Reverse L04

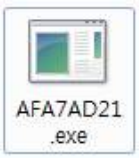
Date : 2010 / 01 / 02
PRIDE

#문제

Korea :
이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디버거를 탐지하는 함수의 이름은 무엇인가

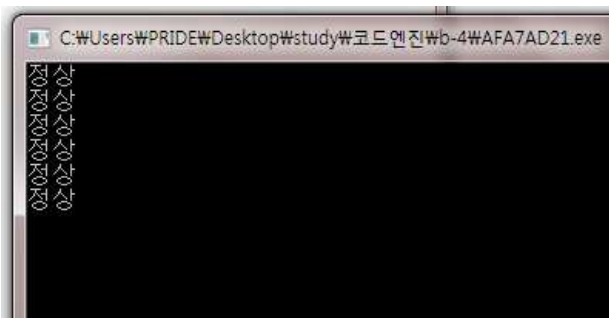
English :
This program can detect debuggers. Find out the name of the debugger detecting function the program uses.

#문제프로그램



#프로그램실행

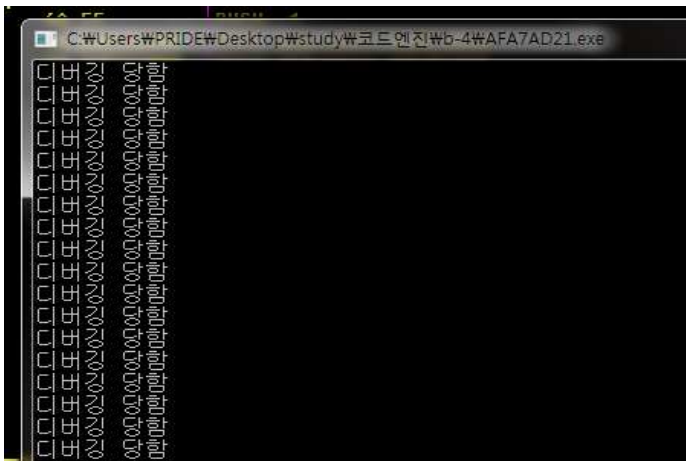
프로그램을 실행했다.



1초마다 정상이라는 문자열만 출력된다. 문제로 미루어보아 디버깅이 감지되면 다른 문자열이 나오도록 한다는 것을 추측할 수 있다.

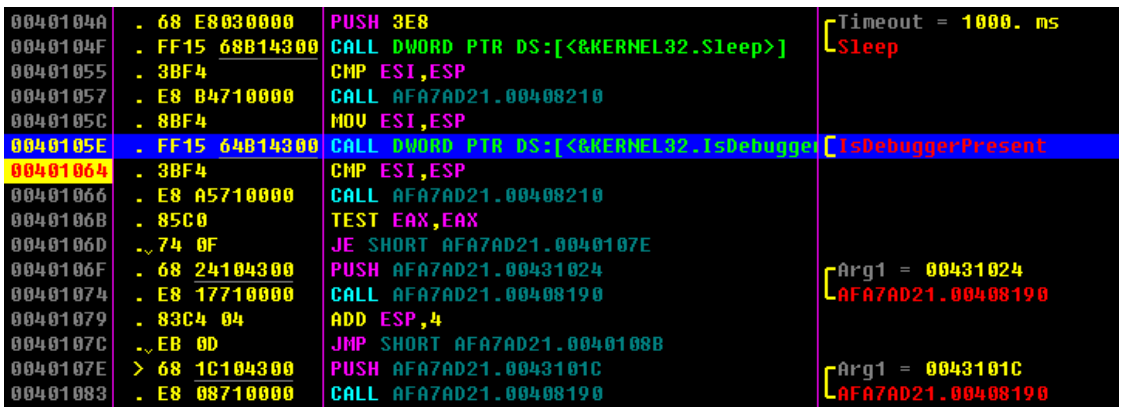
#With Ollydbg

Ollydbg로 해당 프로그램을 열어, F9로 실행시켜보았다.



1초마다 디버깅 당했다는 문자열이 나온다.
문제에서도 알수있지만 디버깅을 감지하는 함수가 있다.
이 디버깅 함수가 디버깅을 감지하면 "디버깅 당함"이라는 문자열을 출력하고,
디버깅을 감지하지 못하면 "정상"이라는 문자열을 출력한다.

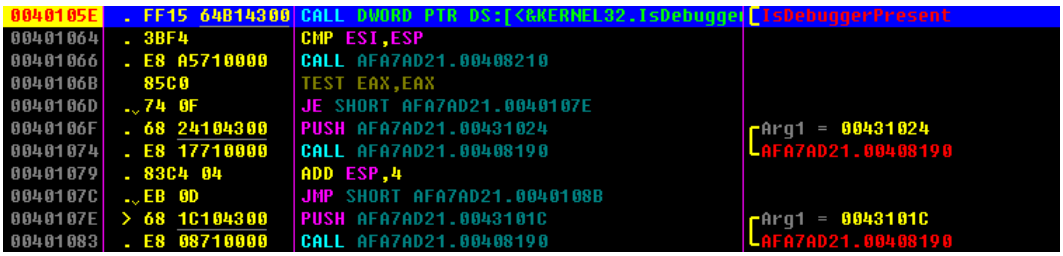
"디버깅 당함"과 "정상" 문자열은 안티디버깅함수와 가까이 있을 것이기 때문에 함수명들을 보기보단 문자열을 참조하는 곳으로 가본다.



0040106F지점에서는 "정상"문자열을 push하고 출력함수를 호출한다.
0040107E지점에서는 "디버깅 당함"문자열을 push하고 출력함수를 호출한다.

그리고 조금 위에는 이름이 엄청나게 디버깅 감지함수처럼 보이는 IsDebuggerPresent함수

가 있다.
그리고 그 위에는 Sleep함수를 호출하는 부분이 있다.
이를 근거로 IsDebuggerPresent함수가 디버깅감지함수라고 추측할 수 있다.
확실하지 않기 때문에 이 부분에 브레이크포인트를 걸고 진행시켜본다.

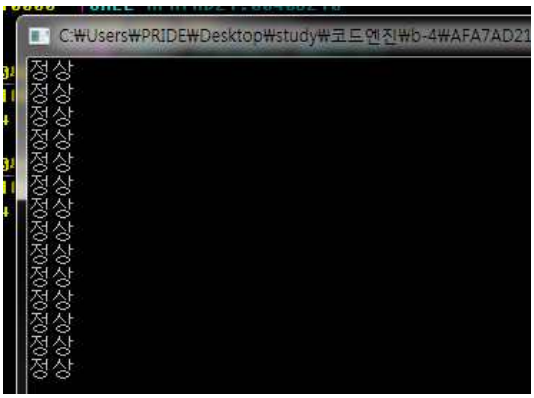


F8로 진행시키게 되면 eax에 리턴된 값이 저장되게된다.
그리고 TEST EAX,EAX연산을 통해 Zero Flag가 1이면 0040107E("정상"문자열 출력부분)로 분기한다.
그러므로 IsDebuggerPresent가 디버깅감지함수임을 확인할 수 있다.
디버깅감지함수 결과값이 있는 eax를 TEST연산을 통해, Zero Flag가 1이면 정상으로 판단하기 때문에 TEST EAX,EAX부분에 Zero Flag가 항상 1이 되도록하는 명령을 넣게되면 항상 정상으로 판단하게 된다. 그러므로 TEST EAX,EAX를 CMP EAX,EAX로 대체한다.

Before

After

진행



정상으로 인식했다.

#답 : IsDebuggerPresent