

# CRACKS LATINOS



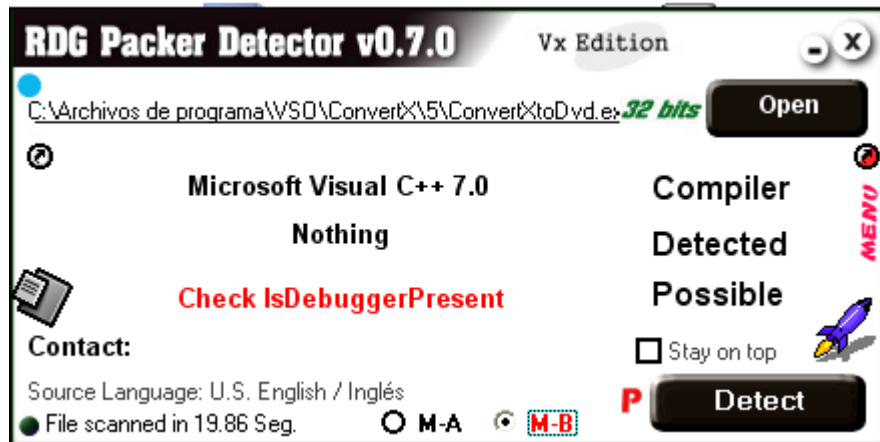
<b>Programa</b>	ConvertXtoDvd 5		
<b>Protección</b>	serial		
<b>Descripción</b>	Un conversor		
<b>Dificultad</b>	¿?¿?¿?		
<b>DownLoad</b>	<a href="http://www.vso-software.fr/products/convert_x_to_dvd/">http://www.vso-software.fr/products/convert_x_to_dvd/</a>		
<b>Herramienta</b>	olly		
<b>Cracker</b>	La Calavera	<b>Fecha</b>	

## INTRODUCCION

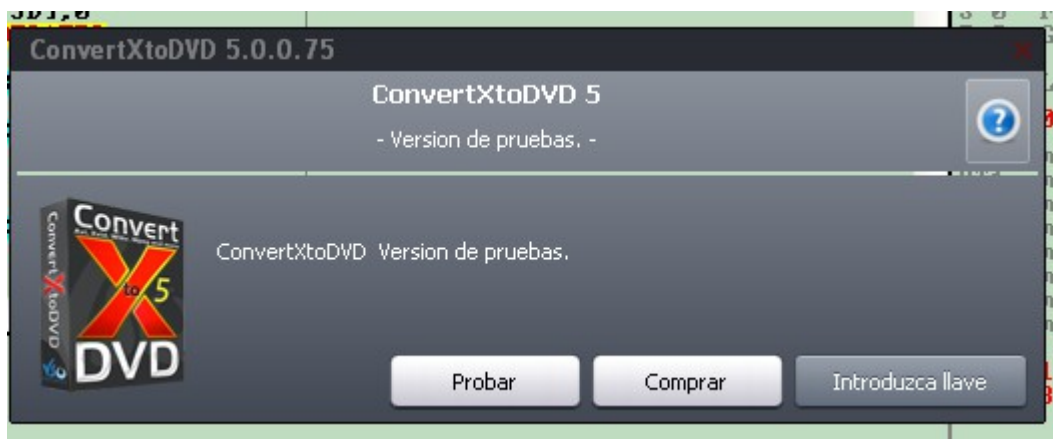
Bueno aquí con otro tute que espero les guste

## AL ATAQUE

Arrancando y veamos con que nos encontramos le pasamos el RDG y nos dice



Bien dice que estamos ante un VC++ 7 así que acto seguido al olly a ver que nos depara el destino ante este programa lo cargamos y ejecutamos a ver que nos muestra





Bueno como ven nos invita directamente a que nos registremos así que vamos a solucionar eso, así que para ello miramos en la imagen y tenemos un lindo “Versión de pruebas” traducido “trial version” :-D así que busque en el olly a ver si lo hallamos y vemos

00D4497E	MOV EAX,ConvertX.00D44F30	UNICODE "Enter key"
00D449B3	MOV EAX,ConvertX.00D44F50	UNICODE "Registered for:"
00D449F6	PUSH ConvertX.00D44F8C	UNICODE "- "
00D449FE	MOV EAX,ConvertX.00D44FA0	UNICODE "Trial version"
00D44A0B	PUSH ConvertX.00D44FC8	UNICODE "- "
00D451C8	PUSH ConvertX.00D45840	UNICODE " "
00D451D0	MOV EAX,ConvertX.00D45854	UNICODE "Trial version"
00D45223	PUSH ConvertX.00D4587C	UNICODE "<FONT color=\"#FF4040\">"
00D5B774	UNICODE "ersion",0	
00D5B819	MOV EDX,ConvertX.00D5B92C	UNICODE "TrialVersion"
00D5B84B	MOV EDX,ConvertX.00D5B954	UNICODE "LicenseKey"
00D5B862	MOV EDX,ConvertX.00D5B954	UNICODE "LicenseKey"

00D89AB0	MOV EAX,ConvertX.00D89C34	UNICODE "version"
00D89AB3	MOV EAX,ConvertX.00D89C50	UNICODE "Trial version"
00D89B0C	MOV EAX,ConvertX.00D89C78	UNICODE "Registered version" 

Bueno esos son todos como verán sale en varios lugares y fui poniendo un BP en cada uno que sale para que cuando para ver como evitarlo así que reiniciamos y veamos que nos encontramos

Address	Hex dump	Disassembly	Comment
00D449A5	. E8 26C8C4FF	CALL ConvertX.009911D0	
00D449A8	. 837D BC 10	CMP DWORD PTR SS:[EBP-44],10	
00D449AE	. 75 46	JNZ SHORT ConvertX.00D449F6	
00D449B0	. 8D55 B4	LEA EDX,DWORD PTR SS:[EBP-4C]	
00D449B3	. B8 504FD400	MOV EAX,ConvertX.00D44F50	UNICODE "Registered for:" 
00D449B8	. E8 DF1BA1FF	CALL ConvertX.0075659C	
00D449BD	. FF75 B4	PUSH DWORD PTR SS:[EBP-4C]	
00D449C0	. 68 7C4FD400	PUSH ConvertX.00D44F7C	
00D449C5	. 33C0	XOR EAX,EAX	
00D449C7	. E8 D4B5C4FF	CALL ConvertX.0098FFA0	
00D449CC	. 8D4D B0	LEA ECX,DWORD PTR SS:[EBP-50]	
00D449CF	. B2 01	MOV DL,1	
00D449D1	. E8 6AC1C4FF	CALL ConvertX.00990B40	
00D449D6	. FF75 B0	PUSH DWORD PTR SS:[EBP-50]	
00D449D9	. 8D45 B8	LEA EAX,DWORD PTR SS:[EBP-48]	
00D449DC	. BA 03000000	MOV EDI,3	
00D449E1	. E8 466D6CFF	CALL ConvertX.0040B72C	
00D449E6	. 8B55 B8	MOV EDI,DWORD PTR SS:[EBP-48]	
00D449E9	. 8B83 A8030000	MOV EAX,DWORD PTR DS:[EBX+3A8]	
00D449EF	. E8 B8E080FF	CALL ConvertX.00552AAC	
00D449F4	. EB 35	JMP SHORT ConvertX.00D44A2B	
00D449F6	. 68 8C4FD400	PUSH ConvertX.00D44F8C	UNICODE "- "
00D449FB	. 8D55 A8	LEA EDI,DWORD PTR SS:[EBP-58]	
00D449FE	. B8 A04FD400	MOV EAX,ConvertX.00D44FA0	UNICODE "Trial version" 
00D44A03	. E8 941BA1FF	CALL ConvertX.0075659C	
00D44A08	. FF75 A8	PUSH DWORD PTR SS:[EBP-58]	

Bien ahí es la primera vez que para si miramos por encima tenemos un “Registered for:” y justo por encima tenemos una CMP y un Call así que ponemos un BP en el CALL y reiniciamos a y cuando para en el call lo pasamos y vemos

00D449A1	. 33C7	XOR EAX,EAX	
00D449A3	. 33D2	XOR EDI,EDI	
00D449A5	. E8 26C8C4FF	CALL ConvertX.009911D0	
00D449A8	. 837D BC 10	CMP DWORD PTR SS:[EBP-44],10	
00D449AE	. 75 46	JNZ SHORT ConvertX.00D449F6	
00D449B0	. 8D55 B4	LEA EDI,DWORD PTR SS:[EBP-4C]	
00D449B3	. B8 504FD400	MOV EAX,ConvertX.00D44F50	UNICODE
00D449B8	. E8 DF1BA1FF	CALL ConvertX.0075659C	
00D449BD	. FF75 B4	PUSH DWORD PTR SS:[EBP-4C]	

Stack SS:[0023F4E0]	=00000005
---------------------	-----------

como ven vale 5 así que entramos al call a ver que tenemos dentro y vemos en el final

009914A0	. 84C0	TEST AL,AL	
009914A2	. 74 07	JE SHORT ConvertX.009914AB	
009914A4	. B8 03000000	MOV EAX,3	
009914A9	. EB 02	JMP SHORT ConvertX.009914AD	
009914AB	. 8BC2	MOV EAX,EDI	
009914AD	. 8903	MOV DWORD PTR DS:[EBX],EAX	
009914AF	. 33C0	XOR EAX,EAX	

Bueno sobre el final del call tenemos un JE en 9914A2 luego un MOV EAX, 3 y un poco mas abajo tenemos otro MOV de EAX a la dirección que apunte EBX.

Bien visto esto ponemos un BP en el JE y otro en 9914AD para ver que valor tiene EAX, reiniciamos y cuando para vemos

0099149D	-	0FBED2	MOVSX EDX,DL
009914A0	-	84C0	TEST AL,AL
009914A2	-	74 07	JE SHORT ConvertX.009914AB
009914A4	-	B8 03000000	MOV EAX,3
009914A9	-	EB 02	JMP SHORT ConvertX.009914AD
009914AB	>	8BC2	MOV EAX,EDX
009914AD	>	8903	MOV DWORD PTR DS:[EBX],EAX
009914AF	-	33C0	XOR EAX,EAX
009914B4	-	FA	POP EBP

Jump is taken  
009914AB-ConvertX.009914AB

Bueno ahí paro y vemos que va a saltar y va a meter el valor que tiene EDX en EAX para luego meterlo en la dirección y si miramos en EDX tenemos

Registers (FPU)	
EAX	00000000
ECX	00000000
EDX	00000005
EBX	0023FE7C
ESP	0023FE0C
EBP	0023FE54
ESI	070EEDF0
EDI	0000001A
EIP	009914A2

como ven tenemos un 5 y si el salto no se realiza tendríamos un 3 en EAX.

Bien ahora veamos a donde mueve EAX o sea a que dirección mete el valor de EAX y que pasa luego

EAX=00000005  
Stack DS:[0023FE7C]=00000005  
Jump from 009914A9

vemos que la mete en 23FE7C seguimos traceando hasta salir del call y vemos

00DA6949	-	33D2	XOR EDX,EDX
00DA694B	-	E8 80A8BEFF	CALL ConvertX.009911D0
00DA6950	-	837D 90 10	CMP DWORD PTR SS:[EBP-70],10
00DA6954	-	75 1D	JNZ SHORT ConvertX.00DA6973
00DA6956	-	BA E0D5FA00	MOV EDX,ConvertX.00FAD5E0
00DA695B	-	8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]
00DA695E	-	8B80 640A0000	MOV EAX,DWORD PTR DS:[EAX+A64]

Cuando salimos llegamos a otra parte no en la que vimos anterior mente pero tenemos algo igual una CMP con 10 y si miramos la dirección vemos

Stack SS:[0023FE7C]=00000005

la misma que vimos antes así que EAX debe valer 10 para que el programa tome como registrado así que volvamos al call a ver como metemos un 10 en EAX

009914A0	-	84C0	TEST AL,AL
009914A2	-	74 07	<del>JMP SHORT ConvertX.009914AB</del>
009914A4	-	B8 03000000	MOV EAX,3
009914A9	-	EB 02	JMP SHORT ConvertX.009914AD
009914AB	>	8BC2	MOV EAX,EDX
009914AD	>	8903	MOV DWORD PTR DS:[EBX],EAX
009914AF	-	33C0	XOR EAX,EAX
009914B1	-	5A	POP EDX
009914B2	-	EB	POP ECX

Bueno menudo lio de líneas hice jajajaja pero analicemos esto “Si 9914A2 NO salta metemos en EAX un 3 luego sigue al JMP que evita 9914AB que mete el valor de EDX en EAX”

o sea que Nopeamos el salto y metemos un 10 en EAX así que los cambios nos quedarían de esta forma

009914A0	-	84C0	TEST AL,AL
009914A2	-	90	NOP
009914A3	-	90	NOP
009914A4	-	B8 10000000	MOV EAX,10
009914A9	-	EB 02	JMP SHORT ConvertX.009914AD
009914AB	>	8BC2	MOV EAX,EDX
009914AD	>	8903	MOV DWORD PTR DS:[EBX],EAX

Bien, volvemos a la CMP que estábamos y teníamos un 5 lo modificamos con un 10 e inhabilitamos los BP y le damos a RUN y el programa arranca sin mostrarnos ningún mensaje de registro vamos al ABOUT



Bueno como ven ya quedo registrado.

Bueno espero que les halla gustado y hasta el próximo TUTE :-D

PD: si guardan los cambios guárdenlos con el mismo nombre del programa ye que genera un error si tiene otro nombre.

Saludos a toda la Lista de CracksLatinos

Daniel – La Calavera

