

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.

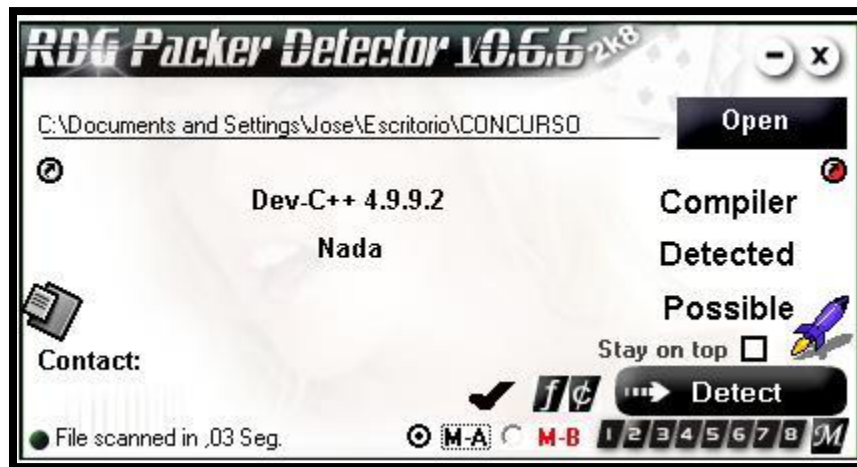
Las palabras de un sabio fueron:

"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.

```
C:\Documents and Settings\Jose\Escritorio\CONCURSO 10\NEWBIES\first_r-Evolution
-----This is our first crackme-----
--So please don't get mad if u don't like it--
-----Let's go-----
-----Made by r-Evolution crew-----

Enter your username: CronuX

Enter you serial: 342210

Invalid serial!Come on you'll solve it i am sure..... :P
Presione una tecla para continuar . . . _
```

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

```

0 PUSH EBP
4 MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "(Initial CPU selection)"
2 MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "-----"
6 MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "--This is our first crackme-----"
A MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "--So please don't get mad if u don't like it--"
E MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "-----Let's go-----"
2 MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "-----Made by r-Evolution crew-----"
6 MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "-----"
0 MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "██Enter your username: "
4 MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "██Enter your serial: "
A MOV DWORD PTR SS:[ESP+4],keygenme.004440 ASCII "██"
E MOV DWORD PTR SS:[ESP],keygenme.0044014 ASCII "██, "Yeah?Well"
8 MOV DWORD PTR SS:[ESP+4],keygenme.0044014 ASCII "PAUSE"
6 MOV DWORD PTR SS:[ESP],keygenme.0044014 ASCII "██, "Invalid se"
2 MOV DWORD PTR SS:[ESP],keygenme.004403E ASCII "PAUSE"
C MOV DWORD PTR SS:[ESP],keygenme.0044041 ASCII "ios_base::_M_grow_words is not valid"
5 MOV DWORD PTR SS:[ESP],keygenme.0044041 ASCII "ios_base::_M_grow_words allocation failed"
B MOV ESI,keygenme.004423F0 ASCII " kC"
8 MOV EAX,keygenme.004423F0 ASCII " kC"
0 MOV DWORD PTR SS:[ESP],keygenme.004404F ASCII "locale::_S_normalize_category: category not found"

```

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

00401531	- C70424 6034400	MOV DWORD PTR SS:[ESP],keygenme.00443460	
00401538	- E8 8B9D0300	CALL keygenme.0043B2C8	
0040153D	- C74424 04 07014400	MOV DWORD PTR SS:[ESP+4],keygenme.00440107	ASCII "██Enter you serial:
00401545	- C70424 C0334400	MOV DWORD PTR SS:[ESP],keygenme.004433C0	
0040154C	- E8 67AF0300	CALL keygenme.0043C488	
00401551	- 8D45 C8	LEA EAX,DWORD PTR SS:[EBP-38]	
00401554	- 894424 04	MOV DWORD PTR SS:[ESP+4],EAX	
00401558	- C70424 60344400	MOV DWORD PTR SS:[ESP],keygenme.00443460	
0040155F	- E8 649D0300	CALL keygenme.0043B2C8	
00401564	- B8 D2FFFFFF	MOV EAX,-2E	
00401569	- 894424 04	MOV DWORD PTR SS:[ESP+4],EAX	
0040156D	- 8D45 B8	LEA EAX,DWORD PTR SS:[EBP-48]	
00401570	- 890424	MOV DWORD PTR SS:[ESP],EAX	
00401573	- E8 88D80200	CALL keygenme.0042F100	
00401578	- 8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	
0040157B	- 8D55 B8	LEA EDX,DWORD PTR SS:[EBP-48]	

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

0040159E	- 890424	MOV DWORD PTR SS:[ESP],EAX
004015A1	- C785 78FFFFFF 010000	MOV DWORD PTR SS:[EBP-88],1
004015A8	- E8 C8AE0300	CALL keygenme.0043C478
004015B0	- 8885 6FFFFFFF	MOV BYTE PTR SS:[EBP-91],AL
004015B6	- EB 74	JMP SHORT keygenme.0040162C
004015B8	- 8D6D 18	LEA EBP,DWORD PTR SS:[EBP+18]

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...

0043C488	- 890424	MOV DWORD PTR SS:[ESP],EAX
0043C48B	- E8 7061FDFF	CALL keygenme.00412600
0043C490	- 8945 FC	MOV [LOCAL.1],EAX
0043C493	- 837D FC 00	CMP [LOCAL.1],0
0043C497	- 0F94C0	SETE AL
0043C49A	- 0FB6C0	MOVZX EAX,AL
0043C49D	- 8945 FC	MOV [LOCAL.1],EAX

Traceamos hasta la call 0x43C48B donde entraremos con F7...

```

00412640 - F3:A6 REPE CMPS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
00412642 - 0F92C0 SETB AL
00412645 - 0F97C2 SETA DL
00412648 - 28C2 SUB DL,AL
0041264A - 0FBEC2 MOVSX EAX,DL
0041264D - 85C0 TEST EAX,EAX
0041264F - 75 05 JNZ SHORT keygenme.00412656
00412651 - 8B45 E4 MOV EAX,[LOCAL_7]
ECX=00000006 (decimal 6.)
DS:[ESI]=[00502574]=33 ('3')
ES:[EDI]=[00502594]=43 ('C')

```

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...

Hex dump	ASCII
43 72 6F 6E 75 58 D2 00 70 68 69 37 41 00 04 00	CronuX0.
20 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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...

```
ca C:\Documents and Settings\Jose\Escritorio\CONCURSO 10\NEWBIES\first_r-Evolution_keyge...
-----
--This is our first crackme--
--So please don't get mad if u don't like it--
--Let's go--
--Made by r-Evolution crew--
-----

Enter your username: CronuX

Enter you serial: CronuX

Yeahp!Well done this is it now make a keygen!
Presione una tecla para continuar . . . _
```

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...

