

# Keygen para el CrackmeMe#02 de LaFarge

KeyGen por injerto

# ÍNDICE

1.	Introducción .....	2
2.	Injerto Light .....	2
3.	KeyGen a partir de la víctima .....	3
4.	Notas finales.....	5
5.	Enlaces .....	5
6.	Crackeando Crackmes by deurus.....	5

*Equipo utilizado:*

*S.O: Windows 7 x32 /Windows 8 x64*

*Depurador: Ollydbg 1.10 (32bits) con plugins*

*Analizador: PEiD 0.95*

## 1. Introducción

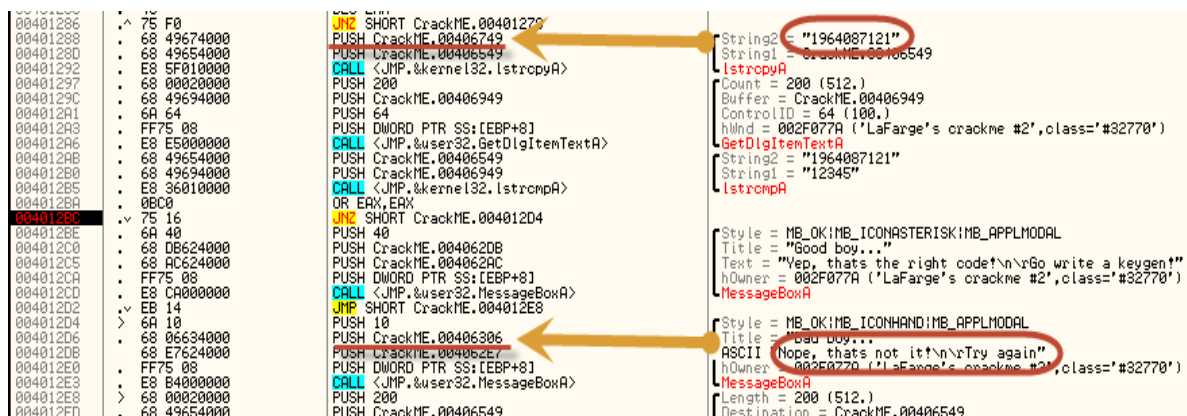
Hoy vamos a hacer algo diferente, vamos a hacer un **keygen con la propia víctima**. El término anglosajón para esto es “**selfkeygening**” y no es que esté muy bien visto por los reversers pero a veces nos puede sacar de apuros.

La víctima elegida es el **Crackme 2 de LaFarge**. Está hecho en ensamblador.

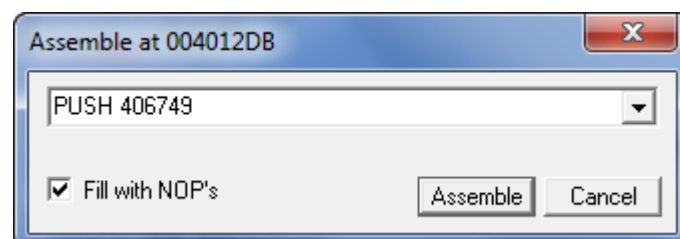
## 2. Injerto Light

Primeramente vamos a realizar un injerto light, con esto quiero decir que vamos a **mostrar el serial bueno en la MessageBox de error**.

Abrimos **Ollly** y localizamos el código de comprobación del serial, tenemos suerte ya que el serial se muestra completamente y no se comprueba byte a byte ni cosas raras. En la imagen inferior os muestro el serial bueno para el nombre deurus y el mensaje de error. Como podeis observar el **serial bueno** se saca de memoria con la instrucción **PUSH 406749** y el mensaje de error con **PUSH 406306**.



Si cambiamos el PUSH del serial por el de el mensaje de error ya lo tendríamos. Nos situamos encima del **PUSH 406306** y pulsamos **espacio**, nos saldrá un diálogo con el push, lo modificamos y le damos a **Assemble**.



Ahora el crackme cada vez que le demos a **Check it!** nos mostrará:



### 3. KeyGen a partir de la víctima

Pero no nos vamos a quedar ahí. Lo interesante sería que el serial bueno lo mostrara en la caja de texto del serial. Esto lo vamos a hacer con la función **user32.SetDlgItemTextA**.

The **SetDlgItemText** function sets the title or text of a control in a dialog box.

```
BOOL SetDlgItemText(  
    HWND hDlg,           // handle of dialog box  
    int nIDDlgItem,      // identifier of control  
    LPCTSTR lpString     // text to set  
);
```

**Parameters**

*hDlg*  
Identifies the dialog box that contains the control.

*nIDDlgItem*  
Identifies the control with a title or text that is to be set.

*lpString*  
Points to the null-terminated string that contains the text to be copied to the control.

Según dice la función **necesitamos** el **handle de la ventana**, el **ID de la caja de texto** y el **string a mostrar**. La primera y segunda la obtenemos fijándonos en la función **GetDlgItemTextA** que recoge el serial introducido por nosotros. La string es el **PUSH 406749**.

00401297	68 00020000	PUSH 200	MaxCount = 512.
0040129C	68 49694000	PUSH 00406949	String = "12345"
004012A1	6A 64	PUSH 64	ItemID = 100.
004012A3	FF75 08	PUSH DWORD PTR SS:[EBP+8]	hDialog
004012A6	E8 E5000000	CALL <a href="#">JMP.&lt;user32.GetDlgItemTextA&gt;</a>	USER32.GetDlgItemTextA

Con esto ya tenemos todo lo que necesitamos excepto el espacio dentro del código, en este caso lo lógico es parchear las MessageBox de error y acierto. Las seleccionamos, click derecho y **Edit > Fill with NOPs**.

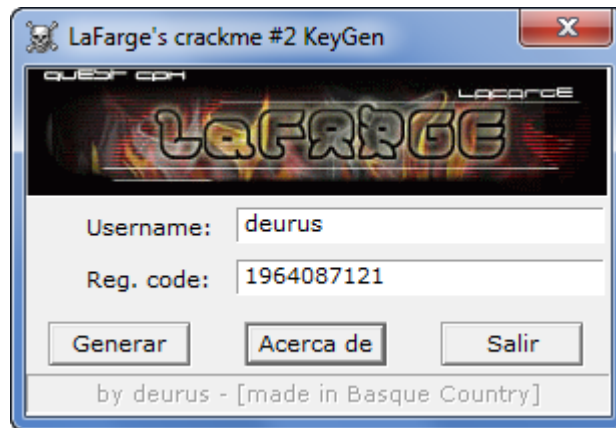
004012B5	• 68 49674000	PUSH CrackME.00406749	Style = MB_OK MB_ICONASTERISK MB_APPLMODAL
004012B6	• E8 36010000	CALL <JMP.&kernel32.istrongA>	Title = "Good boy..."
004012B7	• 90	OR EAX, EAX	Text = "Yep, thats the right code!\n\nGo write a keygen!"
004012B8	• 75 16	JNZ SHORT CrackME.004012D4	hOwner = 7FFD9000
004012B9	• 6A 40	PUSH 40	MessageBoxA
004012BA	• 68 DB624000	PUSH CrackME.004062DB	Style = MB_OK MB_ICONHAND MB_APPLMODAL
004012BB	• 68 AC624000	PUSH CrackME.004062AC	Title = "Bad boy..."
004012BC	• FF75 08	PUSH DWORD PTR SS:[EBP+8]	Text = "Nope, thats not it!\n\nTry again"
004012BD	• E8 CA000000	CALL <JMP.&user32.MessageBoxA>	hOwner = 7FFD9000
004012BE	• EB 14	JMP SHORT CrackME.004012E8	MessageBoxA
004012BF	• 6A 10	PUSH 10	Style = MB_OK MB_ICONHAND MB_APPLMODAL
004012C0	• 68 06634000	PUSH CrackME.00406306	Title = "Bad boy..."
004012C1	• 68 E7624000	PUSH CrackME.004062E7	Text = "Nope, thats not it!\n\nTry again"
004012C2	• FF75 08	PUSH DWORD PTR SS:[EBP+8]	hOwner = 7FFD9000
004012C3	• E8 64000000	CALL <JMP.&user32.MessageBoxA>	MessageBoxA
004012C4	• 75 08	JNZ SHORT CrackME.004012E8	Length = 200 (512.)
004012C5	• 68 00020000	PUSH 200	MessageBoxA
004012C6	• 75 08	JNZ SHORT CrackME.004012E8	Length = 200 (512.)

004012B5	• E8 36010000	CALL <JMP.&kernel32.istrongA>	istrongA
004012B6	• 90	NOP	
004012B7	• 90	NOP	
004012B8	• 90	NOP	
004012B9	• 90	NOP	
004012BA	• 90	NOP	rStyle
004012BB	• 90	NOP	Title
004012BC	• 90	NOP	
004012BD	• 90	NOP	Text
004012BE	• 90	NOP	
004012BF	• 90	NOP	
004012C0	• 90	NOP	hOwner
004012C1	• 90	NOP	
004012C2	• 90	NOP	MessageBoxA
004012C3	• 90	NOP	
004012C4	• 90	NOP	
004012C5	• 90	NOP	
004012C6	• 90	NOP	rStyle
004012C7	• 90	NOP	Title
004012C8	• 90	NOP	
004012C9	• 90	NOP	Text
004012CA	• 90	NOP	
004012CB	• 90	NOP	hOwner
004012CC	• 90	NOP	MessageBoxA
004012CD	• 90	NOP	
004012CE	• 90	NOP	
004012CF	• 90	NOP	
004012D0	• 90	NOP	
004012D1	• 90	NOP	
004012D2	• 90	NOP	
004012D3	• 90	NOP	rStyle
004012D4	• 90	NOP	Title
004012D5	• 90	NOP	
004012D6	• 90	NOP	Text
004012D7	• 90	NOP	
004012D8	• 90	NOP	hOwner
004012D9	• 90	NOP	MessageBoxA
004012DA	• 90	NOP	
004012DB	• 90	NOP	
004012DC	• 90	NOP	
004012DD	• 90	NOP	
004012DE	• 90	NOP	
004012DF	• 90	NOP	
004012E0	• 90	NOP	
004012E1	• 90	NOP	
004012E2	• 90	NOP	
004012E3	• 90	NOP	
004012E4	• 90	NOP	
004012E5	• 90	NOP	
004012E6	• 90	NOP	
004012E7	• 90	NOP	
004012E8	• 68 00020000	PUSH 200	Length = 200 (512.)
004012E9	• 75 08	JNZ SHORT CrackME.004012E8	Length = 200 (512.)

Ahora escribimos el injerto.

004012B8	• 90	NOP	
004012B9	• 90	NOP	
004012BA	• 68 49674000	PUSH CrackME.00406749	Text = ""
004012BB	• 6A 64	PUSH 64	ControlID = 64 (100.)
004012BC	• FF75 08	PUSH DWORD PTR SS:[EBP+8]	hWnd = 7FFD0000
004012BD	• E8 AE5D0D75	CALL user32.SetDlgItemTextA	SetDlgItemTextA
004012BE	• 90	NOP	
004012BF	• 90	NOP	

Finalmente con **Resource Hack** cambiamos el aspecto del programa para que quede más profesional y listo. Tenemos pendiente hacer el keygen puro y duro, venga agur.



## 4. Notas finales

He probado el keygen en varios sistemas y **solo funciona en versiones de 32 bits**, en las de 64 bits da error y se cierra.

## 5. Enlaces

- Crackme
- Keygen + Injertos
- Entrada en el blog

## 6. Crackeando Crackmes by deurus

- [https://deurus.info/archivos/crackmes/CrackME2\\_LaFarge.rar](https://deurus.info/archivos/crackmes/CrackME2_LaFarge.rar)
- [https://deurus.info/archivos/keygens/Lafarge\\_crackme2\\_injerto\\_keygen\\_deurus.rar](https://deurus.info/archivos/keygens/Lafarge_crackme2_injerto_keygen_deurus.rar)