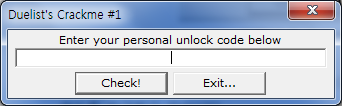
Crack me 문제 보고서

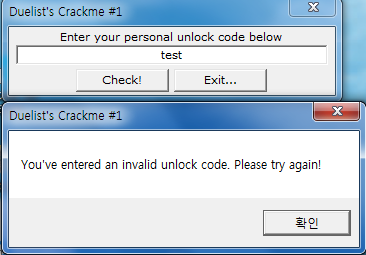
|  |  |
| --- | --- |
| 문제명 | Duelist’s Crack me 01 |
| 파일명 | due-cm1.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/12/26 ~ 2017/01/01 |
| 문제 내용 | 알맞은 unlock code(문자열)을 찾아라 |

문제 풀이:

문제 파일을 실행 시 한 텍스트 박스를 지닌 창을 띄우게 됩니다.

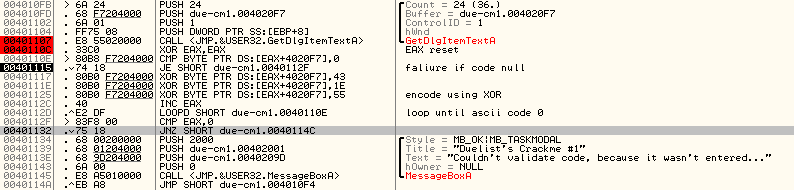


저 텍스트 박스에 문자열을 입력한 후 Check! 버튼을 클릭할 시 결과 창을 띄우게 됩니다. 실패 시에는



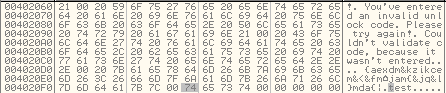
아래와 같은 invalid 결과를 보여주게 됩니다.

알맞은 code를 찾기 위해 실행 파일을 ollydbg를 이용해 실행합니다.



Code 입력 창에서 Check! 버튼을 눌렀을 시 실행되는 코드 부분입니다.

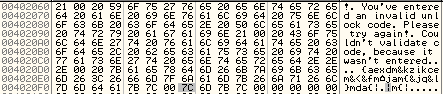
GetDlgItemTextA 시스템 메소드는 item의 text를 가져와 저장하는 기능을 합니다. 이 메소드에서 Buffer 즉, text를 저장하는 주소는 004020F7번입니다.



주소창을 확인해 보면 입력한 code가 저장되어 있는 것을 확인할 수 있습니다.

그 다음 루틴은 0040110C ~ 00401132 구간인데 먼저 EAX를 XOR 의 자기연산을 통해 0으로 초기화 하고 4020F7 주소값이 0임을 체크해 0이면 40112F로 점프합니다. 거기서 EAX가 0이면 그대로 진행해 code가 입력되지 않았음을 알리는 창을 띄웁니다. 즉, 처음 부분은 code의 입력 여부를 검사하는 구간이고 그 후 루프가 시작됩니다.

루프 내부에선 EAX의 증가를 통해 code를 처음부터 끝까지 탐색하며 XOR 의 세번의 연산을 통해 값을 변경합니다. 각 순서대로 43 -> 1E -> 55 값을 XOR 합니다.

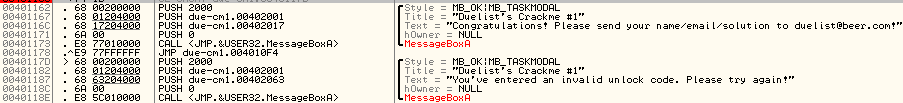


위의 루프를 진행한 후의 code의 변화입니다. 4020F7 이후의 값이 변경됨을 확인할 수 있습니다.

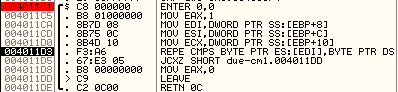
루프는 주소의 값이 0일 때 즉, code의 끝을 지날 때 끝나고 EAX가 0이 아니므로 0040114C로 점프합니다.

2017-01-08 01;06;56.PNG

그러면 3개의 argument를 가지는 함수가 호출되게 되고 그 결과를 EAX로 검사해 0이면 0040117D로 점프하고 아니면 그대로 진행합니다.



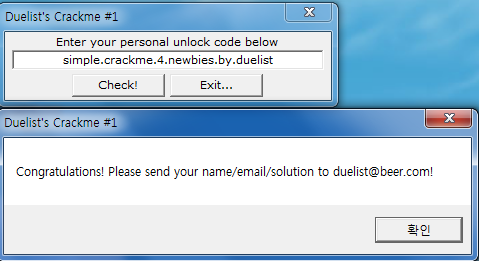
이 이후의 코드는 결과창을 띄우는 부분이므로 004011C1의 결과로 성공이 정해짐을 알 수 있습니다.



004011C1의 루틴입니다. 먼저 EAX에 1을 저장해 true값으로 만든 후 EDI,ESI에 값들을 저장하는데 그 값은 argument로 받은 두 주소 4020F7, 4020D3입니다. 그 후 이 둘을 비교해 같으면 004011DD로 점프해 EAX에 0값을 입력하지 않아 성공처리를 합니다. 즉, 입력한 후 XOR 계산으로 변경된 code값이 4020D3에 저장되어있는 값과 같으면 성공입니다.

2017-01-08 01;22;14.PNG

004020D3에 저장되어 있는 값입니다. 여기서 code의 길이는 35임을 알 수 있습니다. 이에 맞는 code 값은 각 값에 43, 1E, 55 즉, 반대 순서로 XOR 계산한 값입니다. 코드를 작성해 계산된 값은 simple.crackme.4.newbies.by.duelist 입니다.



실제 테스트시 정답이 출력됨을 확인할 수 있습니다.