Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | UnPackMe\_!EP (EXE Pack) 1.2 |
| 파일명 | UnPackMe\_!EP (EXE Pack) 1.2.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/02/12 ~ 2017/02/19 |
| 문제 내용 | \* Unpacking 하라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



역시 unpacking만 하면 되는 문제입니다.



PEiD로 packing 분석한 결과 저번 문제와 같이 AHpack 형식으로 packing 되어있습니다.



Ollydbg로 실행해보면 저번 문제와 같이 PUSHAD가 2개 46B0FF, 46B128 지점에 보입니다. 역시 같은 방식으로 진행하면 POPAD가 2개 나올 것입니다.



break를 걸고 두번째 POPAD까지 진행하면 POPAD 후 return 하는 지점이 보입니다. POPAD 직후 4271B0로 jump하는데 이 주소가 실제 OEP일것입니다.

이 주소로 dump를 뜨고 IAT 복구를 해주면 문제가 해결이 됩니다.