Tutoriales Ingenieria Inversa por CronuX [2010]
[lhcronux@gmail.com]

INTRODUCCIÓN

Este tutorial está hecho con el único fin de dar a entender y mostrar una experiencia satisfactoria relacionada con el arte de la ingeniería inversa, con lo cual el autor no se hace responsable de la utilidad que se le dé a la información.

Las palabras de un sabio fueron:
"Hace poco me preguntaron por qué me dedicaba al cracking y yo contesté por que jugaba mal al ajedrez, Espero que a vosotros sea también un desafío intelectual y no un sistema para adquirir programas gratis. No os dejéis seducir por el lado oscuro de la fuerza..."

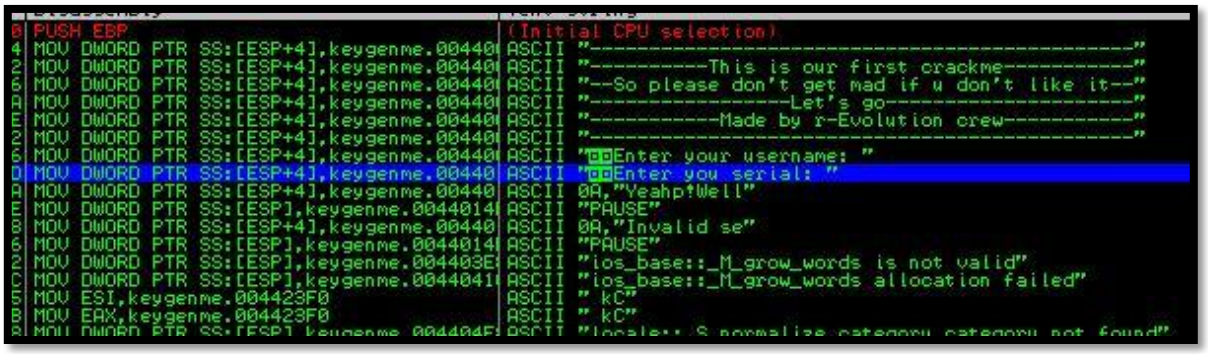
AL ATAQUE

Programa	*keygenme#1.exe*
Compresor/Compilador	*Dev C++ V4.9.9.2*
Dificultad	*Newbie*
Herramientas	*RDG Packer Detector / OllyDBG*
Objetivo	*Keygen*
Reverser/Coder	*CronuX*
Fecha	*Octubre / 2010*

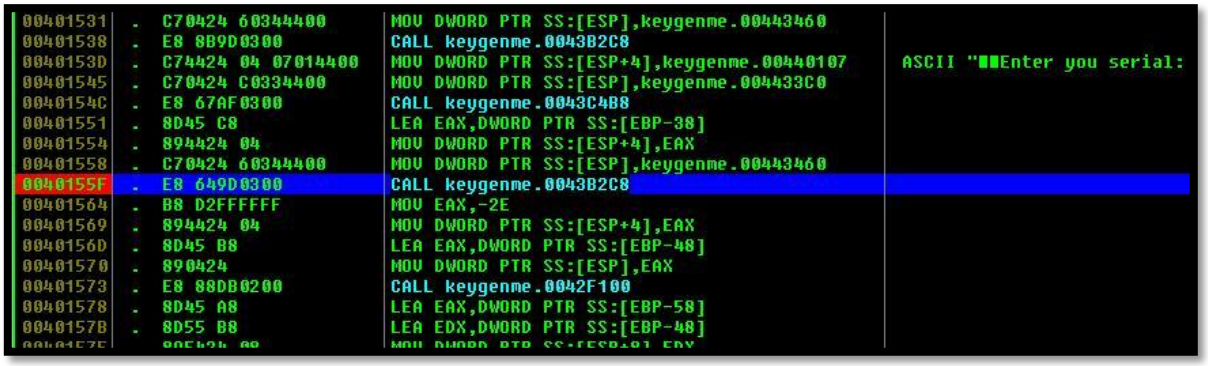
Ejecutamos con el RDG Packer Detector el crackme y así poder saber en qué lenguaje fue programado y que herramientas nos puede facilitar su análisis.

Observamos que está Programado en C++ y no tiene ningún Packer.

Ingresamos unos datos y vemos como nos muestra el mensaje de badboy…



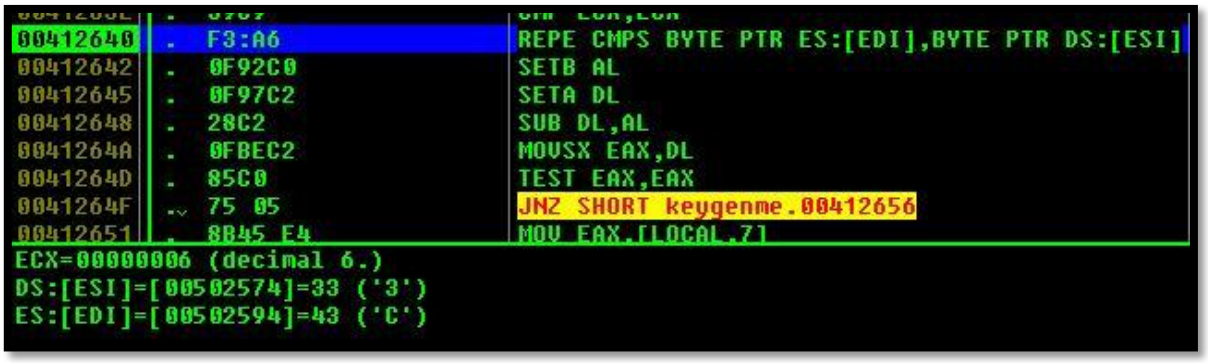
Abrimos el crackme con el OllyDBG y buscaremos entre sus string, Click derecho – Search For – All Referenced Text String…



Estamos en la zona caliente del crackme y pondremos un breakpoint y empezaremos a tracear…

Traceamos hasta llegar a la call 0x4015AB que será donde comparara los dos seriales y moverá un valor a la dirección [EBP-91] que después será comparada para verificar a donde se dirige el salto…

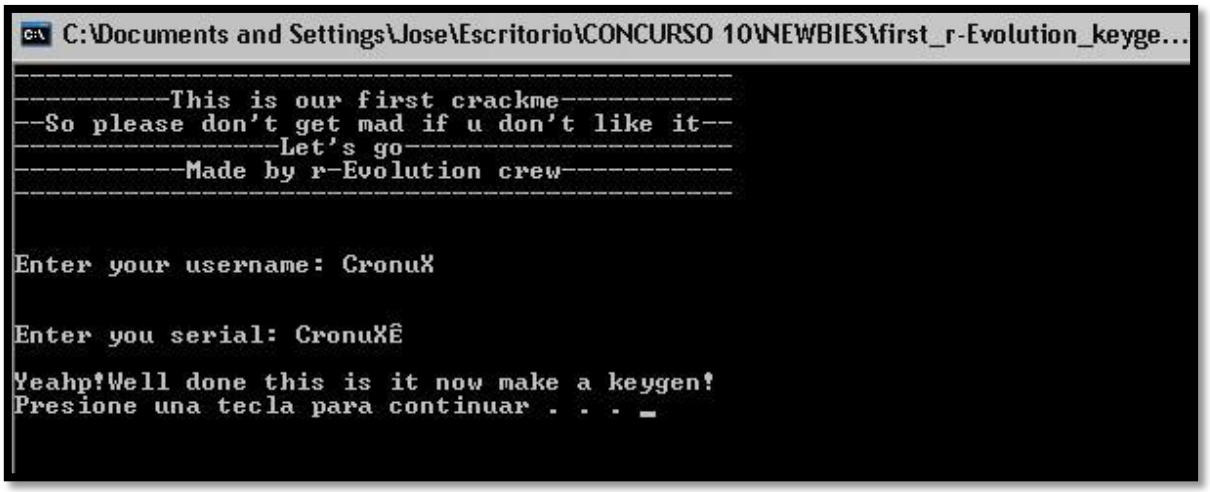
Traceamos hasta la call 0x43C48B donde entraremos con F7…



Allí llegamos hasta donde compara los dos seriales, el verdadero con el ingresado, y con esto vamos a la dirección del Registro EDI que es donde se encuentra en serial valido…

Y podemos observar que el serial es el mismo nombre más el carácter del valor 0xD2 y así con todos los nombres…

Y teniendo conocimiento de cómo se genera el serial valido es la hora de programar un keygen…



Y por último comprobar si estamos en lo correcto y así es y nos muestra el mensaje de goodboy…

Hemos terminado el pequeño análisis de este crackme…

Y otra experiencia más a nuestra mochila de la vida y del aprendizaje…

AGRADECIMIENTOS

A todos que de una u otra manera me han ayudado en este proceso de aprender y sobre todo a ti por tomarte el tiempo de leer esta humilde explicación que espero haya quedado de manera clara y sea de su agrado.

POWERED BY CRONUX™