Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Unpackme 04 |
| 파일명 | Unpackme 04.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/01/10 ~ 2017/01/16 |
| 문제 내용 | \* Unpacking 하여 OEP를 찾아내라.  \* 정답 여부를 판단하는 주소값을 찾아라. |

문제 풀이:



문제 파일을 실행하면 나오는 화면입니다. name과 serial의 조합을 맞춰야 하는 것 같습니다.



ollydbg로 실행 후 시작 시 보이는 화면입니다. packing 된 프로그램이므로 PUSHAD 명령에서 시작하게 됩니다. 그 말은 POPAD로 넘어가는 부분이 있을 것이므로 스택 주소를 break를 걸어 진행합니다.



POPAD에서 정지된 모습입니다. 이 후, 00445834 주소로 jump하므로 저 주소가 시작지점이라고 예측할 수 있습니다.



시작 주소로 진행하면 코드 루틴이 1byte씩으로 해제가 되어 있습니다. 이를 분석하기 위해 ollydbg의 기능 Analysis Code 를 사용합니다.



기능을 쓰면 몇가지 루틴이 분석되나 아직 정확한 코드 상태를 알기는 힘듭니다.



unpacking을 위해 시작 지점에서 정지된 상태로 덤프를 뜹니다. entry point가 변경됨을 알 수 있습니다. 저장되는 파일은 unpackme 04 dumped.exe입니다.

이렇게 덤프된 파일은 IAT가 복구되지 않아 실행이 불가능 하므로 복구해줍니다.



ImpRec 프로그램을 이용해 IAT를 복구합니다. OEP에 발견한 시작 지점을 입력 후 AutoSearch를 누르면 자동으로 import를 찾습니다. 그 후 Fix Dump로 저장합니다. 저장되는 파일명은 unpackme 04 dumped\_.exe 입니다. 이렇게 복구된 파일은 용량이 늘어나고 잘 작동합니다.



복구된 파일에서 참조하는 string 검색 기능으로 정답 여부 체크를 하는 구간을 찾는 과정입니다. 정답을 출력하는 string이 있는것으로 보아 저 부근에서 정답 체크를 할 것입니다.



이동하면 정답 string 위의 코드 중 최종적으로 분기하는 지점은 4454D4 지점으로 403C70의 결과를 통해 분기하게 됩니다.

즉, OEP는 445834, 정답 분기 주소는 4454D4입니다.