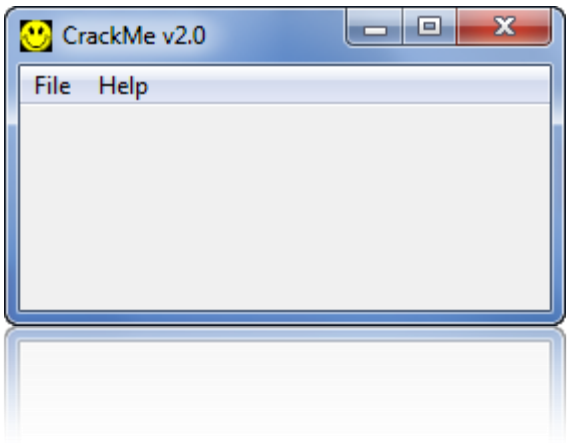
Solución para el CrackMe#2 de Cruehead

eXORcism



By deurus
08/09/2014

ÍNDICE

Equipo utilizado:

S.O: Windows 7 x32 /Windows 8 x64

Depurador: Ollydbg 1.10 (32bits) con plugins

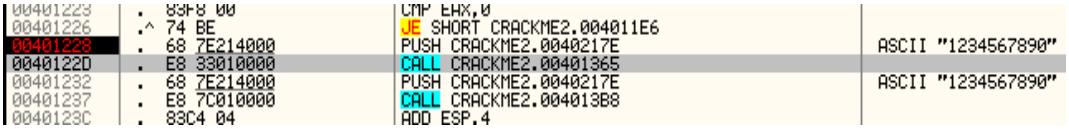
Analizador: PEiD 0.95

1. Introducción

Continuamos con la segunda entrega de **Cruehead**. En este caso nos encontramos con un único campo de contraseña para introducir.

2. El algoritmo

Abrimos con Olly y vemos dos saltos. El primer Call realiza una serie de operaciones con el serial introducido y el segundo comprueba si el serial es correcto.



A continuación llegamos aquí:

```
/$  C605 18214000 00        MOV BYTE PTR DS:[402118],0
|.  8B7424 04               MOV ESI,DWORD PTR SS:[ESP+4]
|.  56                      PUSH ESI
|>  8A06                    /MOV AL,BYTE PTR DS:[ESI]      ; <---
|.  84C0                    |TEST AL,AL
|.  74 19                   |JE SHORT CRACKME2.00401390
|.  FE05 18214000           |INC BYTE PTR DS:[402118]
|.  3C 41                   |CMP AL,41                     ; 41 = A
|.  72 04                   |JB SHORT CRACKME2.00401385    ; ya es mayúscula
|.  3C 5A                   |CMP AL,5A                     ; 5A = Z
|.  73 03                   |JNB SHORT CRACKME2.00401388   ; Convertir a mayúscula
|>  46                      |INC ESI
|.^ EB E9                   |JMP SHORT CRACKME2.00401371   ; Bucle -->
|>  E8 25000000             |CALL CRACKME2.004013B2
|.  46                      |INC ESI
|.^ EB E1                   \JMP SHORT CRACKME2.00401371
|>  5E                      POP ESI
|.  E8 03000000             CALL CRACKME2.00401399         ;Convertido a mayúsculas continuamos
|.  EB 00                   JMP SHORT CRACKME2.00401398
\>  C3                      RETN
```

Si nuestro serial contiene solo letras, las convierte a mayúsculas y seguimos aquí. En resumen hace **XOR byte a byte** entre nuestro serial y la frase "**Messing_in_bytes**"

```
/$  33DB                    XOR EBX,EBX
|.  33FF                    XOR EDI,EDI
|>  8A8F A3214000           /MOV CL,BYTE PTR DS:[EDI+4021A3]  ; Carga el primer byte de 4021A3
|.  8A1E                    |MOV BL,BYTE PTR DS:[ESI]         ;
|.  84DB                    |TEST BL,BL
|.  74 08                   |JE SHORT CRACKME2.004013B1
|.  32D9                    |XOR BL,CL                        ; byteSerial XOR Byte"Messing_in..."
|.  881E                    |MOV BYTE PTR DS:[ESI],BL
|.  46                      |INC ESI                          ;Siguiente byte de "Messing_in_bytes"
|.  47                      |INC EDI                          ;Siguiente byte del serial
|.^ EB EC                   \JMP SHORT CRACKME2.0040139D
\>  C3                      RETN                            ;XOR finalizado volvemos
```

Estado del **DUMP** (memoria) **antes del XOR** y con nuestro serial (12345678) cargado.

```
00402118  00 47 6F 6F 64 20 77 6F 72 6B 21 00 47 72 65 61  .Good work!.Grea
00402128  74 20 77 6F 72 6B 2C 20 6D 61 74 65 21 0D 4E 6F  t work, mate!.No
00402138  77 20 74 72 79 20 74 68 65 20 6E 65 78 74 20 43  w try the next C
00402148  72 61 63 6B 4D 65 21 00 1F 2C 37 36 3B 3D 28 19  rackMe!.,76;=(
00402158  3D 26 1A 31 2D 3B 37 3E 4E 6F 20 6C 75 63 6B 21  =&1-;7>No luck!
00402168  00 4E 6F 20 6C 75 63 6B 20 74 68 65 72 65 2C 20  .No luck there,
00402178  6D 61 74 65 21 00 31 32 33 34 35 36 37 38 39 00  mate!.123456789.
00402188  00 00 00 00 00 00 00 00 00 00 54 72 79 20 74 6F  ..........Try to
00402198  20 63 72 61 63 6B 20 6D 65 21 00 4D 65 73 73 69   crack me!.Messi
004021A8  6E 67 5F 69 6E 5F 62 79 74 65 73 00 00 00 00 00  ng_in_bytes.....
```

Estado del **DUMP después del XOR**.

```
00402118  0A 47 6F 6F 64 20 77 6F 72 6B 21 00 47 72 65 61  .Good work!.Grea
00402128  74 20 77 6F 72 6B 2C 20 6D 61 74 65 21 0D 4E 6F  t work, mate!.No
00402138  77 20 74 72 79 20 74 68 65 20 6E 65 78 74 20 43  w try the next C
00402148  72 61 63 6B 4D 65 21 00 1F 2C 37 36 3B 3D 28 19  rackMe!.,76;=(
00402158  3D 26 1A 31 2D 3B 37 3E 4E 6F 20 6C 75 63 6B 21  =&1-;7>No luck!
00402168  00 4E 6F 20 6C 75 63 6B 20 74 68 65 72 65 2C 20  .No luck there,
00402178  6D 61 74 65 21 00 7C 57 40 47 5C 58 50 67 50 5E  mate!.|W@G\XPgP^
00402188  00 00 00 00 00 00 00 00 00 00 54 72 79 20 74 6F  ..........Try to
00402198  20 63 72 61 63 6B 20 6D 65 21 00 4D 65 73 73 69   crack me!.Messi
004021A8  6E 67 5F 69 6E 5F 62 79 74 65 73                ng_in_bytes
```

A continuación comprueba nuestro serial XOReado con los bytes en memoria.

```
/$  33FF                    XOR EDI,EDI
|.  33C9                    XOR ECX,ECX
|.  8A0D 18214000           MOV CL,BYTE PTR DS:[402118]
|.  8B7424 04               MOV ESI,DWORD PTR SS:[ESP+4]              ; APUNTA AL DUMP 40217E
|.  BF 50214000             MOV EDI,CRACKME2.00402150                 ; APUNTA AL DUMP 402150
|.  F3:A6                   REPE CMPS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]   ; VER NOTA**
\.  C3                      RETN
```

Nota**

Si buscamos el comando **REPE** encontramos que si el flag Z = 1 el bucle se corta y que trabaja con bytes. El problema es que en Olly la instrucción REPE nosotros la vemos con un solo paso y nos puede pasar desapercibida.

En resumen, está comprobando los bytes de las direcciones 402150 (**1F 2C 37 36 3B 3D 28 19 3D 26 1A 31 2D 3B 37 3E)** con nuestro **serial XOReado,** 40217E en adelante, por lo que si hacemos XOR entre los bytes de 402150 y la frase "**Messing_in_bytes**" obtendremos la clave correcta.

Aquí podemos ver el **DUMP** en detalle. En **verde** nuestro serial xoreado, en **morado** los bytes de “Messing_in_bytes” y en **negro** los bytes “mágicos”.

```
00402118  0A 47 6F 6F 64 20 77 6F 72 6B 21 00 47 72 65 61  .Good work!.Grea
00402128  74 20 77 6F 72 6B 2C 20 6D 61 74 65 21 0D 4E 6F  t work, mate!.No
00402138  77 20 74 72 79 20 74 68 65 20 6E 65 78 74 20 43  w try the next C
00402148  72 61 63 6B 4D 65 21 00 1F 2C 37 36 3B 3D 28 19  rackMe!.,76;=(
00402158  3D 26 1A 31 2D 3B 37 3E 4E 6F 20 6C 75 63 6B 21  =&1-;7>No luck!
00402168  00 4E 6F 20 6C 75 63 6B 20 74 68 65 72 65 2C 20  .No luck there,
00402178  6D 61 74 65 21 00 7C 57 40 47 5C 58 50 67 50 5E  mate!.|W@G\XPgP^
00402188  00 00 00 00 00 00 00 00 00 00 54 72 79 20 74 6F  ..........Try to
00402198  20 63 72 61 63 6B 20 6D 65 21 00 4D 65 73 73 69   crack me!.Messi
004021A8  6E 67 5F 69 6E 5F 62 79 74 65 73                ng_in_bytes
```

```
M  e  s  s  i  n  g  _  i  n  _  b  y  t  e  s
4D 65 73 73 69 6E 67 5F 69 6E 5F 62 79 74 65 73
                                              XOR
1F 2C 37 36 3B 3D 28 19 3D 26 1A 31 2D 3B 37 3E
-----------------------------------------------
52 49 44 45 52 53 4F 46 54 48 45 53 54 4F 52 4D
R  I  D  E  R  S  O  F  T  H  E  S  T  O  R  M

Serial: RIDERSOFTHESTORM
```

3. Enlaces

- Crackme
- Cruehead’s Crackme 1.0 Keygen [1/3]
- Cruehead’s Crackme 3.0 Keygen [3/3]

4. Crackeando Crackmes by deurus

- https://mega.co.nz/#F!88BRwYoT!O0TzTSZYCdczKLOrfrOyGw
- Lolabits.es/blogcracking (Clave: **blogcrackhack**)