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 Nº:	**4**

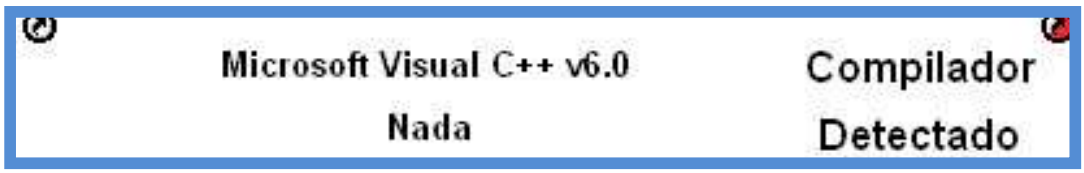
Introducción

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.



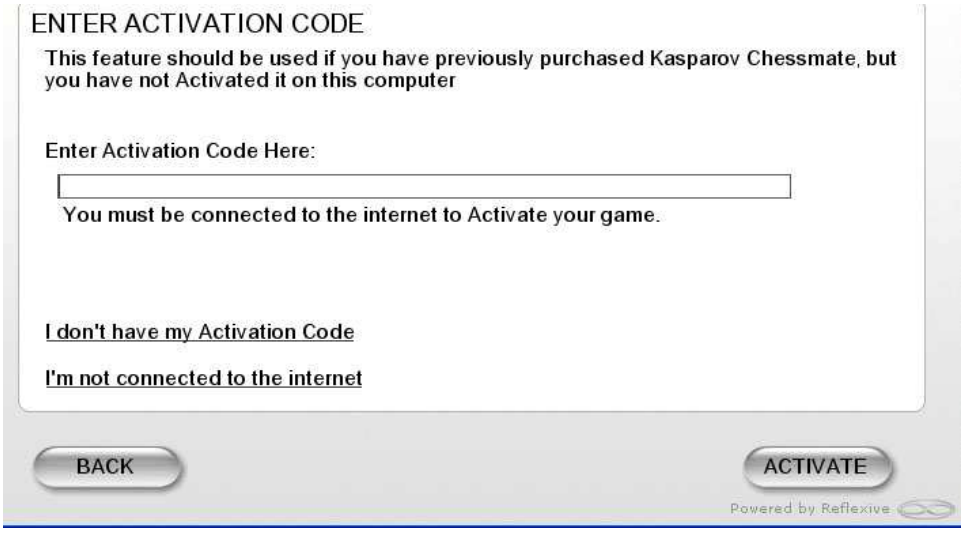
Buena noticia. Cero Packer y es un C++.

Modo de registro

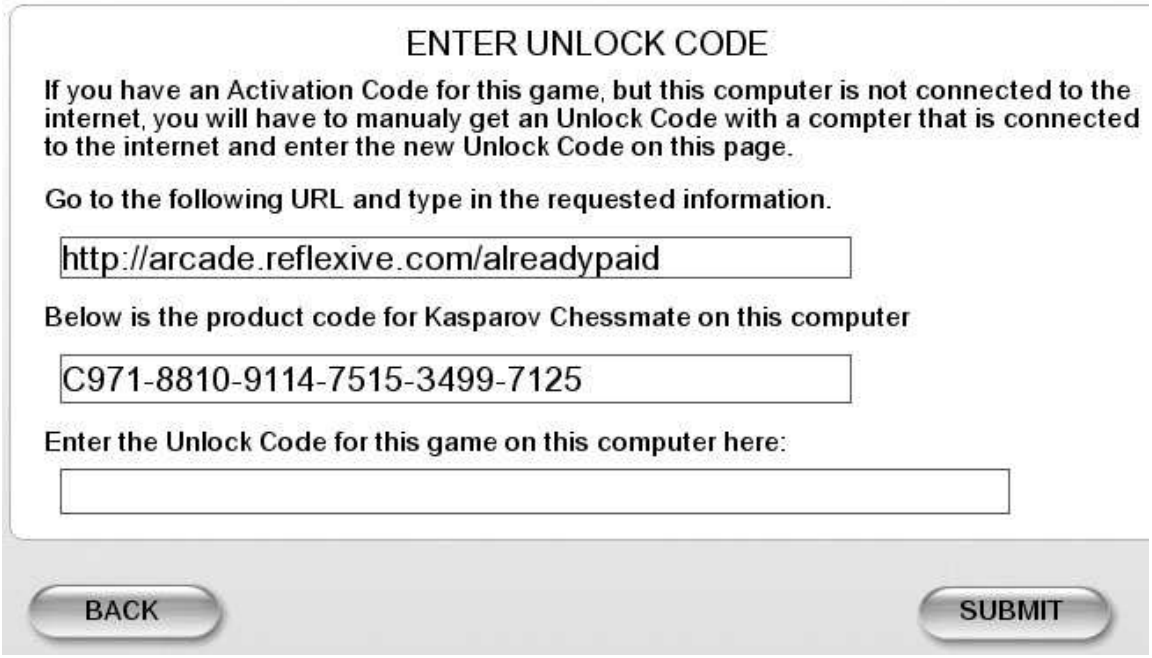
Al ejecutarlo, nos muestra la pantalla principal y podemos ver en la esquina inferior derecha 4 botones y un timer de 60 minutos.

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

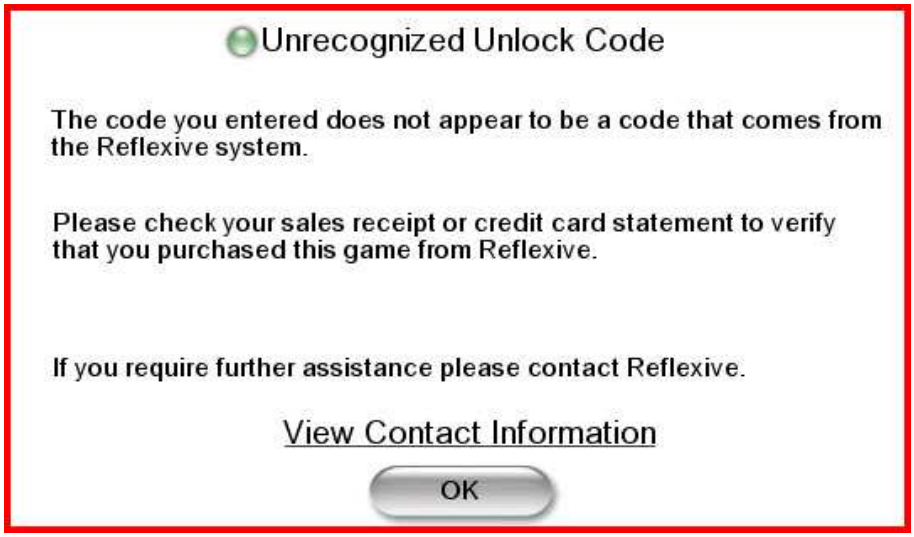
Al presionar el botón 2, nos muestra la siguiente imagen:



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



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

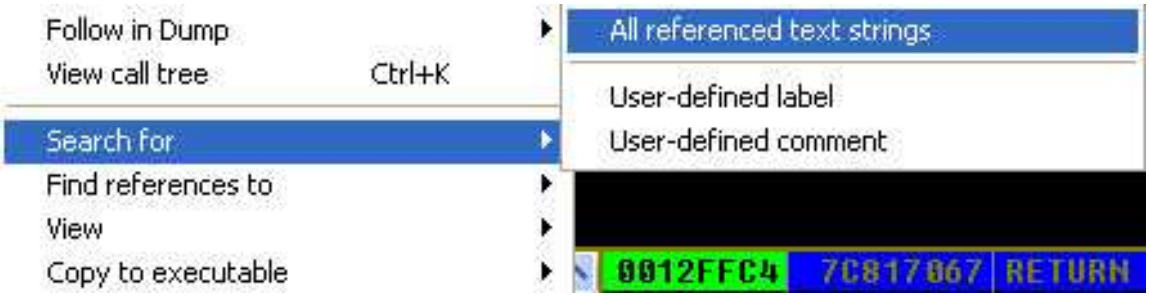


Bueno, estoy fue solo para los que quieran buscar el serial. Como yo no soy muy bueno buscando seriales, decidí parcharlo.

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

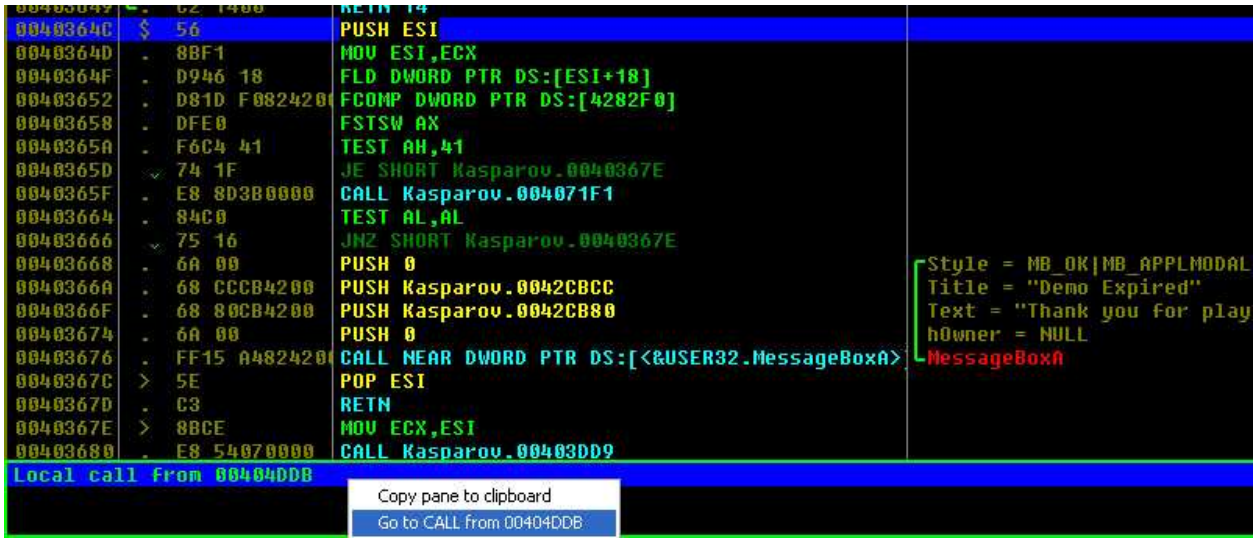
Manos al Olly

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



Y vemos:

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:

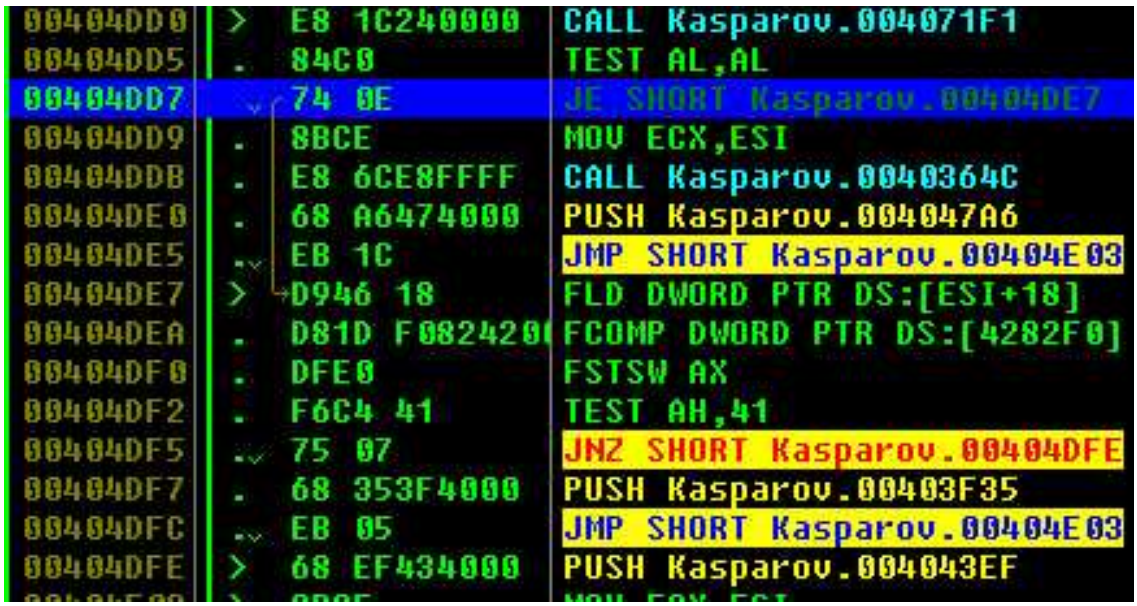
0040365D /EB 1F JMP SHORT Kasparov.0040367E

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:



Tenemos un JE en:

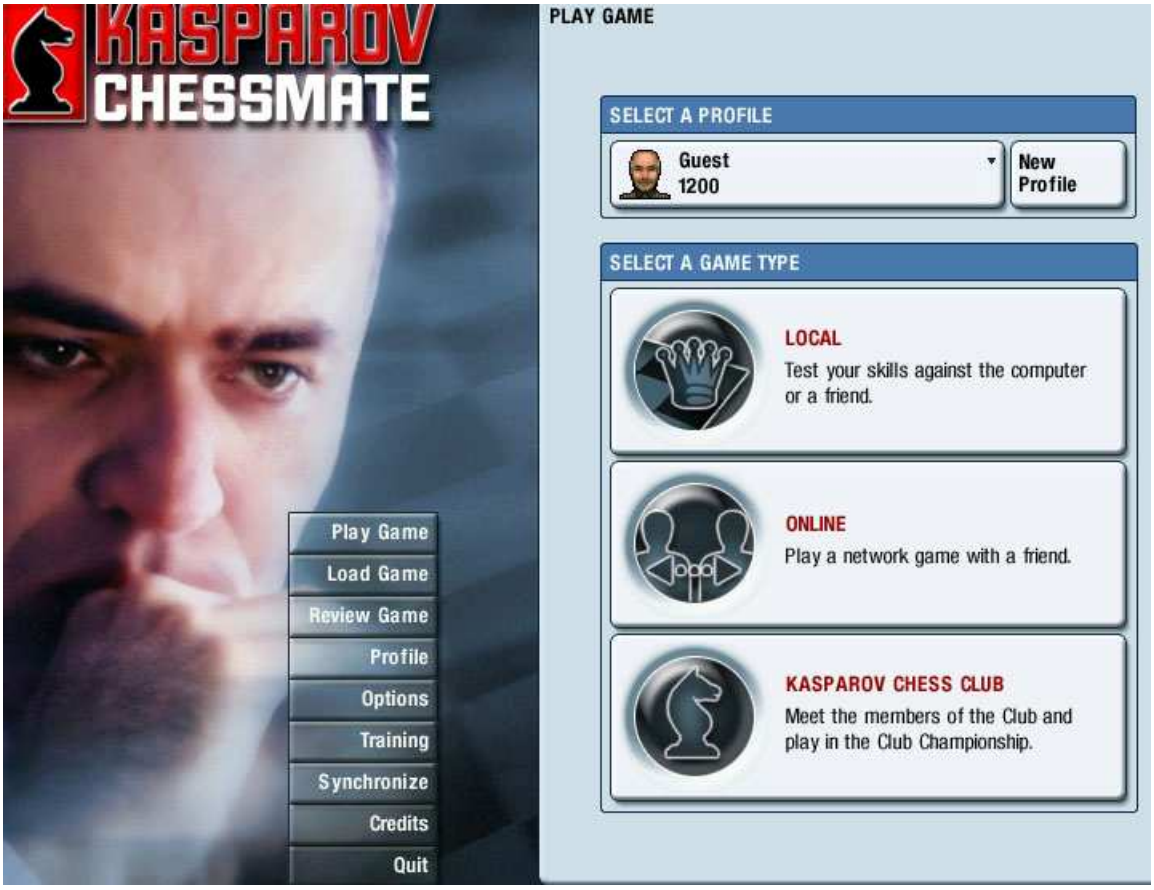
00404DD7 /74 0E JE SHORT Kasparov.00404DE7

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