Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Unpackme.Aspack.2.12 |
| 파일명 | Unpackme.Aspack.2.12.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.



Aspacking 방식으로 packing 되어있는 프로그램입니다. 이것을 unpacking 하는것이 목적입니다.



실제로 PEiD로 확인해보면 ASPack 방식으로 되어있습니다.



Ollydbg로 실행할 시의 화면입니다. PUSHAD로 시작하는 것으로 보아 스택에 모든 레지스터를 저장 후 패킹 해제 후 POPAD로 레지스터를 되돌릴 것입니다. 따라서 PUSHAD 실행 직후의 스택 주소에 break를 걸면 POPAD에 도달할 것입니다.



ASpack 방식의 특징으로는 .Aspack 섹션이 존재하고 프로그램의 시작지점이 되는데 이는 패킹을 해제하기 위해서입니다.

PUSHAD 명령을 실행 후 스택 주소를 저장하는 레지스터 ESP에 follw in dump 기능으로 이동한 후 break를 걸고 진행합니다.



진행한 결과 POPAD 명령 구간으로 이동하였습니다. 진행하면 PUSH 00401560 명령을 진행하게 되는데 이 주소가 실제 OEP 주소일 것입니다.



실제 OEP에 도달한 모습입니다. PUSH EBP 명령으로 시작하게 됩니다.

이제 ollydbg의 덤프 기능을 이용합니다.

덤프를 뜨면 OEP가 바뀐채 저장이 되는데 이대로는 IAT 주소가 잘못되어 실행이 되지 않으므로 복구를 해주어야합니다.



ImpRec 프로그램을 통해 계산한 OEP를 입력하고 AutoSearch를 하면 자동으로 IAT 복구를 해줍니다. Fix Dump를 해주면 복구된 프로그램을 저장합니다.

복구된 프로그램은 packing된 상태보다 용량이 늘어나게 됩니다.