EarMaster

by Apuromafo

Encontré que necesitaban ayuda y me propuse apoyar

CLS
19/08/2013

Hola, no tengo mucho tiempo pero Hoy vamos a revisar un programa “de pago” que da soporte en 3 tipos de versiones, atacaré solo la que me llamó la atención (pro) este escrito es con fines educacionales, saludos Apuromafo

Historia:

Conversaba con un amigo que como lo hacía para reconocer un audio y reproducirlo, me refirió de este programa, pero como era trial, obviamente no había nada que hacer, hoy me propuse antes de dormir que lo vería y me animé, así que aquí el resultado

Así que manos a la obra ,espero les guste ^^

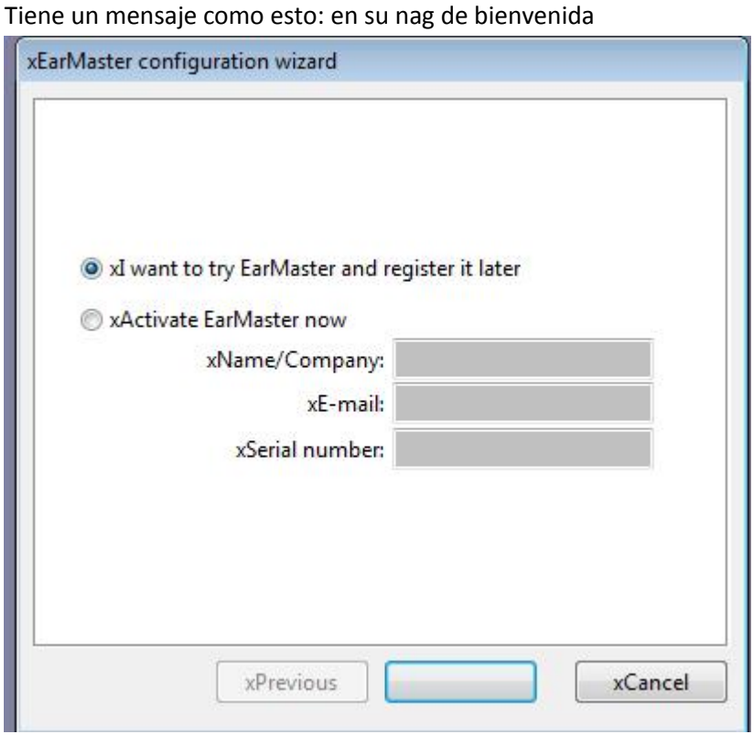
Descarga

No esta packed Se puede descargar luego de ingresar sus datos via mail un ejemplo:

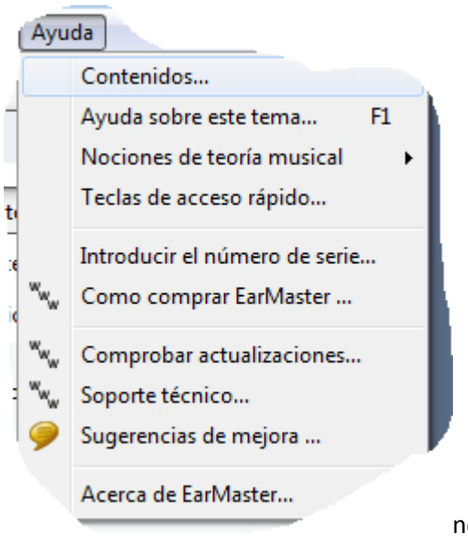
Windows (8/7/Vista/XP):
www.earmaster.com/download/k/303736/Earpro6setup.exe

No parece estar empacado:

Tiene un mensaje como esto: en su nag de bienvenida

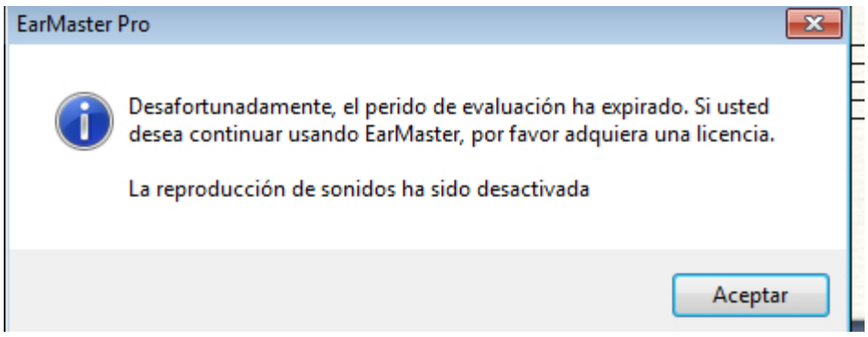


Y al ver el about/ayuda

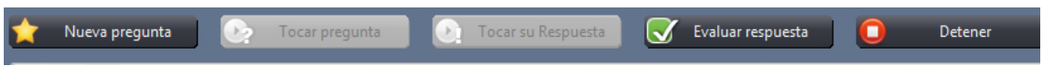


no se ve nada bien, adelantaré las sesiones, tiempo, quiero jugar un rato:

En palabras simples tenemos un programa que evaluará sesiones para escuchar y luego del período funcional ya no funciona más

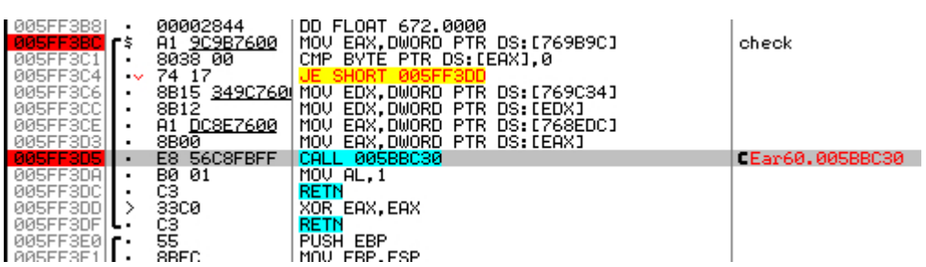


Vemos el menú sin OIR nada



Como ya somos experimentados, abrimos ollydbg, vemos donde llama el mensaje,

Si uno ve el mensaje y realiza los mismos pasos que siempre (pausa retrocesos llegamos a este check)



Aquí se viene lo importante, si es 0 continua, pero si no lo es entonces somos expired (mensaje)

Veamos, cambiaré el valor a cero y NO hay mensaje, se escucha el audio y no hay limitación así que el tema de expired está vencido si logramos mantener ese valor en cero.

Asi que ahora a buscar todos las referencias relacionadas

005FF3BC /$ A1 9C9B7600 MOV EAX,DWORD PTR DS:[769B9C] ; check

005FF3C1 |. 8038 00 CMP BYTE PTR DS:[EAX],0

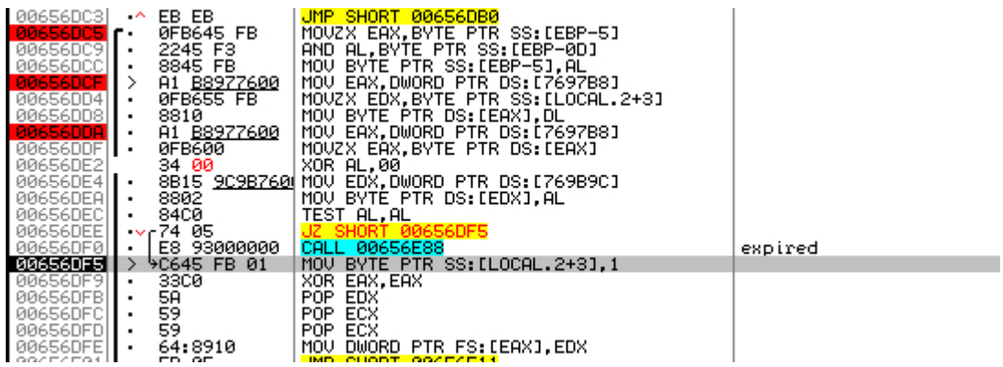
Lo segundo solo para evitar que no me deje escuchar, puedo parcharlo

```
005FF3B4  .  0000B442     DD FLOAT 90.00000
005FF3B8  .  00002844     DD FLOAT 672.0000
005FF3BC /$  A1 9C9B7600  MOV EAX,DWORD PTR DS:[769B9C]      audio off on
005FF3C1 |.  8038 00      CMP BYTE PTR DS:[EAX],0
005FF3C4 |.v 74 17        JE SHORT 005FF3DD
005FF3C6 |   C600 00      MOV BYTE PTR DS:[EAX],0
005FF3C9 |   EB 12        JMP SHORT 005FF3DD
005FF3CB |   90           NOP
005FF3CC |.  8B12         MOV EDX,DWORD PTR DS:[EDX]
005FF3CE |.  A1 DC8E7600  MOV EAX,DWORD PTR DS:[768EDC]
005FF3D3 |.  8B00         MOV EAX,DWORD PTR DS:[EAX]
005FF3D5 |.  E8 56C8FBFF  CALL 005BBC30                      CEar60.005BBC30
005FF3DA |.  B0 01        MOV AL,1
005FF3DC |.  C3           RETN
005FF3DD |>  33C0         XOR EAX,EAX
```

Luego DEL REINICIO tenemos que hay muchas variables que puede comparar:

```
006F6AC6 |.  48           DEC EAX
006F6AC7 |.v 74 0A        JZ SHORT 006F6AD3
006F6AC9 |.  A1 188D7600  MOV EAX,DWORD PTR DS:[768D18]
006F6ACE |.  8038 00      CMP BYTE PTR DS:[EAX],0
006F6AD1 |.v 74 1A        JE SHORT 006F6AED
006F6AD3 |>  A1 A4977600  MOV EAX,DWORD PTR DS:[7697A4]
006F6AD8 |.  8038 00      CMP BYTE PTR DS:[EAX],0
006F6ADB |.v 75 10        JNE SHORT 006F6AED
006F6ADD |.  A1 44957600  MOV EAX,DWORD PTR DS:[769544]
006F6AE2 |.  8B00         MOV EAX,DWORD PTR DS:[EAX]
006F6AE4 |.  0FB740 08    MOVZX EAX,WORD PTR DS:[EAX+8]
006F6AE8 |.  E8 0BAE0400  CALL 007418F8
006F6AED |>  A1 B8977600  MOV EAX,DWORD PTR DS:[7697B8]
006F6AF2 |.  8038 00      CMP BYTE PTR DS:[EAX],0
006F6AF5 |.v 74 14        JE SHORT 006F6B0B
006F6AF7 |.  A1 14997600  MOV EAX,DWORD PTR DS:[769914]
006F6AFC |.  8B00         MOV EAX,DWORD PTR DS:[EAX]
006F6AFE |.  E8 05D1E6FF  CALL 00563C08
006F6B03 |.  A1 98997600  MOV EAX,DWORD PTR DS:[769998]
006F6B08 |.  C600 00      MOV BYTE PTR DS:[EAX],0
006F6B0B |>  A1 B8977600  MOV EAX,DWORD PTR DS:[7697B8]
006F6B10 |.  8038 00      CMP BYTE PTR DS:[EAX],0
006F6B13 |.v 75 0F        JNE SHORT 006F6B24
006F6B15 |.  A1 9C9B7600  MOV EAX,DWORD PTR DS:[769B9C]
006F6B1A |.  8038 00      CMP BYTE PTR DS:[EAX],0
006F6B1D |.v 74 05        JE SHORT 006F6B24
006F6B1F |.  E8 94D6FFFF  CALL 006F41B8
006F6B24 |>  A1 B8977600  MOV EAX,DWORD PTR DS:[7697B8]
006F6B29 |.  8038 00      CMP BYTE PTR DS:[EAX],0
006F6B2C |.v 74 19        JE SHORT 006F6B47
006F6B2E |.  A1 48957600  MOV EAX,DWORD PTR DS:[769548]
006F6B33 |.  8B00         MOV EAX,DWORD PTR DS:[EAX]
006F6B35 |.  8B80 E806000( MOV EAX,DWORD PTR DS:[EAX+6E8]
```

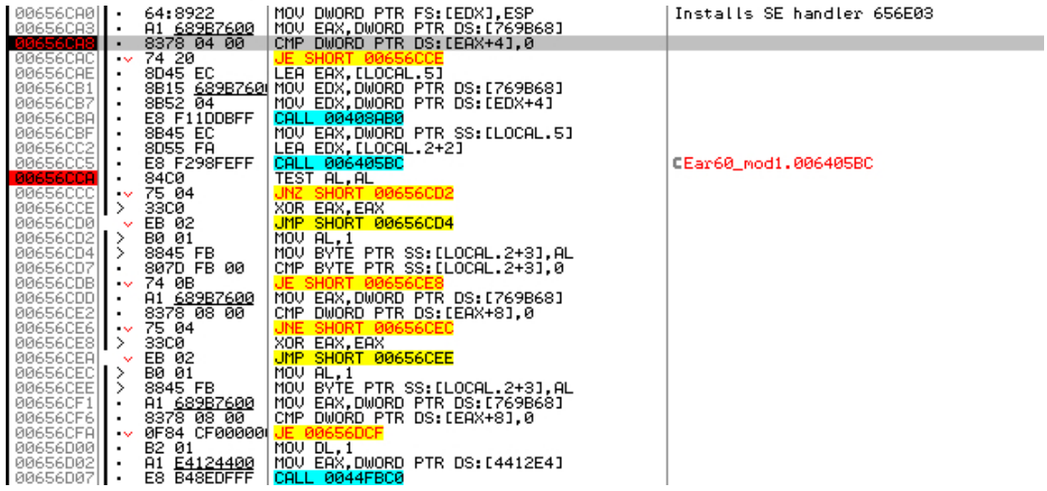
luego de buscar, encontré donde escribe el valor 1 y le coloco un parche provisional mientras medito:



Luego de mirar un poco, Tengo que mueve a eax el valor de un byte resultante de un xor, pero si logro que sea 0, entonces voy bien, pero si logro que el xor sea como lo haría un registrado sería mejor(deberíamos lograr 1 que luego con un xor 1 sería cero).

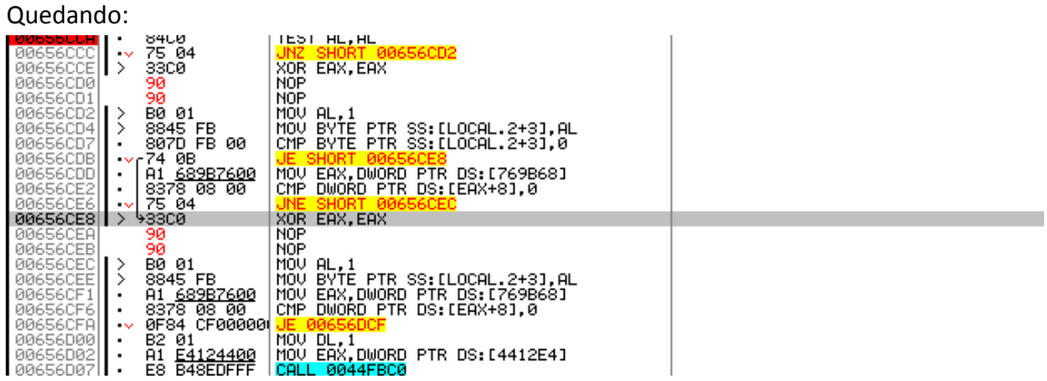
30 minutos jugando con audio y entre estas ventanas, logré registarlo directamente ya que (online) no resultó ahora quito el cambio del xor al,0 y procedo a mostrar del patch que sirve

Luego esta rutina hay 2 partes donde dice mov al,1 y necesito que valga aquello (1) (así que le hago nop en los saltos)



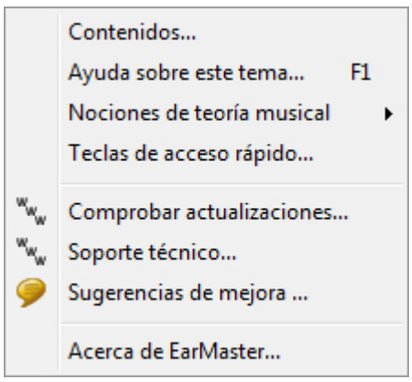
(Hace poco parchamos porque necesitábamos que fuera cero, pero eso viene de más arriba y llega el minuto de meditar, si hacia xor al,1 es porque si era bueno, entonces debía ser 1 entonces necesito el mov al,1 que llegue, por ende el camino más rápido es NOPEAR los saltos de jmp que veo aquí y con ello tengo el valor de 1, al ser 1 entonces el valor de 0 se asegura en el proceso siguiente)

Quedando:



Los cambios se ven a la Vista No hay trial

y el menú de hace no mucho cambió:



http://www.earmaster.com/update.html?build=2c&os=win&lan=espanol&ver=v6

y ahora estoy registrado :

Guardo los cambios, claramente corre bien, si adelanto o atraso el reloj el programa corre de lo más bien este programa no expirará : Programa derrotado, no fue tan complicado.

Saludos a la lista de Crackslatinos y amigos ^^

Saludos Apuromafo