Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Abex Crackme 05 |
| 파일명 | Abexcm5.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2017/01/02 ~ 2017/01/09 |
| 문제 내용 | 알맞은 serial 값을 찾아라. |

문제 풀이:



문제 파일을 실행하면 serial 입력 화면이 뜹니다. Check 버튼을 클릭하면 serial을 체크하게 됩니다.



코드 흐름 중 Check 버튼을 누르게 되면 40106C 시점으로 이동되어 GetDlgItemTextA로 input string을 받아오게 된후 특정 string이 합쳐진 후 비교하게 됩니다. 최종적으로 비교하는 string은 402324 주소와 402000 주소인데 402324는 GetDlgItemTextA의 buffer 즉, input string이고 402000은 세 번의 strcatA 메소드로 합쳐진 최종 string입니다. 그럼 4010F7에 break를 걸어 최종 string을 알아봅니다.



먼저 첫번째 strcat에선 4562-ABEX와 빈 string이 합쳐저서 40225C에 합쳐집니다. 그 후, 40225C ~40225F 주소에 1씩 값을 더하는 루프를 DL register를 이용해 2번 실행하므로 4562는 6784가 되어 40225C의 string은 6784-ABEX가 됩니다. 두 번째 strcat에선 L2C-5781을 402000 주소의 빈 string에 합치게 되고 세 번째 strcat에선 402000("L2C-5781")에 40235C("6784-ABEX") 주소를 합치므로 결과는 "L2C-57816784-ABEX" 입니다. 이 string이 알맞은 serial입니다.



구한 serial을 입력해 정답을 확인한 화면입니다.