Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | CodeEngn reverse L19 |
| 파일명 | 19.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/01/30 ~ 2017/02/05 |
| 문제 내용 | \* 문제 프로그램이 실행 후 몇 초 후에 종료되는지 알아내시오 |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



창이 하나 뜨고 얼마 후에 자동 종료되게 됩니다.



프로그램은 UPX로 packing 되어 있습니다.



기존의 UPX unpacking 방식대로 PUSHAD에 대입되는 POPAD를 찾고 jump 지점을 찾습니다.



unpacking 된 파일을 ollydbg에서 진행하면 위와 같은 창이 뜨면서 진행이 멈춥니다. 디버거를 막는 기능이 있는 것 같습니다.



실제로 진행해보면 isDebuggerPresent라는 함수로 디버거 진행을 막는 함수가 존재합니다. 진행을 위해 이 함수를 NOP 처리합니다.

그 후에 진행을 해도 루틴을 잘 알기 힘들기에 이 프로그램에서 시간과 관련된 함수를 호출하는지를 확인합니다.



호출되는 함수 중 timeGetTime이라는 함수가 보입니다. 이 함수의 기능은 프로그램의 실행 후 경과 시간을 불러오는 함수입니다.



이 함수를 intermodular call로 모든 call 지점을 검색해 전부 break를 걸고 진행합니다.



진행한 결과 timeGetTime 함수에서 멈췄습니다. 이 곳의 루틴을 보면 EDI에 timeGetTime 값을 저장하고 ESI에 주소 48E8D3 값을 가져와 444C61에서 두 값을 비교해 timeGetTime 값이 더 크면 444D38로 jump합니다.



그렇게 jump하면 EAX에 ESI값을 뺀후 특정 값과 비교하여 크면 444C71로 jump합니다. 그렇지 않다면 위의 비교를 다시 하게 됩니다. 444C71 지점후에는 EndDlg로 종료를 하게 되므로 여기서의 값이 진행 후의 종료 시간이 될 것입니다.



마지막 분기에서의 stack 값입니다. 0x2B70(=11120) 값이 millisecond로 프로그램이 종료되는 시간일 것입니다.