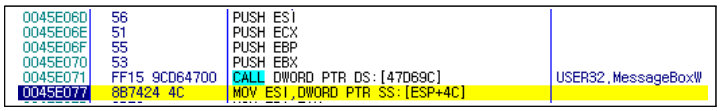
- Ezbeat -

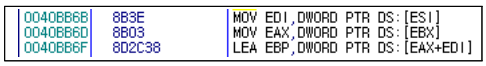
이 문제를 풀기 전에 심심해서 전 엔터를 계속 누르고 있으면서 언제 끝나나 봐보았습니다. 그 결과 790까지 간 다음 꺼지더군요 -_-;; 그래서 MD5변환 하고 인증했더니 문제가 풀렸습니다. 그래서 귀차니즘 결과 그냥 넘길려고 했지만 제 성격상 항상 문서화를 해야해서 풀이를 써보았습니다. 쫌 길게 풀었지만 여기서는 간략하게만 적겠습니다.

처음에 Back to user mode로 메시지 창 있는 곳을 잡아보았습니다.



메시지박스 인자로 4개가 PUSH되고 있는데요. 그 숫자가 내용에 표시되므로 두 번째 전달 인자입니다. 그래서 EBP값을 봐보았더니 그 수가 맞더군요. (정확히는 문자열..)

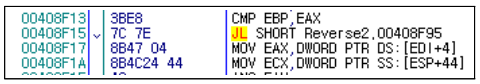
그래서 그 문자열이 어디서 오는지를 체크해서 하드웨어 브레이크 포인트를 계속 걸어가며 (Hardware, on write) 역으로 추적했습니다. 그 결과 메시지 창이 뜨고 그 문자열에 있는 숫자가 +1이 될탠데 그 부분을 찾았습니다.



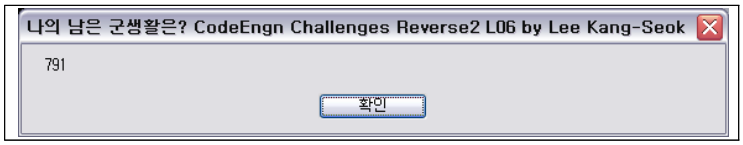
요 부분에서 그 전 값을 +1 시키더군요. 처음에 이렇게 생각했었습니다. 그러면 어떠한 값하고 비교해서 그 값보다 크면 이 루틴을 들어오지 않겠구나... 라고 생각하고 위쪽으로 계속 봐보았지만.. 시간낭비였습니다.. 가장 쉬운 방법을 놔두고 헛수고를 했습니다 ;;

그래서 +1된 값을 어디선가 비교를 하겠구나로 생각을 전환하고 다시 하드웨어 브레이크 포인트를 걸었습니다. (Hardware, on access)

어떠한 부분에서 멈추더군요. 그 부분입니다.



EBP에는 316이라는 값이 있었고 EAX에는 출력하려고 하는 값이 있었습니다.
그 아래 JL이므로 316보다 더 크면 점프를 하겠죠. 그래서 강제 점프를 시켜보았더니 프로그램이 끝나더라구요. 316은 10진수로 790이므로 맞는 답은 찾은 것 같습니다.
그래서 790까지 출력시키고 여기를 왔었을 때 점프를 안 시키면 791도 출력이 되더군요. 뭐..당연한 결과겠지만요 . (스샷..)



정답 : 790
MD5 : 2DACE78F80BC92E6D7493423D729448E