Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Unpackme.Aspack.2.2 |
| 파일명 | Unpackme.Aspack.2.2.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/02/20 ~ 2017/02/26 |
| 문제 내용 | \* Unpacking 하라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



ASpack 2.12와 같은 방식의 ASPacking 형태의 Packing이 되어있으므로 unpacking 합니다.



PEiD로 확인해보면 역시 ASPack 방식임을 확인할 수 있습니다.



Ollydbg로 실행하면 PUSHAD로 레지스터를 저장합니다. 이를 반환하는 POPAD를 찾아야하므로 명령 실행 후의 ESP 레지스터 값을 따라가 break를 겁니다.

이전 방식대로 진행해보면 문제가 생기는데 PUSHAD 후 CALL 명령을 실행하면 바로 창이 뜨게 됩니다. 추가적인 진행이 필요해보입니다. 우선 F7키로 CALL 내부로 들어간 후 진행합니다. 스택 주소에 대한 break는 여전히 걸려있는 채입니다.





CALL 메소드 내부에서 진행하면 POPAD 지점에 도달하게 됩니다. ASpack의 버전 업이 되면서 특정 메소드를 CALL 한 후 패킹 해제가 되게 변경된 것 같습니다. 이 후 진행하면 4271B0 주소로 넘어가고 그 지점이 실제 OEP임을 알 수 있습니다.



실제 OEP 주소로 넘어온 화면입니다. 여기서 덤프를 뜹니다.



덤프를 뜬 프로그램은 ImpRec으로 IAT 복구를 해주면 용량이 늘어나고 잘 실행이 되게 됩니다.