Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Duelist’s Crack me 5 |
| 파일명 | due-cm5.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/12/26 ~ 2017/01/01 |
| 문제 내용 | \* Unpacking 하라.  \* 메세지 박스를 없애라.  \*Registered로 변경하라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



파일이 unregistered 되어있다는 화면입니다. 이를 register로 변경하는것이 목적입니다.



Ollydbg로 실행시 entry point가 code 외부에 존재한다는 메세지가 뜹니다.



실행 시 나오는 코드는 기존 실행 파일의 루틴과 다르게 각 기능이나 흐름을 알기 힘들게 되어 있습니다. 이는 실행 파일이 packing 되어있기 때문에 실행 지점이 보이지 않는 것임으로 한 루틴씩 진행하며 실제 코드의 시작지점을 찾아야 합니다.



진행을 하다보면 406663에서 JMP를 하게 되고 완전히 새로운 코드가 나타나게 되는데 이곳이 시작지점입니다.



이제 이 코드를 실제로 동작하는 루틴으로 분석하는 작업이 필요한데 방법은 unpacking 툴을 사용하는 등 여러가지가 있지만 여기서는 Ollydbg의 기능을 사용하겠습니다. Ctrl + A 버튼을 누르면 packing 된 코드를 자동으로 분석해주게 됩니다.



분석이 된 코드입니다. 루틴을 알아볼 수 있게 되었습니다.



코드를 진행해 message 창을 띄우는 루틴에 도달한 모습입니다.

이제 해결해야하는 목표는 unregister 창을 띄우지 않는 것과 텍스트 내부의 메세지를 register로 변경하는것입니다.

먼저 unregister 창은 MessageBoxA 메소드를 통해 띄워지므로 MessageBoxA의 실행을 NOP로 변경해 출력을 막습니다.



MessageBoxA를 NOP 으로 처리한 루틴입니다. 더 이상 메세지창이 띄워지지 않습니다.

다음 MessageBoxA는 unregister text를 출력하는 창인데 메세지의 내용을 40205C 주소에서 가져오고 있습니다.



메세지창이 참조하는 주소입니다. Unregistered 메세지가 저장되어 있습니다. 그 옆의 주소에는 Registered 메세지가 저장되어 있으므로 참조하는 주소를 402050으로 변경하면 될 것입니다.





최종적으로 변경한 코드와 이를 실행한 결과입니다.