

Crackslatinos

LEMTWHC / KBR ... S



Ivinson 2012



Software:	Kasparov Chessmate
Versión:	1.0.1.4
Objetivo:	Parchar y eliminar nag
Cracker:	Ivinson
Download:	http://www.mediafire.com/file/rvo3wm23l6wtdq9/Kasparov_Chessmate.rar
Fecha:	12/01/12
Team:	Crackslatinos
Tutorial N°:	4

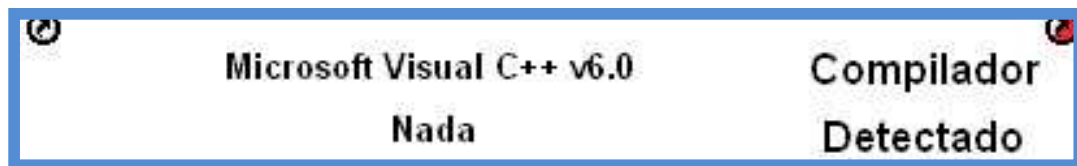
Introducción

Año nuevo, tuto nuevo. Saludos compañeros crackers. Espero que hayan pasado unas excelentes navidades. Aparte del cracking, me gusta jugar ajedrez. Por la web me encontré el software Kasparov Chessmate con un elo máximo de 2300. Claro, también se puede ajustar al nivel que uno se sienta más cómodo.

Acción

¿Estará empacado?

Revisémoslo con RDG Packer Detector v. 0.6.7.

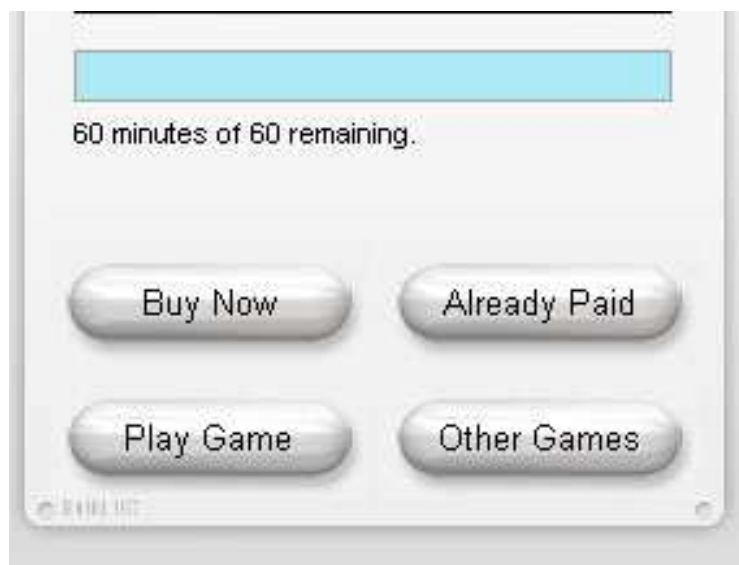


Buena noticia. Cero Packer y es un C++.

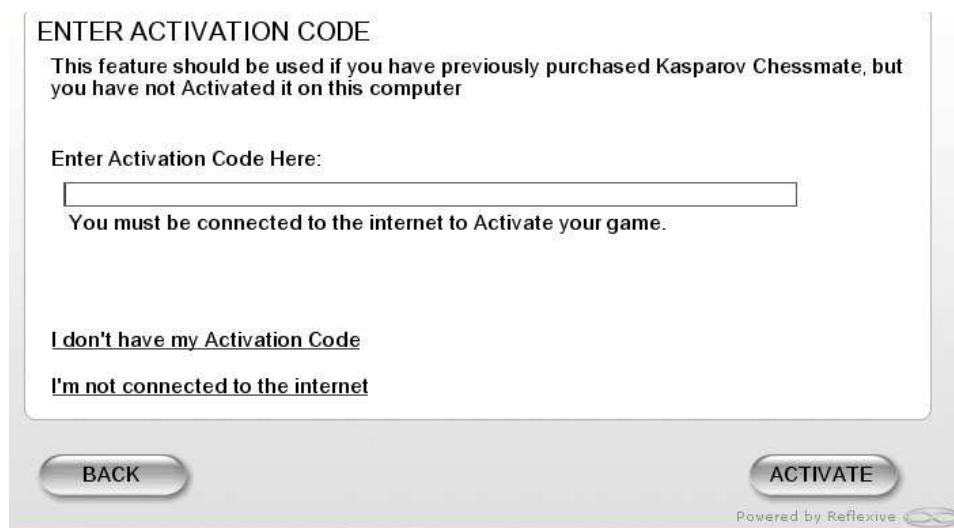
Modo de registro

Al ejecutarlo, nos muestra la pantalla principal y podemos ver en la esquina inferior derecha 4 botones y un timer de 60 minutos.

Botón 1= Comprar ahora. Botón 2= Ya pagado. Botón 3= Jugar.
Botón 4= Otros juegos.



Al presionar el botón 2, nos muestra la siguiente imagen:



Le damos click a, “I’m not connected to the internet” o sea, “Registro offline.”

ENTER UNLOCK CODE

If you have an Activation Code for this game, but this computer is not connected to the internet, you will have to manually get an Unlock Code with a computer that is connected to the internet and enter the new Unlock Code on this page.

Go to the following URL and type in the requested information.

http://arcade.reflexive.com/alreadypaid

Below is the product code for Kasparov Chessmate on this computer

C971-8810-9114-7515-3499-7125

Enter the Unlock Code for this game on this computer here:

BACK

SUBMIT

Después de meter un serial malo, nos muestra el chico malo.

Unrecognized Unlock Code

The code you entered does not appear to be a code that comes from the Reflexive system.

Please check your sales receipt or credit card statement to verify that you purchased this game from Reflexive.

If you require further assistance please contact Reflexive.

[View Contact Information](#)

OK

Bueno, estoy fue solo para los que quieran buscar el serial. Como yo no soy muy bueno buscando seriales, decidí parcharlo.

De todas maneras, da igual porque ni siquiera dice “registrado para: Usuario”.

Manos al Olly

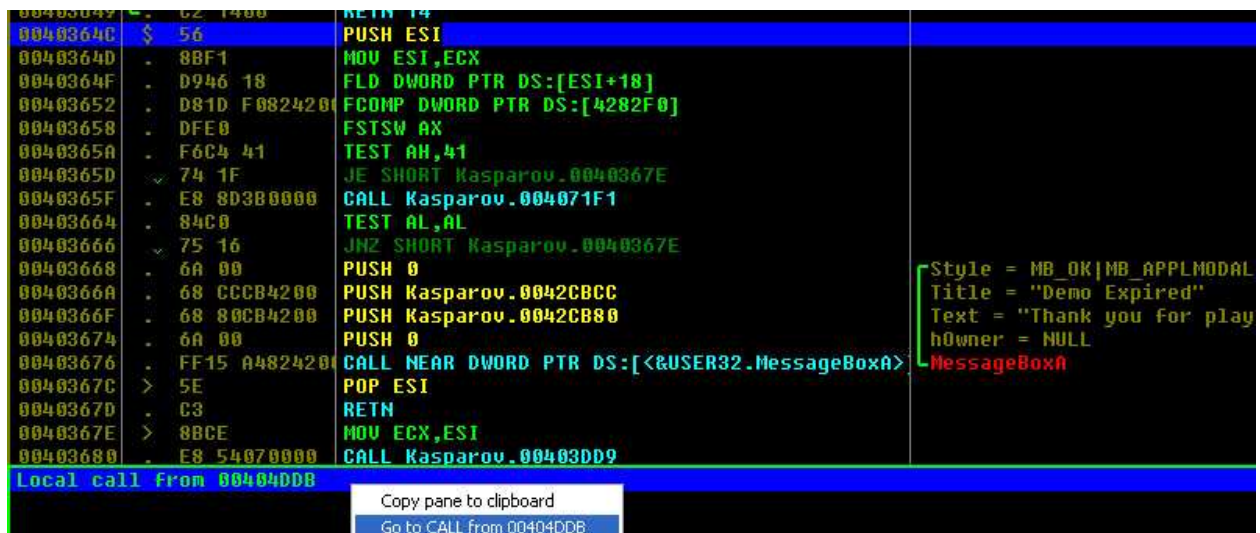
Al abrirlo con Olly, click derecho en el desensamblado y buscamos las “Referenced text strings”.



Y vemos:

```
0040366A PUSH Kasparov.0042CBCC ASCII "Demo Expired"
0040366F PUSH Kasparov.0042CB80 ASCII "Thank you for playing, your demo has expired."
00403712 PUSH Kasparov.0042CC68 ASCII "GameWrapper: Duplicate Thread Failed. Last er
```

Demos doble click a: **0040366A**. “Demo Expired” (La demo expiró)



Vemos un salto condicional en:

0040365D /74 1F **JE SHORT** Kasparov.0040367E

Forcemos ese salto así:

0040365D /EB 1F **JMP SHORT** Kasparov.0040367E

Con esto, así el timer llegue a 0, no caduca nunca, pero no se ve estético. La idea es que arranque de una vez sin mostrar la nag principal.

En la imagen de arriba vemos la ayuda de Olly “\$” que quiere decir de donde es llamada esa rutina. (Ver tuto sobre el Crackme de Cruehead 1 por Ricnar)

0040364C \$ 56 **PUSH ESI**

Seleccionamos (imagen superior) Local call from **0040DDB**, click derecho y Go to CALL from **0040DDB** y caemos en:

00404DD0	>	E8 1C240000	CALL Kasparov.004071F1
00404DD5	.	84C0	TEST AL,AL
00404DD7	✓	74 0E	JE SHORT Kasparov.00404DE7
00404DD9	.	8BCE	MOV ECX,ESI
00404DDB	.	E8 6CE8FFFF	CALL Kasparov.0040364C
00404DE0	.	68 A6474000	PUSH Kasparov.004047A6
00404DE5	✓	EB 1C	JMP SHORT Kasparov.00404E03
00404DE7	>	D946 18	FLD DWORD PTR DS:[ESI+18]
00404DEA	.	D81D F0824200	FCOMP DWORD PTR DS:[4282F0]
00404DF0	.	DFE0	FSTSW AX
00404DF2	.	F6C4 41	TEST AH,41
00404DF5	✓	75 07	JNZ SHORT Kasparov.00404DFE
00404DF7	.	68 353F4000	PUSH Kasparov.00403F35
00404DFC	✓	EB 05	JMP SHORT Kasparov.00404E03
00404DFE	>	68 EF434000	PUSH Kasparov.004043EF
00404E00	>	0005	MOV EBX,ESI

Tenemos un **JE** en:

00404DD7 /74 0E **JE SHORT** Kasparov.00404DE7

Lo nopeamos para que ejecute la CALL:

00404DDB |. E8 6CE8FFFF CALL Kasparov.**0040364C**

Y pase directamente por el JMP del “Demo Expired” y listo. Adiós nag.

Guardamos todos los cambios, cerramos Olly ejecutamos el software:



Gracias por leer.

lpadilla63@gmail.com