2014

Code Engn Basic 19

4.Z320

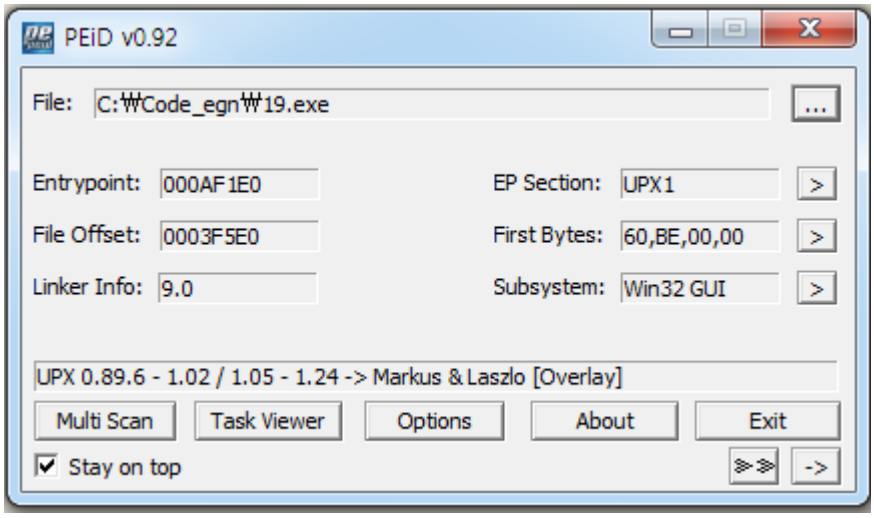
elttzero@gmail.com

Challenges : Basic 19

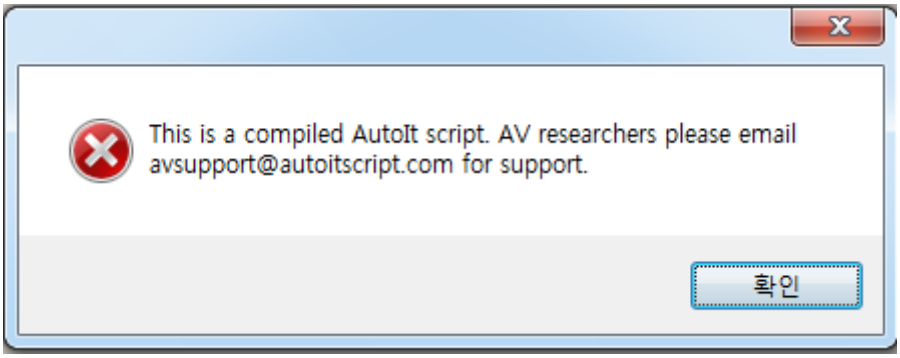
Author : CodeEngn

KO : 이 프로그램은 몇 밀리세컨드 후에 종료 되는가
EN : How many milliseconds does it take for this program to terminate

프로그램이 종료되는 시간을 찾아내는 문제입니다.

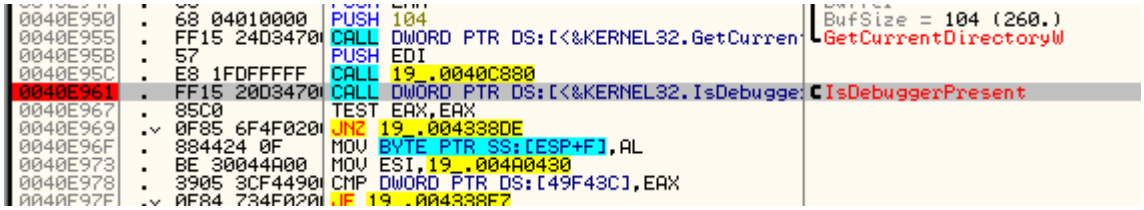


프로그램을 확인하면 UPX 로 패킹되어 있음을 알 수 있습니다. UPX 로 언팩해 줍시다.

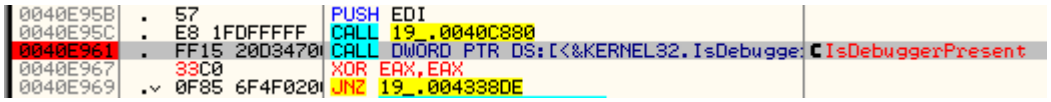


OllyDbg 로 실행하다 보면 정상실행이 되지 않고 이렇게 에러가 뜨는것을 확인할 수 있습니다.

안티디버깅이 의심되므로 우선 IsDebugPresent 부터 찾아봅니다.

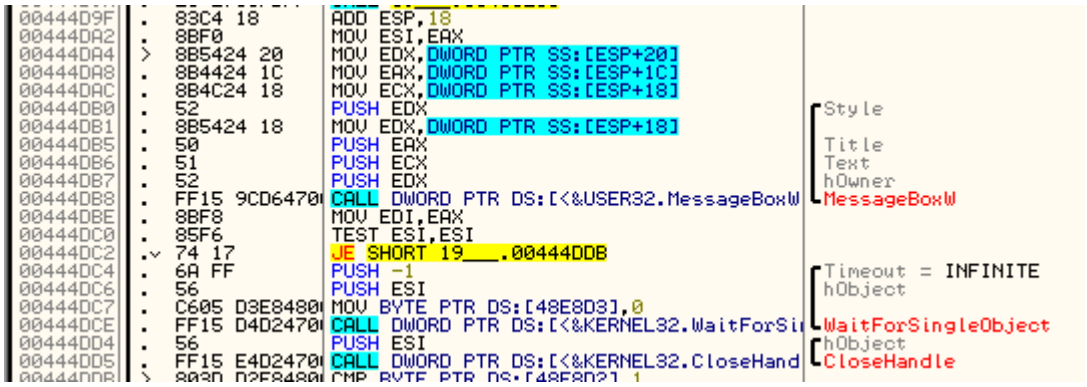


찾아낸 IsDebugPresent 는 TEST EAX EAX 를 실행 후 JNZ 를 통해여 프로그램을 종료시킵니다.



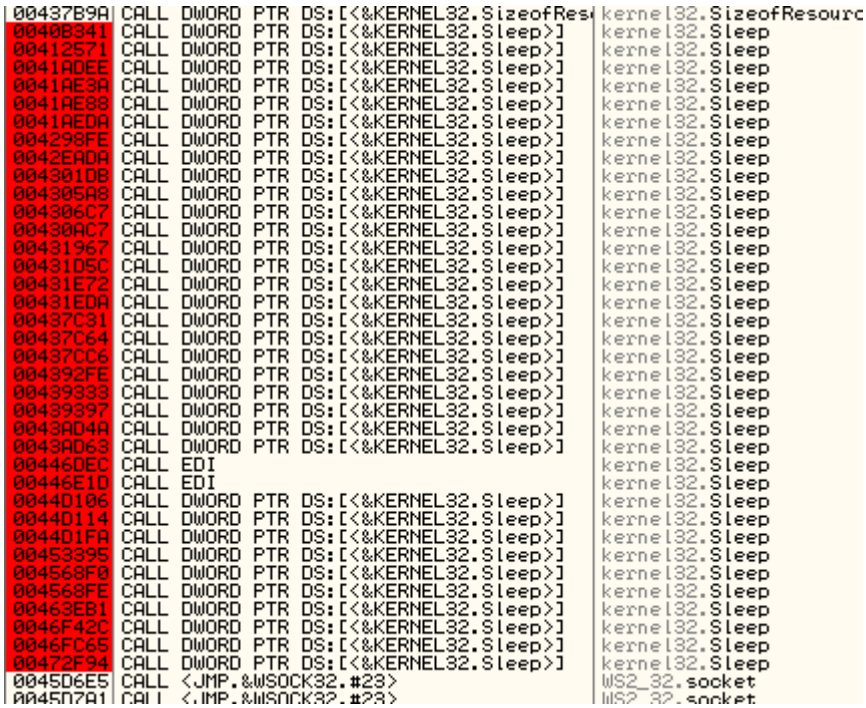
이를 회피하기 위해서는 JNZ 부분을 NOP 으로 처리하여도 되지만

수정하는 부분을 최소화 시키기 위해 TEST 를 XOR 로 바꾸어 회피하도록 하겠습니다.

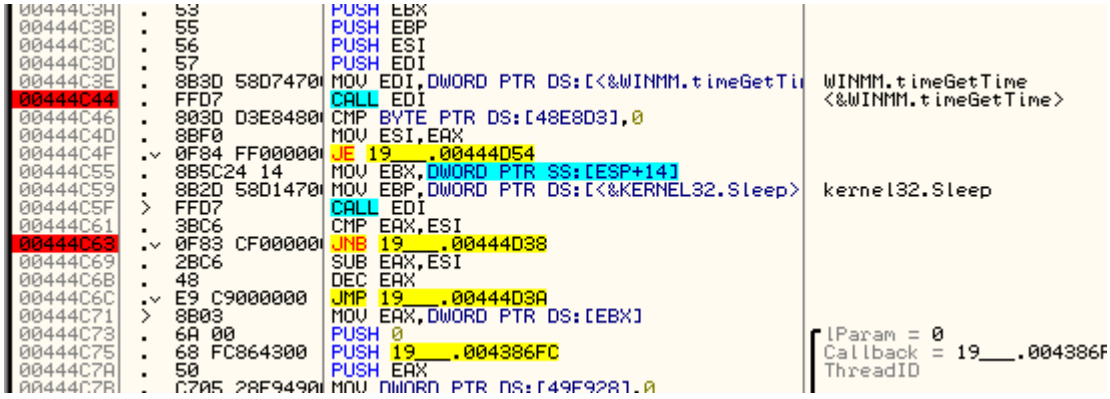


메세지 박스를 만드는 구간입니다만 딱히 시간을 가지고 카운트 하는 부분이 없습니다.

이를 찾기 위하여 함수 리스트에서 시간을 구하거나 Sleep 등을 찾아 모두 Break Point 를 걸어봅니다.



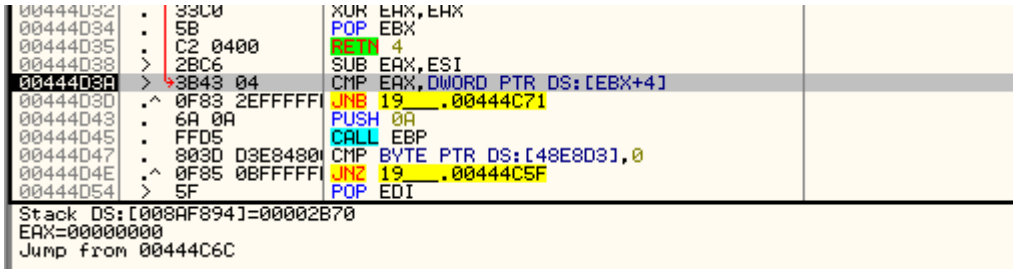
그리고 실행을 하게 되면



이부분에서 실행이 멈추게 됩니다.

우선 TimeGetTime 함수를 통하여 시스템의 시간을 msec 단위로 구한 뒤 이를 ESI 에 보관합니다.

그리고 한번 더 실행하고 EAX 와 ESI 를 비교, EAX 가 ESI 보다 크거나 같으면 JMP 를 하게 됩니다.



그리고 이곳에 도착한 뒤 EAX 에 ESI 를 뺀 뒤 EAX 와 [EBX+4]를 비교연산 합니다.

그리고 EAX 가 [EBX+4] 즉 0x2B70 과 같아질때까지 다시 위로 올라가 CALL EDI 를 통해 EAX 값을 갱신하게 되고 이런식으로 계속 반복연산을 하다가 0x2B70 이상의 값이 되면 CMP 구문 밑의 JNB 를 통하여 프로그램을 종료하는 루틴으로 넘어가게 됩니다.

따라서 이번 문제의 정답은 0x2B70 즉 11120 초가 됩니다.