

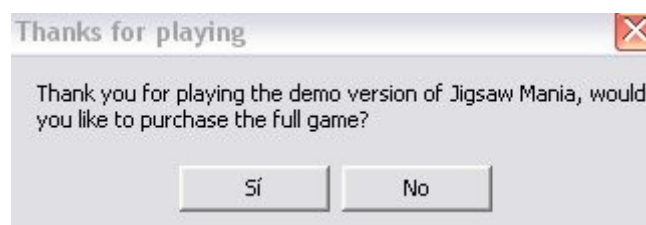


URL	http://www.InertiaSoftware.com
Victima	Jigsaw Mania
Herramientas	Olly
Cracker	ZiKaTRiZ
Dificultad	Facil
Fecha	4 – agosto - 2011

Hola, hoy nos encontramos con este paciente, que tiene la enfermedad del trial versión, una enfermedad muy habitual.

Al ejecutar el software, comprobamos los tres puntos importantes que debemos corregir :

1. Jigsaw Mania trial version
2. Trial version expired
3. Y el aviso final , que te da las gracias por jugar, pero que si no lo compras, caduca.



Carguemoslo en Olly

### Primer punto:

Miramos en las String references y nos encontramos

```
0040A035 PUSH Jigsaw_M.004A2418 ASCII "Jigsaw Mania trial version - "
0040A041 PUSH Jigsaw_M.004A2408 ASCII "Jigsaw Mania - "
```

pulsamos con el ratón en cualquiera de las dos referencias y nos manda a

0040A02F	74 0C	JE SHORT Jigsaw_M.0040A03D	
0040A031	804C24 04	LEA ECX,DWORD PTR SS:[ESP+4]	
0040A035	68 18244A00	PUSH Jigsaw_M.004A2418	ASCII "Jigsaw Mania trial version - "
0040A03A	51	PUSH ECX	
0040A03B	EB 0A	JMP SHORT Jigsaw_M.0040A047	
0040A03D	8D5424 04	LEA EDX,DWORD PTR SS:[ESP+4]	
0040A041	68 08244A00	PUSH Jigsaw_M.004A2408	ASCII "Jigsaw Mania - "
0040A046	52	PUSH EDX	

```
00415EF3 PUSH Jigsaw_M.004A270C ASCII "This trial version has now expired, tha
004160AF PUSH Jigsaw_M.004A27D0 ASCII "%Quit"
```

aquí nos encontramos con un salto condicional, bueno pues le diremos que cuando llegue a la dirección 0040A02F realice el salto sin pensar. Colocándonos en ese dirección pulsaremos las teclas CTRL+E o botón derecho del ratón Binary – Edit. Cambiaremos el 74 0C por EB 0C , como muestra la siguiente imagen.

0040A02F	EB 0C	JMP SHORT Jigsaw_M.0040A03D	
0040A031	8D4C24 04	LEA ECX,DWORD PTR SS:[ESP+4]	
0040A035	68 18244A00	PUSH Jigsaw_M.004A2418	ASCII "Jigsaw Mania trial version - "
0040A03A	51	PUSH ECX	
0040A03B	EB 0A	JMP SHORT Jigsaw_M.0040A047	
0040A03D	8D5424 04	LEA EDX,DWORD PTR SS:[ESP+4]	
0040A041	68 08244A00	PUSH Jigsaw_M.004A2408	ASCII "Jigsaw Mania - "

## Segundo punto:

00415EF3 PUSH Jigsaw\_M.004A270C ASCII "This trial version has now expired,"

podemos ver que hace referencia a la llamada de una call con la dirección 00415EBB como muestra la siguiente imagen

00415ED0	6A FF	PUSH -1	
00415ED2	68 D05A4800	PUSH Jigsaw_M.00485AD0	SE handler instal
00415ED7	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
00415EDD	50	PUSH EAX	
00415EDE	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
00415EE5	83EC 64	SUB ESP,64	
00415EE8	6A 00	PUSH 0	
00415EEA	8D4C24 04	LEA ECX,DWORD PTR SS:[ESP+4]	
00415EEE	E8 CD000000	CALL Jigsaw_M.00415FC0	
00415EF3	68 0C274A00	PUSH Jigsaw_M.004A270C	ASCII "This trial
00415EF8	8D4C24 64	LEA ECX,DWORD PTR SS:[ESP+64]	
00415EFC	C74424 70 00000000	MOV DWORD PTR SS:[ESP+70],0	
00415F04	E8 30170500	CALL Jigsaw_M.00467639	
00415F09	A1 24A24A00	MOV EAX,DWORD PTR DS:[4AA24A]	
00415F0E	C74424 5C 01000000	MOV DWORD PTR SS:[ESP+5C],1	
00415F16	85C0	TEST EAX,EAX	
00415F18	74 0A	JE SHORT Jigsaw_M.00415F24	
00415F1A	C780 88000000 01000	MOV DWORD PTR DS:[EAX+88],1	
00415F24	8D4C24 00	LEA ECX,DWORD PTR SS:[ESP]	
00415F28	E8 B9690500	CALL Jigsaw_M.0046C8E6	
00415F2D	6A 00	PUSH 0	
00415F2F	FF15 D8A54800	CALL DWORD PTR DS:[<&USER32.PostQuitMe	ExitCode = 0 PostQuitMessage
00415F35	8D4C24 60	LEA ECX,DWORD PTR SS:[ESP+60]	
00415F39	C74424 6C 01000000	MOV DWORD PTR SS:[ESP+6C],1	
00415F41	E8 6A150500	CALL Jigsaw_M.00467480	
00415F46	8D4C24 00	LEA ECX,DWORD PTR SS:[ESP]	
00415F4A	C74424 6C FFFFFFFF	MOV DWORD PTR SS:[ESP+6C],-1	
00415F52	E8 81650500	CALL Jigsaw_M.0046C4D8	
00415F57	8B4C24 64	MOV ECX,DWORD PTR SS:[ESP+64]	
00415F5B	64:8900 00000000	MOV DWORD PTR FS:[0],ECX	
00415F62	83C4 70	ADD ESP,70	
00415F65	C3	RETN	
00415F66	00	NOB	

Local call from 00415EBB

colocándonos en el inicio de la rutina, botón derecho del ratón Goto Call from 00415EBB

00415EB3	7E 10	JLE SHORT Jigsaw_M.00415EC5	
00415EB5	8BCE	MOV ECX,ESI	
00415EB7	C646 18 01	MOV BYTE PTR DS:[ESI+18],1	
00415EBB	E8 10000000	CALL Jigsaw_M.00415ED0	
00415EC0	32C0	XOR AL,AL	
00415EC2	5E	POP ESI	
00415EC3	59	POP ECX	
00415EC4	C3	RETN	
00415EC5	B0 01	MOV AL,1	
00415EC7	5E	POP ESI	
00415EC8	59	POP ECX	
00415EC9	C3	RETN	

otro salto condicional, bueno pues le diremos que cuando llegue a la dirección 00415EB3 realice el salto sin pensar. Colocándonos en ese dirección pulsaremos las teclas CTRL+E o botón derecho del ratón Binary – Edit. Cambiaremos el 7E 10 por EB 10 , como muestra la siguiente imagen.

00415EB3	EB 10	JMP SHORT Jigsaw_M.00415EC5	
00415EB5	8BCE	MOV ECX,ESI	
00415EB7	C646 18 01	MOV BYTE PTR DS:[ESI+18],1	
00415EBB	E8 10000000	CALL Jigsaw_M.00415ED0	
00415EC0	32C0	XOR AL,AL	
00415EC2	5E	POP ESI	
00415EC3	59	POP ECX	
00415EC4	C3	RETN	
00415EC5	B0 01	MOV AL,1	
00415EC7	5E	POP ESI	
00415EC8	59	POP ECX	
00415EC9	C3	RETN	

Con esto, no caduca y eliminamos el purchase automáticamente

## Tercer punto:

Mirando en las string references vemos

00427631	PUSH Jigsaw_M.004A4C34	ASCII "Thanks for playing"
00427636	PUSH Jigsaw_M.004A4BD0	ASCII "Thank you for playing the demo version of Jigsaw Mania,

Vallamos a la dirección 00427631, como podemos comprobar el salto JE que tenemos justo encima de las referencias, es el que decide si nos muestra el aviso de que estamos en una demo o no.

00427620	§ A1 ECA14A00	MOV EAX,DWORD PTR DS:[4AA1EC]	
00427625	. 56	PUSH ESI	
00427626	. 8BF1	MOV ESI,ECX	
00427628	. 8A48 04	MOV CL,BYTE PTR DS:[EAX+4]	
0042762B	. 84C9	TEST CL,CL	
0042762D	✓ 74 1F	JE SHORT Jigsaw_M.0042764E	
0042762F	. 6A 04	PUSH 4	
00427631	. 68 344C4A00	PUSH Jigsaw_M.004A4C34	ASCII "Thanks for playing"
00427636	. 68 D04B4A00	PUSH Jigsaw_M.004A4BD0	ASCII "Thank you for playing th
0042763B	. 8BCE	MOV ECX,ESI	
0042763D	. E8 A72D0400	CALL Jigsaw_M.0046A3E9	
00427642	. 83F8 06	CMP EAX,6	
00427645	✓ 75 07	JNZ SHORT Jigsaw_M.0042764E	
00427647	. 8BCE	MOV ECX,ESI	
00427649	. E8 62E9FFFF	CALL Jigsaw_M.00425FB0	
0042764E	> 5E	POP ESI	
0042764F	. C3	RETN	
00427650	. 51	PUSH ECX	
00427651	. 51	PUSH ECX	
00427652	. 8BCC	MOV ECX,ESP	
00427654	. 896424 04	MOV DWORD PTR SS:[ESP+4],ESP	
00427658	. 60 4B4C4A00	PUSH Jigsaw_M.004A4C40	ASCII "Thanks for playing"

[004AA1EC]=00000000  
Local calls from 00421199, 00425E7F

bueno pues le diremos que cuando llegue a la dirección 0042762D realice el salto sin pensar. Colocándonos en ese dirección pulsaremos las teclas CTRL+E o botón derecho del ratón Binary – Edit. Cambiaremos el 74 1F por EB 1F , y de esta manera cuando cerremos el programa lo cerrará sin necesidad de darnos las gracias por jugar en su versión demo

00427620	§ A1 ECA14A00	MOV EAX,DWORD PTR DS:[4AA1EC]	
00427625	. 56	PUSH ESI	
00427626	. 8BF1	MOV ESI,ECX	
00427628	. 8A48 04	MOV CL,BYTE PTR DS:[EAX+4]	
0042762B	. 84C9	TEST CL,CL	
0042762D	✓ EB 1F	JMP SHORT Jigsaw_M.0042764E	
0042762F	. 6A 04	PUSH 4	
00427631	. 68 344C4A00	PUSH Jigsaw_M.004A4C34	ASCII "Thanks for
00427636	. 68 D04B4A00	PUSH Jigsaw_M.004A4BD0	ASCII "Thank you f
0042763B	. 8BCE	MOV ECX,ESI	
0042763D	. E8 A72D0400	CALL Jigsaw_M.0046A3E9	
00427642	. 83F8 06	CMP EAX,6	
00427645	✓ 75 07	JNZ SHORT Jigsaw_M.0042764E	
00427647	. 8BCE	MOV ECX,ESI	
00427649	. E8 62E9FFFF	CALL Jigsaw_M.00425FB0	
0042764E	> 5E	POP ESI	
0042764F	. C3	RETN	

Listo.

ZiKaTRiZ