

# CRACKS LATINOS



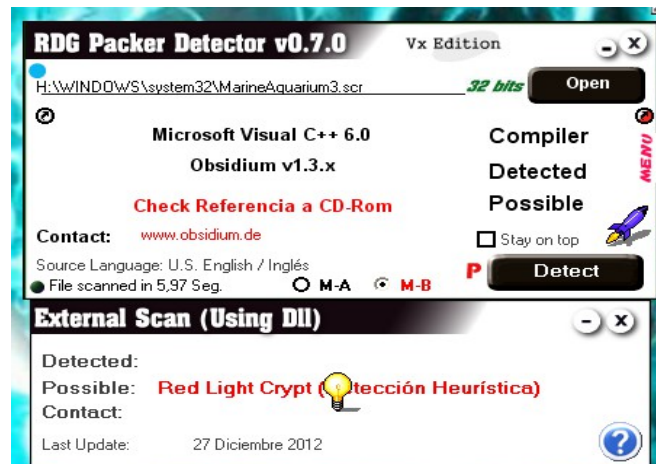
<b>Programa</b>	Marine Aquarium 3		
<b>Protección</b>	Serial y limite		
<b>Descripción</b>	Un screensaver		
<b>Dificultad</b>	Pues.....		
<b>DownLoad</b>	softonic		
<b>Herramienta</b>	olly		
<b>Cracker</b>	La Calavera	<b>Fecha</b>	

## INTRODUCCION

Bueno esto sigue siendo como desde un principio solo para el aprendizaje y nada de piratería ;-)

## AL ATAQUE

Bueno comencemos lo primero analizarlo a ver si esta comprimido y con que esta compilado



bueno ahí tenemos los que nos dice el RDG veamos el exeinfo PE



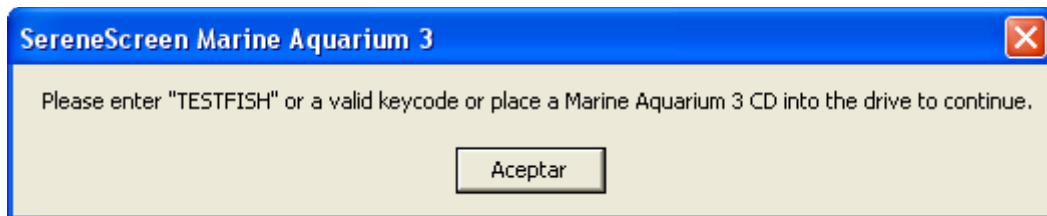
bueno como ven ambos dicen que es un VC++ así que manos a la obra lo cargamos con el olly y nos muestra el EP

Address	Hex dump	Disassembly
004894BB	55	PUSH EBP
004894BC	8BEC	MOV EBP,ESP
004894BE	6A FF	PUSH -1
004894C0	68 D0034C00	PUSH MarineAq.004C03D0
004894C5	68 18004800	PUSH MarineAq.00480018

le damos a F9 y nos sale



bueno como ven nos pide que ingresemos el serial que hemos adquirido para registrar o TESTFISH para entrar en modo de prueba bien ingresamos un serial “calavera” que tiene un largo de 8 caracteres y le damos a OK y nos muestra



Bien vamos a ver entre las string si sale el dicho cartelito buscamos keycode y no sale nada, probemos con el TESTFISH a que si encontramos algo

0041EDF9	MOV ESI,MarineAq.0055A960	ASCII "calavera"
0041EED2	PUSH MarineAq.0055A960	ASCII "calavera"
0041EEDF	PUSH MarineAq.0055A960	ASCII "calavera"
0041EEE4	PUSH MarineAq.0055A83C	ASCII "calavera"
0041EEF4	MOV ECX,MarineAq.0055A960	ASCII "calavera"
0041EF5E	PUSH MarineAq.004C6168	ASCII "TESTFISH"
0041EF63	PUSH MarineAq.0055A960	ASCII "calavera"
0041EFC0	PUSH MarineAq.0055A960	ASCII "calavera"

pues no hay muchos que decir si estamos cerca no?? jejeje hacemos doble clic y caemos aquí

0041EF37	SHC3	CMP AL,BL	
0041EF39	75 C6	JNZ SHORT MarineAq.0041EF01	
0041EF3B	83FE 14	CMP ESI,14	
0041EF3E	881A	MOV BYTE PTR DS:[EDX],BL	
0041EF40	5E	POP ESI	
0041EF41	75 13	JNZ SHORT MarineAq.0041EF56	
0041EF43	A0 6CAB5500	MOV AL,BYTE PTR DS:[55AB6C]	
0041EF48	50	PUSH EAX	
0041EF49	53	PUSH EBX	
0041EF4A	E8 51F8FFFF	CALL MarineAq.0041E7A0	
0041EF4F	83C4 08	ADD ESP,8	
0041EF52	84C0	TEST AL,AL	
0041EF54	75 2E	JNZ SHORT MarineAq.0041EF04	
0041EF56	381D 2CA75500	CMP BYTE PTR DS:[55A72C],BL	
0041EF5C	75 32	JNZ SHORT MarineAq.0041EF90	
0041EF5E	68 68614C00	PUSH MarineAq.004C6168	
0041EF63	68 60A95500	PUSH MarineAq.0055A960	
0041EF68	E8 13B60600	CALL MarineAq.0048A580	
0041EF6D	83C4 08	ADD ESP,8	
0041EF70	85C0	TEST EAX,EAX	
0041EF72	C7 1C	JNZ SHORT MarineAq.0041EF90	
0041EF74	C705 A0A95500	MOV DWORD PTR DS:[55A7A0],1	

ASCII "TESTFISH"  
ASCII "calavera"

como ven en el recuadro lo compara con el serial de prueba si es igual entra en modo de demostración y un poco mas arriba vemos algo muy interesante 41EF3B un comparación con 14h osea 20 en decimal ponemos un BP en la comparación, aceptamos el mensaje y apretamos nuevamente en OK y cuando para en la comparación vemos

```

0041EF37 | . 3AC3      CMP AL,BL
0041EF39 | . ^ 75 C6     JNZ SHORT MarineAq.0041EF01
0041EF3B | > 83FE 14    CMP ESI,14
0041EF3E | . 881A      MOV BYTE PTR DS:[EDX],BL
0041EF40 | . 5E        POP ESI
0041EF41 | . v 75 13     JNZ SHORT MarineAq.0041EF56
0041EF43 | . A0 6CAB5500 MOV AL,BYTE PTR DS:[55AB6C]
0041EF48 | . 50        PUSH EAX

ESI=00000008
Jump from 0041EEFF

```

como ven compara el largo de mi serial con 14h así que le damos a OK y pongo “calaveracalaveracala” :-> que es un largo de 20 decimal y le doy a OK, cuando para vemos que tenemos el largo correcto pero el serial ni ahí jajajaja, así que sigamos a ver donde nos lleva comenzamos a tracear

```

0041EF41 | . /75 13     JNZ SHORT MarineAq.0041EF56
0041EF43 | | A0 6CAB5500 MOV AL,BYTE PTR DS:[55AB6C]
0041EF48 | | 50        PUSH EAX
0041EF49 | | 53        PUSH EBX
0041EF4A | | E8 51F8FFFF CALL MarineAq.0041E7A0
0041EF4F | | 83C4 08    ADD ESP,8
0041EF52 | | 84C0      TEST AL,AL
0041EF54 | | 75 2E     JNZ SHORT MarineAq.0041EF84

```

hasta el call traceamos y entramos en el y vemos

```

0041E79F | . 90        NOP
0041E7A0 | $ 81EC 34010000 SUB ESP,134
0041E7A6 | . 53        PUSH EBX
0041E7A7 | . 55        PUSH EBP
0041E7A8 | . 56        PUSH ESI
0041E7A9 | . 57        PUSH EDI
0041E7AA | . 68 C8000000 PUSH 0C8
0041E7AB | . C705 A0A95500 MOV DWORD PTR DS:[55A9A0],0
0041E7AD | . E8 7B970600 CALL MarineAq.00487F39
0041E7BE | . 8B1D E8049000 MOV EBX,DWORD PTR DS:[<&KERNEL32.GetWind kernel32.GetWindow
0041E7C4 | . 8B2D E4804900 MOV EBP,DWORD PTR DS:[<&KERNEL32.GetVolum kernel32.GetVolume
0041E7CA | . 894424 18   MOV DWORD PTR SS:[ESP+18],EAX
0041E7CE | . 8A8424 4C0100 MOV AL,BYTE PTR SS:[ESP+14C]
0041E7D5 | . 83C4 04     ADD ESP,4
0041E7D8 | . 84C0      TEST AL,AL
0041E7DA | . v 75 5C     JNZ SHORT MarineAq.0041E838
0041E7DC | . 8D4424 40   LEA EAX,DWORD PTR SS:[ESP+40]

```

bien analizamos un poco y veamos el final del call que valores sale EAX o AL para que estemos registrado

```

0041EB3F | . 83C4 04     ADD ESP,4
0041EB42 | . 33C0      XOR EAX,EAX
0041EB44 | . 83F9 02     CMP ECX,2
0041EB47 | . 5F        POP EDI
0041EB48 | . 5E        POP ESI
0041EB49 | . 5D        POP EBP
0041EB4A | . 5B        POP EBX
0041EB4B | . 0F94C0     SETE AL
0041EB4E | . 81C4 34010000 ADD ESP,134
0041EB54 | . C3        RETN
0041EB55 | . 90        NOP

```

como vemos primero pone a EAX en cero luego compara a ECX con 2 y luego setea si la comparación dio OK pone a EAX o AL en 1 si no lo deja en cero así que debemos buscar donde mete el 2 en ECX mirando un poco mas arriba vemos

```

0041EAF0 > 6A 00          PUSH 0
0041EAF0 > C705 A0A95500 MOU DWORD PTR DS:[55A9A0],2
0041EAF0 > E8 B5F7FFFF    CALL MarineAq.0041E2C0
0041EB0B . 83C4 04        ADD ESP,4
0041EB0E > EB 1F          JMP SHORT MarineAq.0041EB2F
0041EB10 > E8 AB000000    CALL MarineAq.0041EBC0
0041EB15 . 83C4 08        ADD ESP,8
0041EB18 . 83F8 64        CMP EAX,64
0041EB1B > 7C 03          JL SHORT MarineAq.0041EB20
0041EB1D . 83C0 9C        ADD EAX,-64
0041EB20 > 3B05 90304C00 CMP EAX,DWORD PTR DS:[4C3090]
0041EB26 > 7D 07          JGE SHORT MarineAq.0041EB2F
0041EB28 . C605 6EAB5500 MOU BYTE PTR DS:[55AB6E],1
0041EB2F > 8B4424 14      MOU EAX,DWORD PTR SS:[ESP+14]
0041EB33 . 50             PUSH EAX
0041EB34 . E8 85910600    CALL MarineAq.00487CBE
0041EB39 . 8B0D A0A95500 MOU ECX,DWORD PTR DS:[55A9A0]
0041EB3F . 83C4 04        ADD ESP,4

```

como ven en 41EAF0 mueve un 2 a 55A9A0 y luego en 41EB39 lo mueve a ECX bien ahí tenemos la dirección a la cual debemos llegar así que como estamos parados en el inicio del call comenzamos a tracear y ver que salto evita caer en esta zona, vamos traceando y si miran un poco verán que el serial lo pasa a binarios así que yo me olvide de hallarlo así que seguimos traceando hasta esta dirección

```

0041EA2F . 3BE8          CMP EBP,EAX
0041EA31 > 0F85 F8000000 JNZ MarineAq.0041EB2F
0041EA37 . 6A 08         PUSH 8
0041EA39 . 56            PUSH ESI
0041EA3A . E8 81010000    CALL MarineAq.0041EBC0
0041EA3F . 83C4 08        ADD ESP,8
0041EA42 . 85C0          TEST EAX,EAX
0041EA44 > 0F85 E5000000 JNZ MarineAq.0041EB2F
0041EA4A . 8B5424 14      MOU EDX,DWORD PTR SS:[ESP+14]

```

como ven el salto se va a efectuar y nos manda lejos de donde queremos llegar así que lo nopeamos y seguimos

```

0041EA42 . 85C0          TEST EAX,EAX
0041EA44 > 0F85 E5000000 JNZ MarineAq.0041EB2F
0041EA4A . 8B5424 14      MOU EDX,DWORD PTR SS:[ESP+14]
0041EA4E . 50            PUSH EAX
0041EA4F . 8D4C24 24      LEA ECX,DWORD PTR SS:[ESP+24]
0041EA53 . 6A 0A         PUSH 0A
0041EA55 . 51            PUSH ECX

```

el próximo es es y efectivamente también va a saltar así que lo nopeamos y seguimos

```

0041EA7E . 83FA 05       CMP EDI,5
0041EA81 > 0F84 A8000000 JE MarineAq.0041EB2F
0041EA87 . 84DB          TEST BL,BL
0041EA89 > 0F85 A0000000 JNZ MarineAq.0041EB2F
0041EA8F . A1 90304C00   MOU EAX,DWORD PTR DS:[4C3090]
0041EA94 . 85C0          TEST EAX,EAX

```

lo mismo nopeamos los 2 ya que van a la misma dirección y seguimos



0041EA96	-	8BF8	MOU EDI,EAX
0041EA98	-	75 05	JNZ SHORT MarineAq.0041EA9F
0041EA9A	-	BF 01000000	MOU EDI,1
0041EA9F	>	8B5424 14	MOU EDX,DWORD PTR SS:[ESP+14]
0041EAA3	-	6A 07	PUSH 7

ese como es un salto corto lo dejamos ya que no influye seguimos

0041EABD	-	56	PUSH ESI
0041EABE	-	75 50	JNZ SHORT MarineAq.0041EB10
0041EAC0	-	E8 FB000000	CALL MarineAq.0041EBC0
0041EAC5	-	83C4 08	ADD ESP,8
0041EAC8	-	83F8 64	CMP EAX,64
0041EACB	-	7C 2D	JL SHORT MarineAq.0041EAF8
0041EACD	-	6A 07	PUSH 7

como vemos este salto se va a efectuar y evita nuestra zona así que lo mismo NOP y seguimos traceando

0041EAE0	-	E8 03000000	CALL MarineAq.0041E750
0041EAE3	-	84C0	TEST AL,AL
0041EAEF	-	75 09	JNZ SHORT MarineAq.0041EAF8
0041EAF1	>	C605 6DAB5500	MOV BYTE PTR DS:[55AB6D],1
0041EAF8	-	EB 35	JMP SHORT MarineAq.0041EB2F
0041EAF8	>	6A 00	PUSH 0
0041EAF8	-	C705 A0A95500	MOV DWORD PTR DS:[55A9A0],2
0041EAF8	-	E8 B5F7FFFF	CALL MarineAq.0041E2C0
0041EB06	-	83C4 04	ADD ESP,4

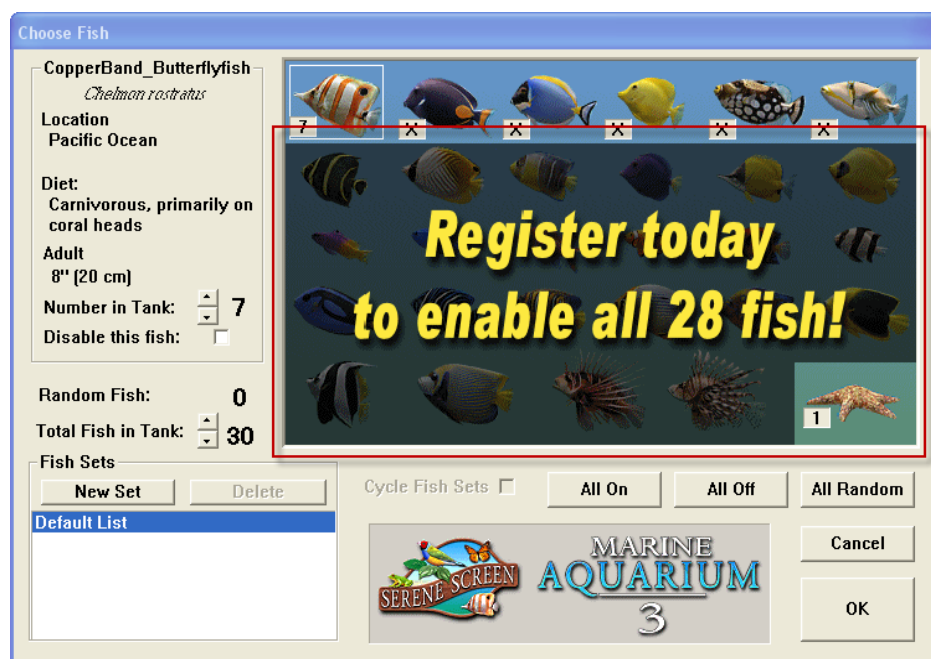
bueno llegamos y como vemos el salto no se va a efectuar y llegamos al JMP que evita nuestra zona y si el salto se efectúa mete el dichoso 2 a nuestra dirección así que lo cambiamos por un JMP 41EAF8 y le damos a F9 y arranca el panel de control del screensaver



vamos a Settings y vemos



como ven salen todos los peces que trae el programa



y esa es una captura del programa sin registrar de la misma ventana como ven el screensaver quedo registrado.

Bueno esto es para toda la maravillosa lista CracksLatinos y este es un regalito de cumple AÑOS

Saludos y vamos por muchos años massssss!!!!!!!!!!!!!!!!!!!!!!

Daniel

