Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | UnPackMe\_!EP (EXE Pack) 1.0 |
| 파일명 | UnPackMe\_!EP (EXE Pack) 1.0.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.



unpacking 문제이므로 실행된 프로그램에서 딱히 무언가를 풀진 않는 것 같습니다. unpacking을 진행해봅니다.



PEiD로 분석해본 결과 AHpack 방식으로 packing 되어 있습니다.



Ollydbg로 실행한 모습입니다. packing시의 OEP 지점에 PUSHAD가 있는 것으로 보아 POPAD를 하는 구간이 나올 것임을 예상할 수 있습니다.

PUSHAD가 B20FF, B212F 두 곳에 있으므로 POPAD 역시 두번 호출 될 것입니다. 각 PUSHAD의 다음 주소를 진행 시의 스택에 break를 걸어 진행해 봅니다.



OEP로 jump하는 지점이 나올 것입니다. 계속 진행해봅니다.



진행하면 JUMP구간과 return 구간이 혼재되어 있는데 JMP가 공통으로 4B22D8 지점으로 jump하므로 실제로 리턴되는 지점은 4B22DF 지점의 return입니다.



return 후 jump하는 지점으로 오면 실제 OEP에 도착하게됩니다. 이제 이 OEP 지점에서 dump를 뜹니다.



OEP 지점으로 dump를 뜨고 IAT 복구를 해줍니다.