Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | CodeEngn Reverse2 L06 |
| 파일명 | Advance 06.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/02/12 ~ 2017/02/19 |
| 문제 내용 | \*프로그램이 실행된 후 종료되는 시간을 구하시오 |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



1이 써져있는 창이 하나 뜨고 누르면 2로 증가한 창이 생깁니다. 그렇게 계속 카운트 하다가 마지막으로 종료되기 직전의 숫자를 구하면 되는 것 같습니다. 숫자가 큰 것 같으므로 단순히 누르는 것으로 알아내는것은 시간이 많이 걸릴것 같습니다.



packing 방식은 UPX로 분석되었습니다.



ollydbg로 실행하면 PUSHAD로 시작합니다. 평소에 UPX를 unpacking한 방식대로 POPAD를 찾습니다.



POPAD를 찾고 그 밑에 jump구간이 있으므로 jump를 하면 실제 OEP가 나타날 것입니다.



실제 OEP로 이동한 모습입니다. 이제 전의 프로그램처럼 디버깅을 방해하는 요소가 없는지 interdullar call 기능으로 찾아봅니다.



검색한 결과 IsDebuggerPresent가 있으므로 이동하여 주석처리를 해줍니다.

주석처리를 하고 진행하면 40EA13의 call에서 메세지 창이 뜨므로 이동해봅니다. 이동하면 루틴을 알기 힘들기 때문에 다른 방법으로 검색해봅니다.



문제가 창을 계속 띄우는 것이므로 messagebox 함수 호출을 찾아봅니다. 그러면 각 messagebox의 호출부분을 찾을 수 있고 이 부분에서 문제 창이 출력되었으므로 여기서 루프를 도는 것 같습니다. messageBoxW는 4개의 인자를 받는데 그 중 EBP가 내용 text이므로 이 부분에 어떤 값이 들어오는지 검사해야할 것입니다. EBP의 메모리 주소(27EFD90)에 접근하는 지점을 break를 걸고 진행합니다.



걸고 진행하면 이 부분에 도착하게 되는데 EBP, EAX를 비교하고 있습니다. EAX에는 현재 text(경과된 시간), EBP에는 비교값이 저장되어 있는데 0x316 값이 저장되어 있어 EBP가 EAX보다 작으면 408F95로 점프하는데 거기서 종료되므로 EBP 값이 카운트 해야할 값일 것입니다.