Keygen para el CrackmeMe#02 de LaFarge

KeyGen por injerto

By deurus
14/09/2014

ÍNDICE

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.

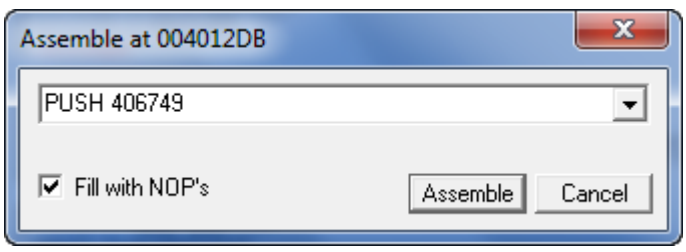
La víctima elegida es el **Crackme 2 de LaFarge**. Está hecho en ensamblador.

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 **Olly** 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 tendriámos. 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
 );
```

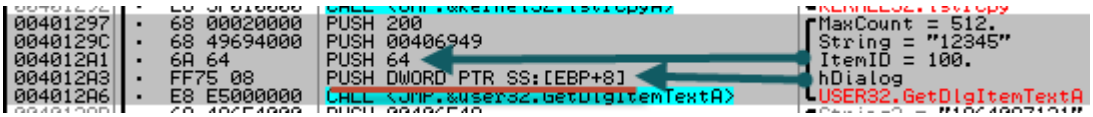
Parameters

hDlg
Identifies the dialog box that contains the control.

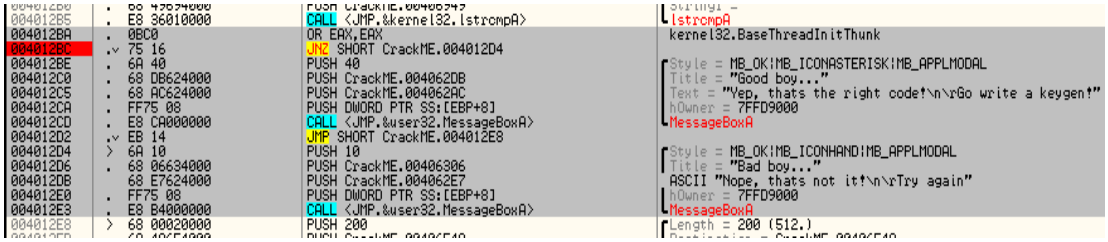
nIDDlgItem
Identifies the control with a title or text that is to be set.

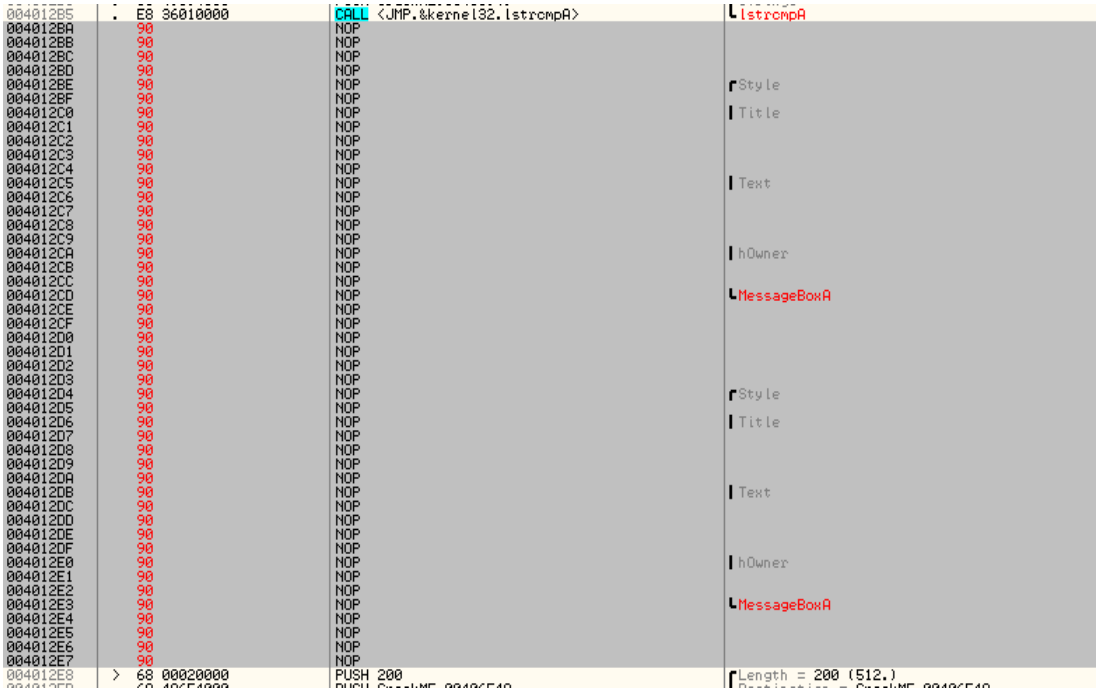
lpString
Points to the null-terminated string that contains the text to be copied to the control.

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 recoje el serial introducido por nosotros. La string es el **PUSH 406749**.

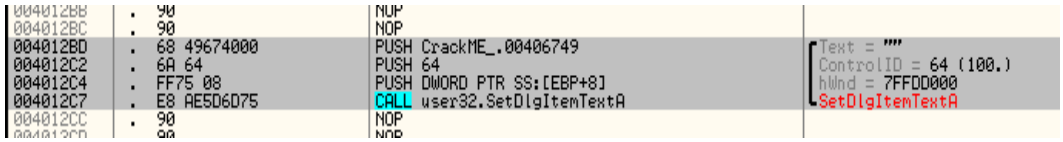


Con esto ya tenemos todo lo que necesitamos excepto el espacio dentro del código, en este caso lo lógico es parchear las MessageBox de error y acierto. Las seleccionamos, click derecho y **Edit > Fill with NOPs**.

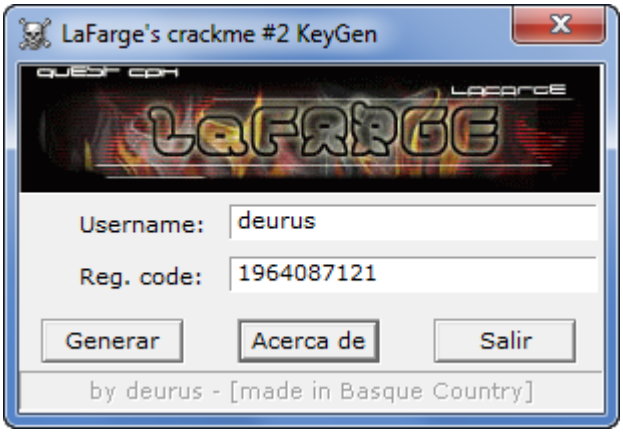




Ahora escribimos el injerto.



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/keygens/Lafarge_crackme2_injerto_keygen_deurus.rar