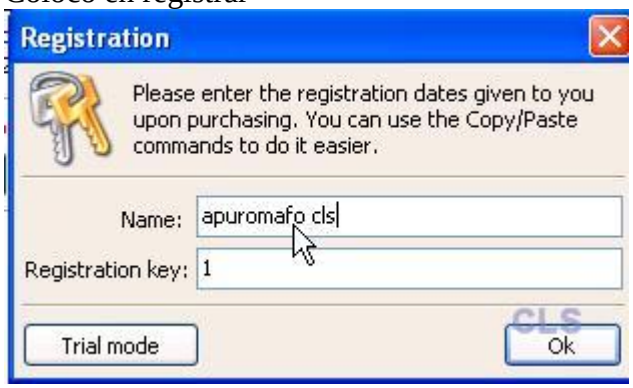
Desempaco (no mostrare)
Pero realmente no es que venga registrado, pues tiene todo lo anterior para que sea trial



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 desapàrece esa ventana

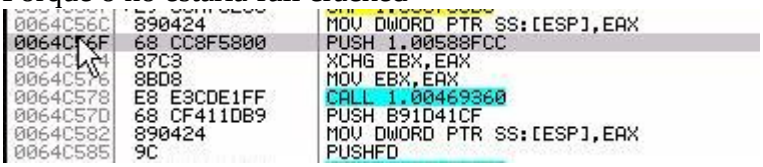
pero el programa sigue trial (eso creia)

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

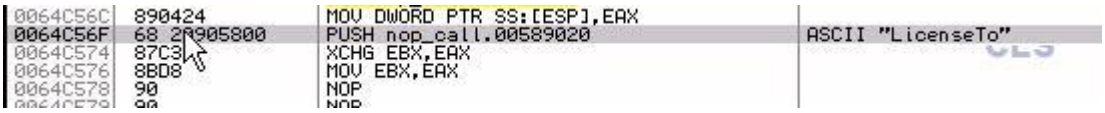
Chachan ;) toma el registro del otro
Saludos Apuromafo

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

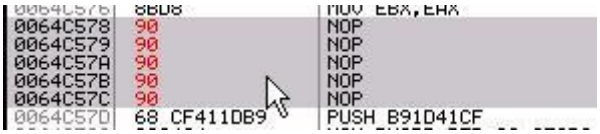


La nag aparecia con esta direccion
Encontrarla no fue tan difícil
(busque el push 588fcc)
Se puede cambiar a otro mensaje o sea aparecera la nag con otro mensaje



Luego dije, noo, mejor que no aparezca el mensaje

Anule el call nopeandolo



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
y en registrar coloca
nombre:apuromafo CLS
contraseña:1
luego de aceptarlo ve y descarga este
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