Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Raz0r Crack me 1 |
| 파일명 | Raz0r1.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/01/17 ~ 2017/01/23 |
| 문제 내용 | \* Unpacking 하여 OEP를 찾아내라.  \* serial 번호를 알아내라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



목표는 Serial 번호를 찾는것인데 ollydbg를 사용할 시 packing 되어있어 unpacking을 먼저 진행해야합니다.



이런 식으로 PUSHAD 명령부터 시작하므로 POPAD 지점을 찾은 후 그 지점 후 jmp하는 구간이 OEP일것입니다.



429A3A 지점에서 POPAD가 나오고 그 후, JMP 명령으로 이동하는 지점입니다. 따라서 OEP는 00401360 주소임을 알 수 있습니다.



unpacking 후의 시작 코드입니다. 보통의 C++ 프로그램은 unpacking 되면 각 모듈이 알기 쉽게 나오지만 이 프로그램은 잘 나오지 않았습니다. 그래도 window 프로그램의 특성상 dlgitem의 값을 받아오는 부분이 있을테니 이 시스템 콜을 하는 지점을 intermodular call 기능으로 찾습니다.



이 모듈에서 불러오는 메소드들입니다. GetDlgItemTextA 메소드가 있는 것으로 보아 저 지점에서 입력한 serial 값을 가져올 것입니다.



GetDigItemTextA 지점으로 이동한 모습입니다. 고맙게도 처리 부분이 바로 밑에 나오게 됩니다. 40107D 주소가 분기점인데 string 값 두개가 맞지 않으면 wrong serial 구문으로 이동하므로 위의 "AD46DFS547" string 과 입력값이 맞아야 할 것입니다. 즉, 이 string이 알맞은 serial 값입니다.



실제로 확인 결과를 얻어낸 모습입니다.