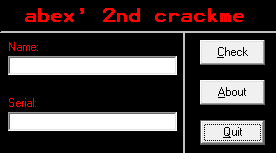
Crack me 문제 보고서

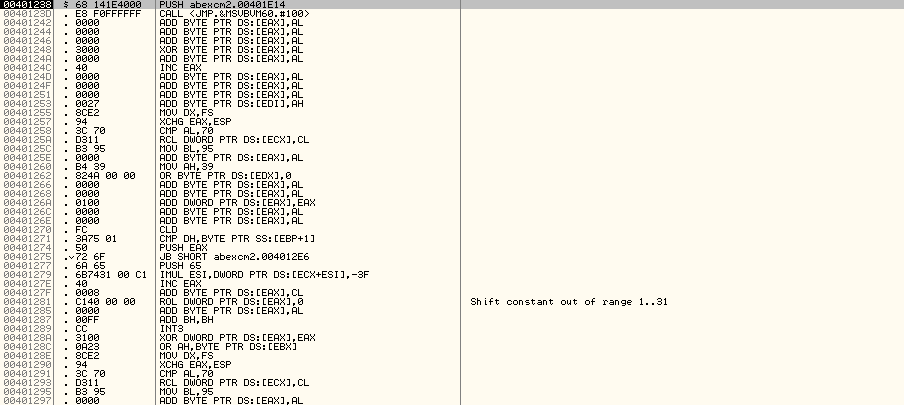
|  |  |
| --- | --- |
| 문제명 | Abex Crackme 02 |
| 파일명 | Abexcm2.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2017/01/02 ~ 2017/01/09 |
| 문제 내용 | 알맞은 register값을 찾아라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



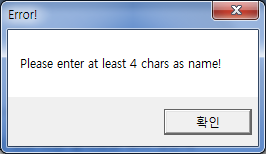
이름과 시리얼 값을 입력하는 창이 나오고 Check를 누를시 정답 여부를 알려주게 됩니다.



분석을 위해 Ollydbg로 실행한 화면입니다.

코드의 모양이 일반 C언어 기반으로 작성된 것과 다른 형식으로 되어 있는데 40123D의 MSVBVM60 DLL CALL을 하는 것으로 보아 Visual Basic 언어로 작성된 코드임을 알 수 있습니다.

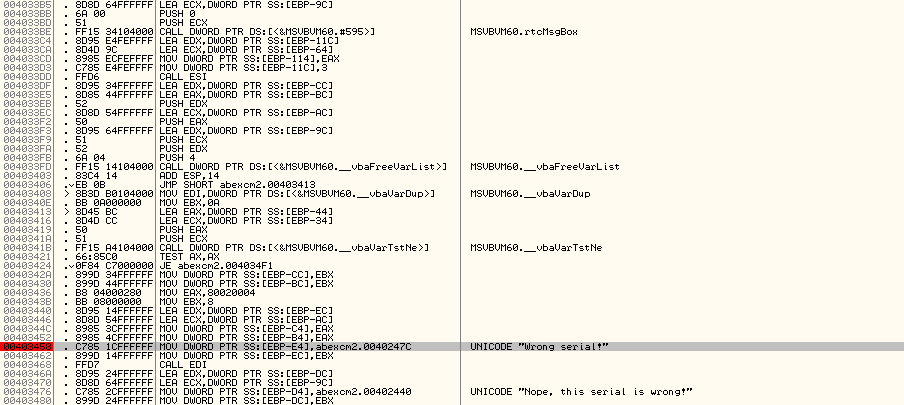
이 코드를 하나씩 실행시켜도 흐름을 파악하기 어려우니 다른 힌트가 필요합니다. 우선 값을 입력하지 않고 Check시 한 Message 박스가 출력됩니다.



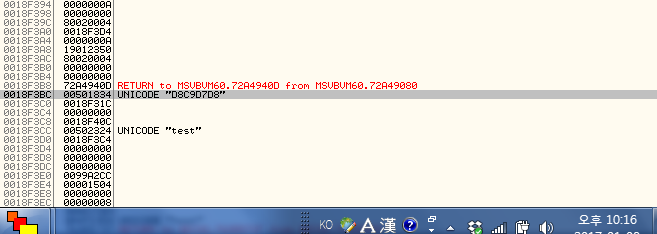
Name에 4자 이상의 글자를 입력하라는 내용입니다. Ollydbg의 All referenced text strings 기능을 이용해 어느 주소에서 출력하는지 파악합니다.



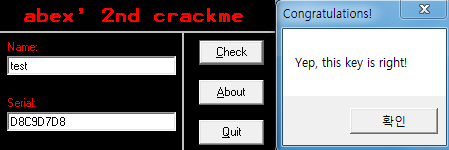
Text string이 참조되는 주소들입니다. 살펴보니 정답을 출력하는 text와 오답임을 알리는 text가 존재하므로 그쪽으로 이동해 살펴봅니다. 우선 오답인 403458 주소로 이동합니다.



오답 쪽의 코드로 이동하여 흐름을 파악하려 하나 역시 파악하기 쉽지 않습니다. 또 다른 정보를 얻기 위해 name의 4자리 조건을 맞춰(“test”) 실행합니다.



오답에 break를 걸어 도달한 지점에서의 stack 정보입니다. 501834 주소에 UNICODE로 name이 변경된 것으로 보이는 code가 나오게 됩니다. 저 code가 name인 test에 맞는 code임을 예측할 수 있습니다.



실제로 입력한 결과 정답임을 확인 할 수 있습니다.

이렇게 푸는 방식은 실제 name에 맞는 serial 값을 루틴을 통해 알아낸 것이 아니지만 목적 달성은 이루어 냈으므로 이 문제는 일단 이 풀이로 종료하고 후에 보충하겠습니다.