Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Abex Crackme 04 |
| 파일명 | Abexcm4.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2017/01/02 ~ 2017/01/09 |
| 문제 내용 | 알맞은 serial 값을 찾아라. |

문제 풀이:



문제 파일을 실행시 나오는 화면입니다. serial code를 입력하는 text 칸이 있고 Registered 버튼이 존재하는데 활성화 되어있지 않습니다. 이 버튼을 활성화 시키는것이 목표가 될것입니다.



Ollydbg로 실행해보면 실행 파일이 Visual Basic 언어로 생성되었음을 알 수 있습니다. 이 언어로 제작된 코드는 흐름의 파악이 어려우니 All referenced Text String 기능으로 실행 파일에 쓰인 text들을 검색해 정보를 찾습니다.



text들을 살펴보면 정답을 알리는 text가 존재함을 확인할 수 있습니다. 저 위치로 이동해 새로운 정보를 찾습니다.



정답 메세지 출력 루틴으로 왔지만 특별히 code를 검사하는 기능은 보이지 않습니다. 또 다른 정보를 찾기 위해 이번엔 name in current module 기능을 통해 이 실행 파일에서 쓰인 API 메소드들을 검색합니다.



사용된 메소드의 목록이 뜹니다. 그중, visual basic에서 string의 비교를 하는 메소드인 strcmp가 보입니다. 이 메소드를 호출하는 주소를 Selected address 기능으로 찾습니다.



검색 결과 총 2곳에서 호출함을 알 수 있습니다. 그 중 첫 번째는 import의 정의이므로 두 번째로 이동합니다.



strcmp가 호출되는 지점으로 이동했습니다. 이 메소드가 호출될 때 비교될 올바른 code string이 들어올테니 break를 걸고 실행해 봅니다.



strcmp 호출에서 break가 걸렸을때의 register 상태입니다. ECX register에 2248955 값이 들어있는데 이것이 code 값임을 예측할 수 있습니다.



찾아낸 값을 입력한 결과 Register 버튼이 활성화되고 정답 화면이 출력됩니다.