Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Basse 2012 Crack me 1 |
| 파일명 | Basse.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/01/17 ~ 2017/01/23 |
| 문제 내용 | \* Key 값을 찾아내라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



알맞은 key 값을 입력해 Check하여 정답 여부를 판단하는 것으로 보입니다.



ollydbg로 실행한 화면입니다. 로직은 간단하게 GetDlgItemInt로 입력한 값을 받아온 후 중간에 처리를 하여 40107D에서 EAX 레지스터의 값이 0x7A2896BF와 같으면 jmp를 실행하지 않아 정답처리가 됩니다. 특이 사항으로는 입력 값을 받아오는 것이 GetDlgItemInt로 숫자 입력만 받아오게 됩니다. 즉, 숫자 값을 입력하면 EAX 레지스터에 저장하고 그 값이 중간에 변형되어 마지막에 0x7A2896BF와 같으면 됩니다.

중간의 로직은 403000 번지에 저장되어 있는 문자열을 4문자씩 읽어 EBX에 저장한후 40110F 메소드를 call합니다. EAX의 변형은 저 메소드 내부에서 일어날 것으로 추정됩니다.



메소드의 루틴입니다. EBX(string의 앞의 4 주소의 값), EAX(입력 값)을 EDX,ECX에 저장하고 EAX, EBX에 INC -> NOT 계산을 합니다. 그 후, 다시 한 번 INC를 하므로 이 때의 EAX, EBX 값은

~(EAX + 1) + 1 = ~EAX입니다. 그 후, EAX에는 EBX의 값을 EBX에는 EAX의 값을 AND로 계산한 후 두 값을 더합니다. 이 일련의 루틴이 한 번만 돌면 규칙을 알기 힘들지만 EBX의 모든 문자열을 처리하고 나서 EAX값을 보면 16진수로 원래 입력했던 값이 그대로 남아있게 됩니다. 이 루틴은 일종의 함정인듯 합니다. 결국 serial은 0x7A2896BF에 맞는 10진수 값입니다.



계산기로 값을 구한 후 체크한 결과입니다. 정답을 확인하였습니다.