BASIC RCE Level 4

CodeEngn
ReverseEngineering Conference

2013 07/12
Malcook90@naver.com

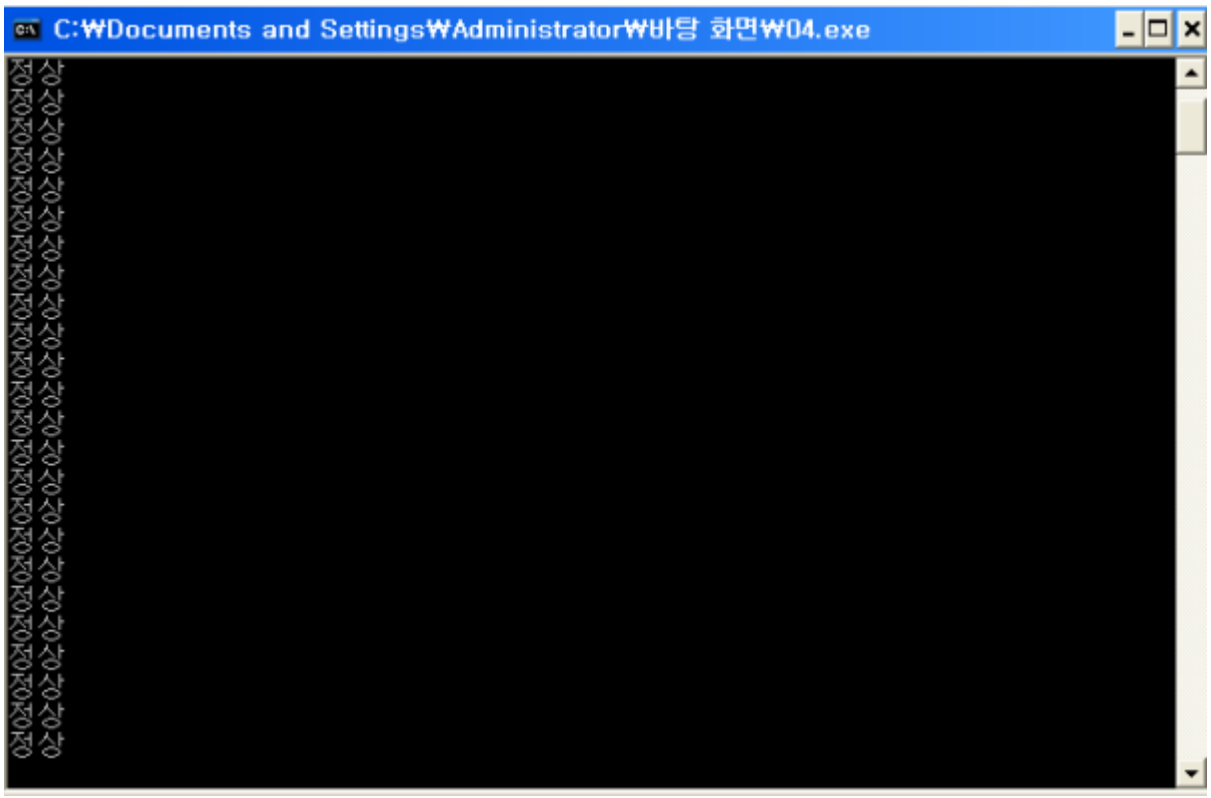
Challenges : Basic 04

Author : CodeEngn

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.

이 또한 검색으로도 충분히 찾을 수 있는 답이지만.. 한번 실행해 보도록 하자



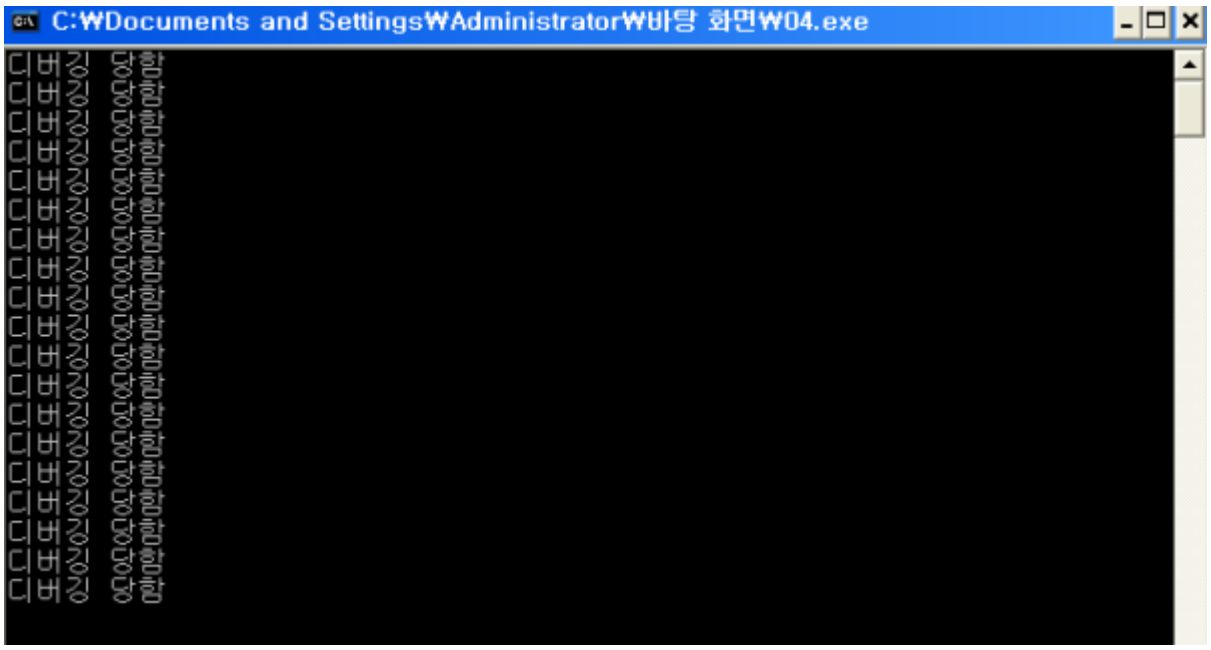
이처럼 매 초마다 '정상' 이라는 문자값을 출력하고 있다.

```
0040842F   .  E8 7C430000    CALL 04.0040C7B0
00408434   .  8B0D 48894300  MOV ECX,DWORD PTR DS:[438948]
0040843A   .  890D 4C894300  MOV DWORD PTR DS:[43894C],ECX
00408440   .  8B15 48894300  MOV EDX,DWORD PTR DS:[438948]
00408446   .  52             PUSH EDX
00408447   .  A1 40894300    MOV EAX,DWORD PTR DS:[438940]
0040844C   .  50             PUSH EAX
0040844D   .  8B0D 3C894300  MOV ECX,DWORD PTR DS:[43893C]
00408453   .  51             PUSH ECX
00408454   .  E8 B68BFFFF    CALL 04.0040100F
00408459   .  83C4 08        ADD ESP,8
0040845C   .  8945 E4        MOV DWORD PTR SS:[EBP-1C],EAX
0040845F   .  8B55 E4        MOV EDX,DWORD PTR SS:[EBP-1C]
00408462   .  52             PUSH EDX
00408463   .  E8 88430000    CALL 04.0040C7F0
00408468   .  8B45 EC        MOV EAX,DWORD PTR SS:[EBP-14]
0040846B   .  8B08           MOV ECX,DWORD PTR DS:[EAX]
0040846D   .  8B11           MOV EDX,DWORD PTR DS:[ECX]
0040846F   .  8955 E0        MOV DWORD PTR SS:[EBP-20],EDX
00408472   .  8B45 EC        MOV EAX,DWORD PTR SS:[EBP-14]
```

OllyDBG 로 open 시켜서 F8 로 하나하나 실행해 나가다 보면

다음과 같은 주소값을 만나게 된다.

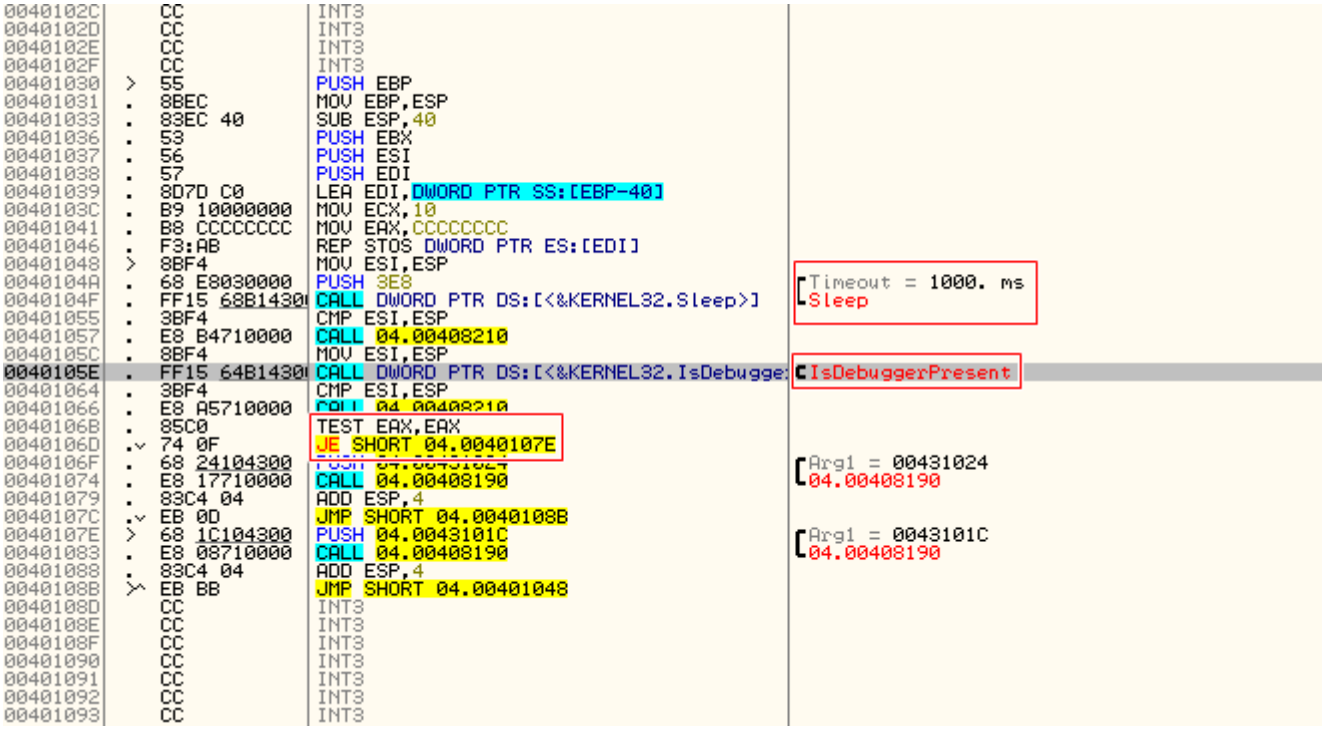
여기서 F8을 누르면...



이렇게 프로그램이 실행되면서 앞으로 더 이상 디버깅이 안된다.

함수 내부로 들어가 보기 위해 주소 [00408454] 에 BP 걸고 F9로 실행시켜

F7 로 코드 내부로 들어가 보도록 하자



스크롤을 조금 내리다 보면 다음과 같은 코드들이 보입니다.

문제에서 찾고자 하는 답인 [IsDebuggerPresent] 라는 함수가 보이네요

또한 Sleep 함수을 사용하여 매 초마다 출력하는 것을 알수 있고,

TEST EAX, EAX 값을 통해 디버깅 판단 유무을 출력하는 것을 알 수 있습니다.

본 지문에서 찾고자 하는 것은 아니기에.. 생략하겠습니다 ^^;