CodeEngn Challenges: Basic 05

대구대학교 정보보호영재교육원 고등전문B 문성훈

2017년 07월 19일 작성

Challenges : Basic 05

Author: Acid Bytes [CFF]

Korean:

이 프로그램의 등록키는 무엇인가

English:

The registration key of this program is?

Download

```
UPA I: 004436D0
                               UU 2024610911,
UPX1:00443CD0
                               dd 462C0EE9h,
UPX1:00443CD0
                               dd 0D2D0F7BDf
UPX1:00443CD0
                               dd 0C5F0BF24t
UPX1:00443CD0
                               dd 0BA400900t
UPX1:00443CD0
                               dd 4164658Ah,
UPX1:00443CD0
                               dd 9210B141h,
UPX1:00443CD0
                               dd 58AF0B1Ah,
UPX1:00443CD0
                               dd 0A0DEC47h,
UPX1:00443CD0
                               dd 7FB0E40Eh,
UPX1:00443CD0
                               dd 20E40E4Dh,
UPX1:00443CD0
                               dd 3EAD2E0h,
UPX1:00443CD0
                               dd 0D8CBBEB1f
UPX1:00443CD0
                               dd ODF370CDFt
UPX1:00443CD0
                               dd 9AD08EC0h,
```

처음엔 이걸 IDA로 열고 잠깐 어리둥절했었다,

근데 자주보던 단어 UPX를 보고 패킹이 되어있음을 짐작 할수있었다.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Users\Users\Users\Unitercomer\Users\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upers\Upe
```

인터넷에서 간단하게 UPX언패킹 툴을 구해 언패킹 할수 있었다.



프로그램을 열어보니 시리얼키를 맞추는 문제같다.

```
ODE:00440F72 ; -----
ODE:00440F72
ODE:00440F72 loc 440F72:
                                                               ; CODE XREF: CODE:00440F561j
ODE:00440F72
                                  push
ODE:00440F74
                                           ecx, offset aBeggarOff ; "Beggar off!"
                                  MOV
ODE:00440F79
                                           edx, offset aWrongSerialTry; "Wrong Serial,
                                  mov
ODE:00440F7E
                                            eax, ds:off 442C44
                                  mov
ODE:00440F83
                                  mov
                                            eax, [eax]
ODE:00440F85
                            Text search (slow!)
ODE:00440F8A
ODE:00440F8C
                             String Wrong
ODE:00440F8C
ODE:00440F8C loc_440F80
                                 Parameters
                                                            Direction
ODE:00440F8C
ODE:00440F8E
                                                           Search Down
                                 Case sensitive
ODE:00440F93
                                                           Search Up
UVE - BUTTUEOD
                                      aular avnraccian
                      에러메세지를 추적하여 그근처를 뒤져보려고 했다.
  CODE: 00440F21
                               mov
                                       eax, [ebx+2C4h]
  CODE:00440F27
                               call
                                       sub_420E20
                                       eax, [ebp-4]
  CODE:00440F2C
                               mov
  CODE: 00440F2F
                                       edx, offset aRegisteredUser; "Registered User"
                               mov
  CODE:00440F34
                                       sub_403B2C
                               call
                                       short loc_440F8C
                                       edx, [ebp-4]
  CODE:00440F3B
                               1ea
                                       eax, [ebx+2C8h]
sub_420E20
  CODE:00440F3E
                               mov
  CODE: 00440F44
                               call
                                       eax, [ebp-4]
edx, offset aGfx754Ier954 ; "GFX-754-IER-954"
  CODE:00440F49
                               mov
  CODE:00440F4C
                               MOV
  CODE:00440F51
                                       sub_403B2C
                               call
  CODE:00440F58
                               push
                                       0
                                       ecx, offset aCrackmeCracked ; "CrackMe cracked successfully
  CODE:00440F5A
                               mov
                                       edx, offset aCongratsYouCra ; "Congrats! You cracked this Cr
  CODE:00440F5F
                               mnv
  CODE:00440F64
                               mnu
                                       eax, ds:off 442C44
  CODE:00440F69
                               mov
                                       eax, [eax]
  CODE: 00440F6B
                               call
                                       sub 43D068
  CODE:00440F70
                                       short loc_440FA4
                               jmp
```

무방비한 상태로 있는 User와 Serial을 볼수 있었다.

