

# CodeEngn Basic RCE L05 Writeup



Daniel Smith

Feb 18 · 2 min read

Let's start RCE

Filename: 05.exe  
Description: 이 프로그램의 등록키는 무엇인가  
Author: Acid Bytes [CFF]

Crackers For Freedom CrackMe v3.0

## Official CFF CrackMe v3.0

Unregistered...

Coder Acid Bytes [CFF]

754-GFX-IER-954

Rel. Date 05/08/2000

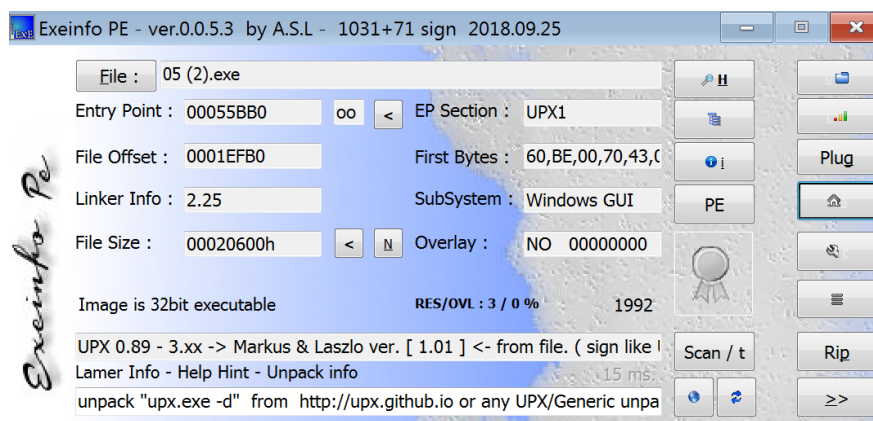
Register now !

Quit the CrackMe

This is the official CFF CrackMe  
If you can manage to crack it,  
mail Name/Serial to:

[acidbytes@gmx.net](mailto:acidbytes@gmx.net)

제품키 크랙 문제인 것 같다



Exeinfo PE 로 열어봤는데 UPX 로 패킹되어 있는 것 같다  
언패킹을 한 뒤에 다시 열어보자

```

→ Downloads upx -d ./05.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2018
UPX 3.95      Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

   File size      Ratio      Format      Name
-----
315392 <- 132608 42.05%   win32/pe   05.exe

Unpacked 1 file.

```

```

00440F2F MOV EDX,05.00441014 ASCII "Registered User"
00440F4C MOV EDX,05.0044102C ASCII "GFX-754-IER-954"
00440F5A MOV ECX,05.0044103C ASCII "CrackMe cracked successfully"

```

프로그램 상의 문자열을 보니 성공 메시지 바로 뒤에 키와 유저 네임이  
나와있다  
한번 시도 해보자

