Basic RCE L04

Korea :

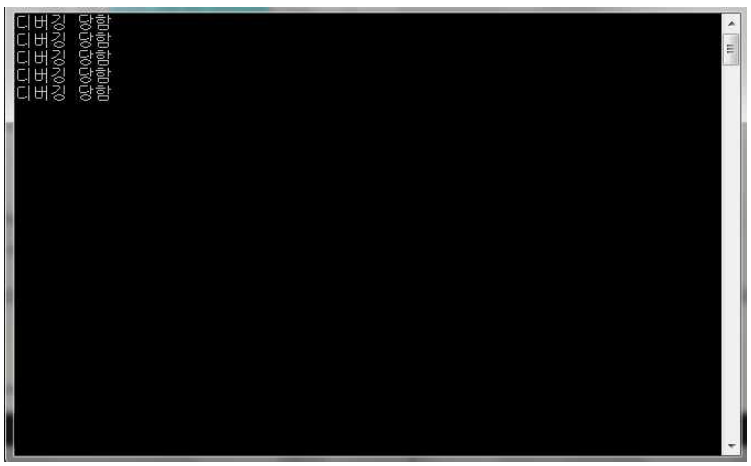
이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디버거를 탐지하는 함수의 이름은 무엇인가

English :

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

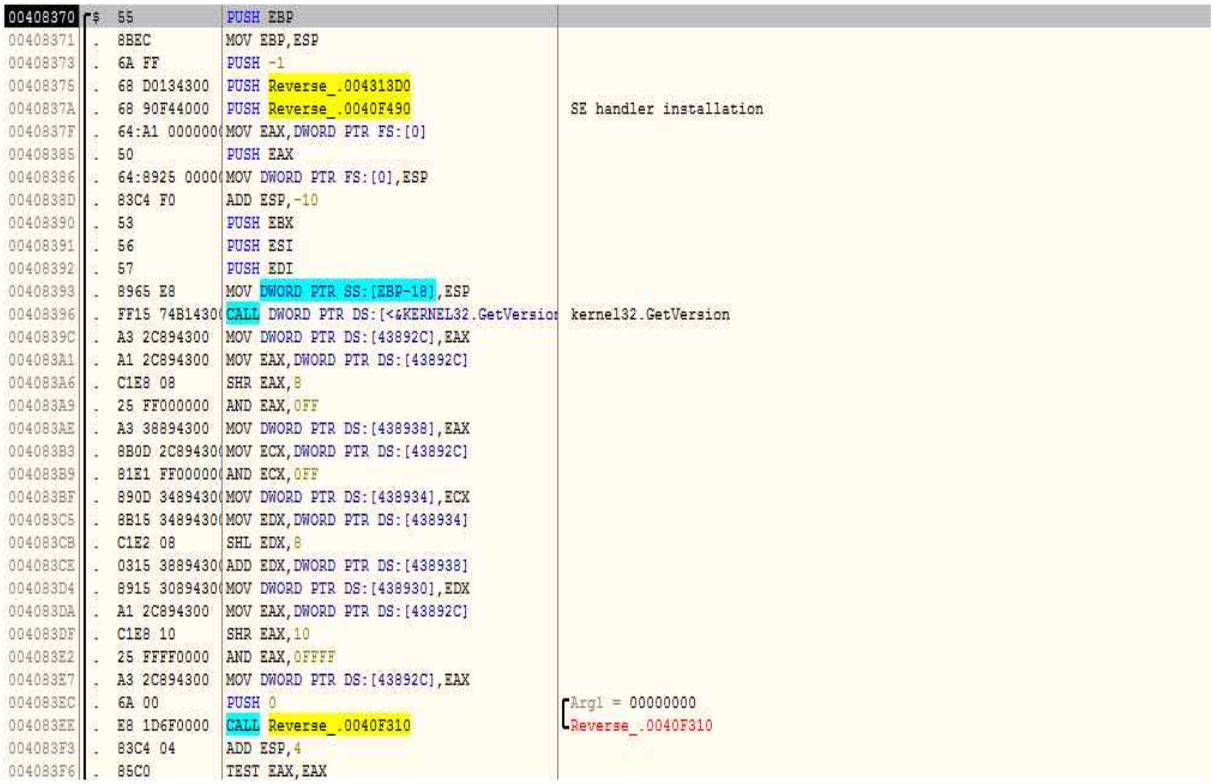
프로그램을 실행시키자.

실행시키니 콘솔창에 정상이라는 메시지가 계속 출력된다. 문제가 디버거 탐지 함수를 구하라는 것이다. 그럼 한번 올리디버거로 디버거를 해보자. F9를 눌러 실행시키기전에는 그저 아무것도 출력하고 있지 않다가 F9를 눌러서 실행 해 보니 디버깅 당함 이라는 메시지가 계속 뜬다.

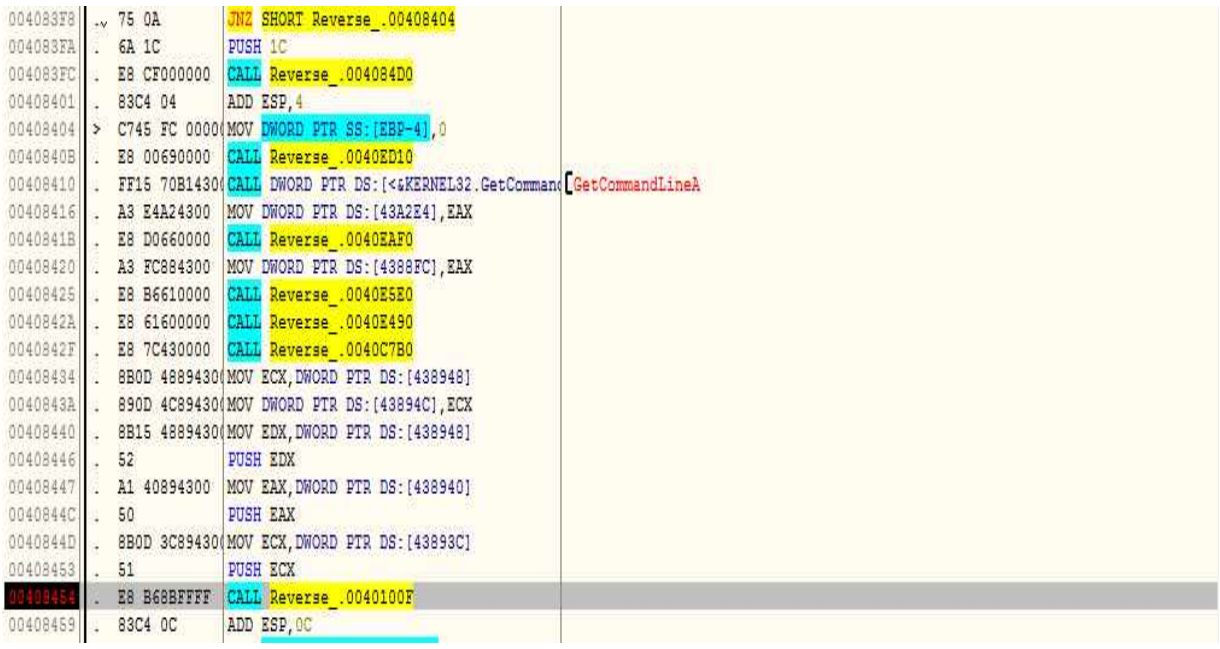


올리디버거로 열엇더니 정상 이라는 메시지에서 디버깅 당함 이라는 메시지로 바뀌었다. 답은 아마도 이렇게 바꿔주는 함수를 찾는 것인가 보다.

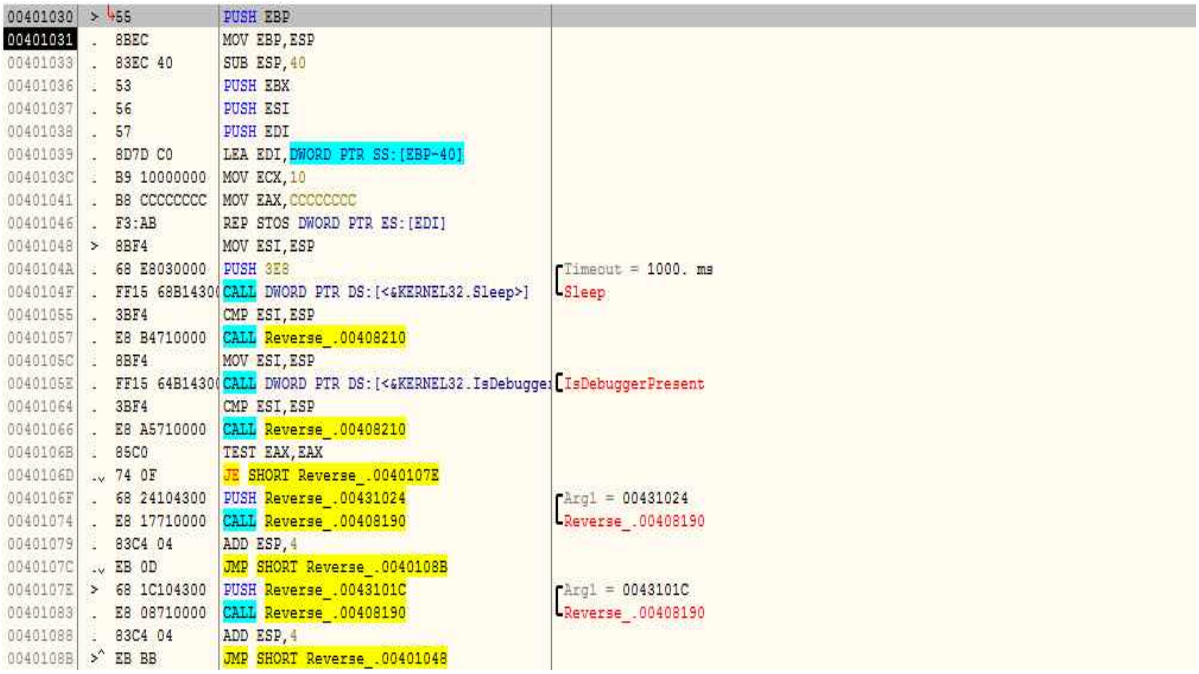
일단 오른쪽키를 눌러 [Search for] - [All referenced text strings]를 눌러 문자열들을 봤다. 하지만 딱히 눈에 보이는건 없었다. API함수들까지 보려고 햇지만 딱히 생각나는 함수가 없어서 그냥 실행하면서 나가기로 했다.
일단 Ctrl + F2를 눌러서 다시 처음화면으로 가보자.



처음 코드는 이곳이다. 뭐 보이는게 별로 없다. 그래서 F8로 한단계씩 실행을 해 봐야 겠다. F8로 한단계씩 실행하거나 꾹 눌러서 실행하다 보면 어느순간 멈추고 콘솔창에는 “디버깅 당함“ 이라는 메시지가 출력될 때가 있을 것이다. 바로 00408454 주소의 CALL Reverse_.0040100F 코드이다. 이곳에 BP를 걸고 다시 Ctrl + F2를 눌러서 처음으로 간후 F9를 눌러보자.



그리고 F7을 눌러서 내부로 들어가보자. 들어가면 JMP Reverse_.00401030 명령어가 보이는데,
점프를 하고나면 이런 코드들이 보일 것이다.



대충 해석을 하자면 Sleep 함수로 1초씩(1000ms, ms = 밀리세컨드 = 1/1000초) 기다리고
IsDebuggerPresent API함수를 호출 한다. 이 함수가 무엇인지 알아보기 위해 마우스 오른쪽키를 눌러 [Help on symbolic name]을 눌러보자. 내 경우엔 win32.hlp 파일에 IsDebuggerPresent 함수에 대한 설명이 없었는지 뜨질 않았다. 그럼 구글링을 해보자. MSDN에 설명되어 있는데,
함수 원형은 BOOL WINAPI IsDebuggerPresent(void); 이고, 인수값은 받질 않으며,

Return Value

If the current process is running in the context of a debugger, the return value is nonzero.

If the current process is not running in the context of a debugger, the return value is zero.

이게 리턴값이다. 해석을 하자면

현재 프로그램이 디버거로 실행 되고 있으면은 0이 아닌값을 리턴한다.

현재 프로그램이 디버거로 실행 되고 있지 않으면은 0을 리턴한다.

해석이 틀렸을 수도 있다. 영어를 잘 못하기에.. 하지만 대충 이런뜻인건 분명한 것 같다.
우리가 찾는 디버깅 탐지 함수가 바로 이 함수인 것 같다. 그걸 말해주듯이 IsDebuggerPresent 함수를 실행시키면은 EAX에 1이 반환되는걸 볼 수 있다. 즉 디버거로 실행 됨을 의미한다.
Continue 칸에 IsDebuggerPresent 를 입력해보자. 5번 문제가 나올 것이다.

2011.08.16

Made by hypen1117
hypen1117@daum.net
http://hypen1117.tistory.com

리버싱을 그렇게 잘하지 못해 구체적이지 못하고 잘못 될 수 있습니다.
잘못되거나 부족한 부분 지적해 주시길 바랍니다.