Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Unpackme 08 |
| 파일명 | Unpackme 08.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/01/10 ~ 2017/01/16 |
| 문제 내용 | \* Unpacking 하여 OEP를 찾아내라.  \* IAT의 RVA 값을 찾아내라. |

문제 풀이:



문제 파일을 실행하면 저번 문제와 같은 화면이 나옵니다. 역시 내부의 시작 주소와 RVA를 찾는 문제입니다.



ollydbg로 실행한 화면입니다. 저번 문제와 같이 PUSHAD가 보이지 않고 코드도 매우 짧습니다.



문제는 PEiD 프로그램도 packing 방식을 찾지 못하고 있다는 것입니다. 일단은 코드를 진행해봅니다.



처음 코드 진행에서 40B265 주소에서 jump를 하자 401000의 지점으로 넘어왔고 거기서 analysis code를 사용하자 제대로된 코드가 나왔습니다. 처음의 코드에서 PUSH ECX, PUSH EAX가 PUSHAD의 역할을 하는 것 같습니다.

이 지점에서 덤프를 저장합니다. 그 후, IAT를 복구합니다.



ImpRec 프로그램으로 복구한 IAT 정보입니다. 역시 fix dump로 저장하면 잘 실행이 됩니다.