REPORT:

코드엔진 Basic RCE 19 Writeup

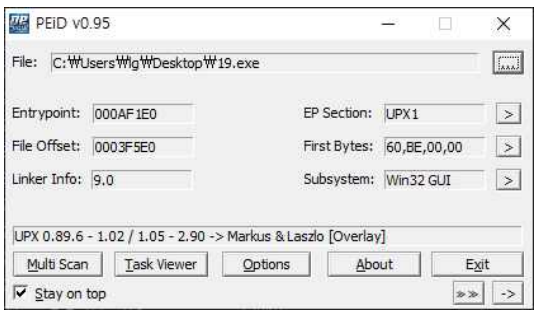
COLONY
1824275 정상지

2021.07.24

이 프로그램은 몇 밀리세컨드 후에 종료되는가

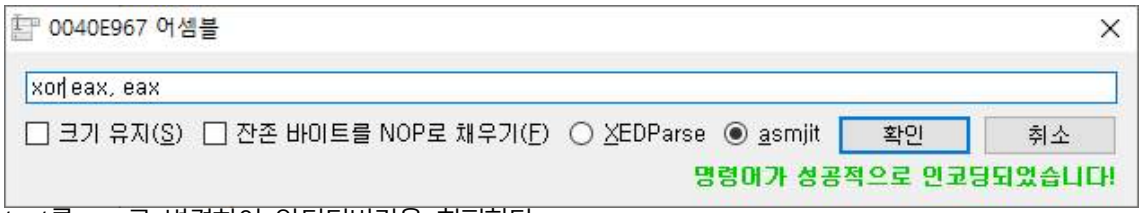
프로그램 실행 시 위와 같이 메시지 박스를 띄워준다

해당 프로그램을 PEid로 확인 결과 upx로 패킹되어있는 것을 볼 수 있다



언패킹 후 프로그램 디버깅 시 정상실행이 되지 않는 것으로 보아 안티디버깅이 있는 것으로 유추할 수 있다

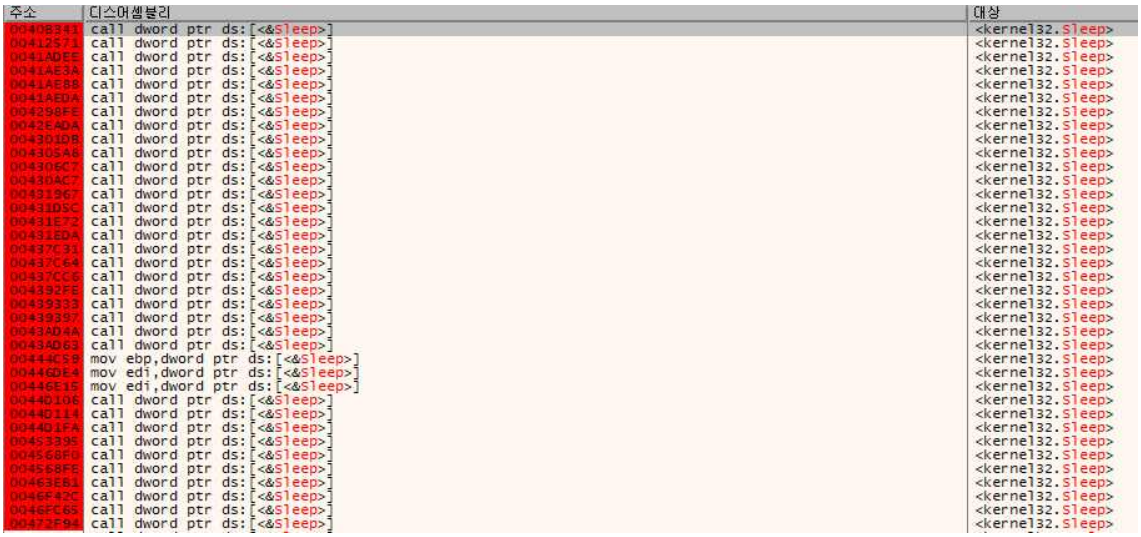
따라서 모듈 간 호출에서 IsDebuggerPresent함수를 발견한다



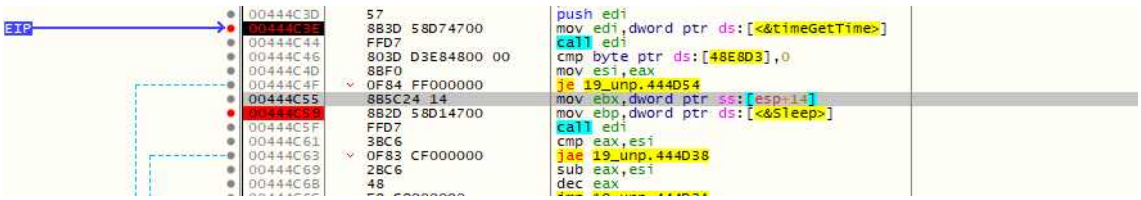
test를 xor로 변경하여 안티디버기을 회피한다

메시지 박스출력 부분을 확인해본 결과 시간을 건드는 함수는 보이지 않는다

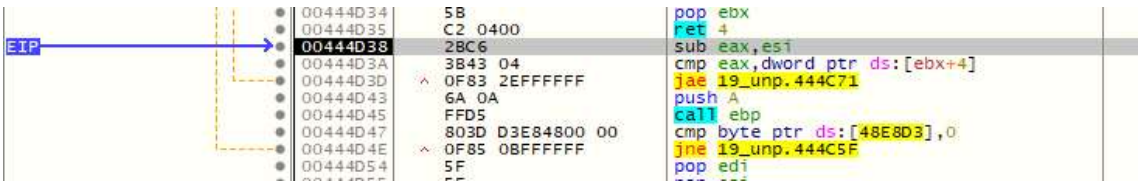
sleep 및 시간과 관련된 함수에 breakpoint를 걸어 확인한다

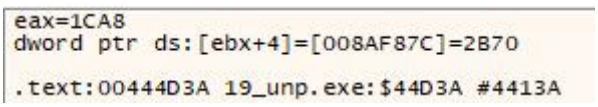


timegettime함수를 통해 시스템의 시간을 esi에 msec로 받아온다
esi에 들어온 값과 eax의 값을 비교하여 eax가 esi보다 크거나 같을 경우 jmp를 실행



jmp 실행 시 넘어오는 곳에서 esi를 뺀 eax와 [ebx+4]와 비교연산





eax는 시스템에서 시간을 받아온 후부터 지금까지의 시간
[ebx+4]는 2B70으로 eax가 2B70의 값을 넘을 때까지 eax값을 갱신하고 해당 값을 넘을 경우 루틴이 종료되는 것을 알 수 있다
0x2B70은 11120이므로

정답 : 11120밀리세컨드