

BASIC RCE Level 4

CodeEngn
ReverseEngineering Conference

2013 07/12

Malcook90@naver.com

Challenges : Basic 04

Author : CodeEngn

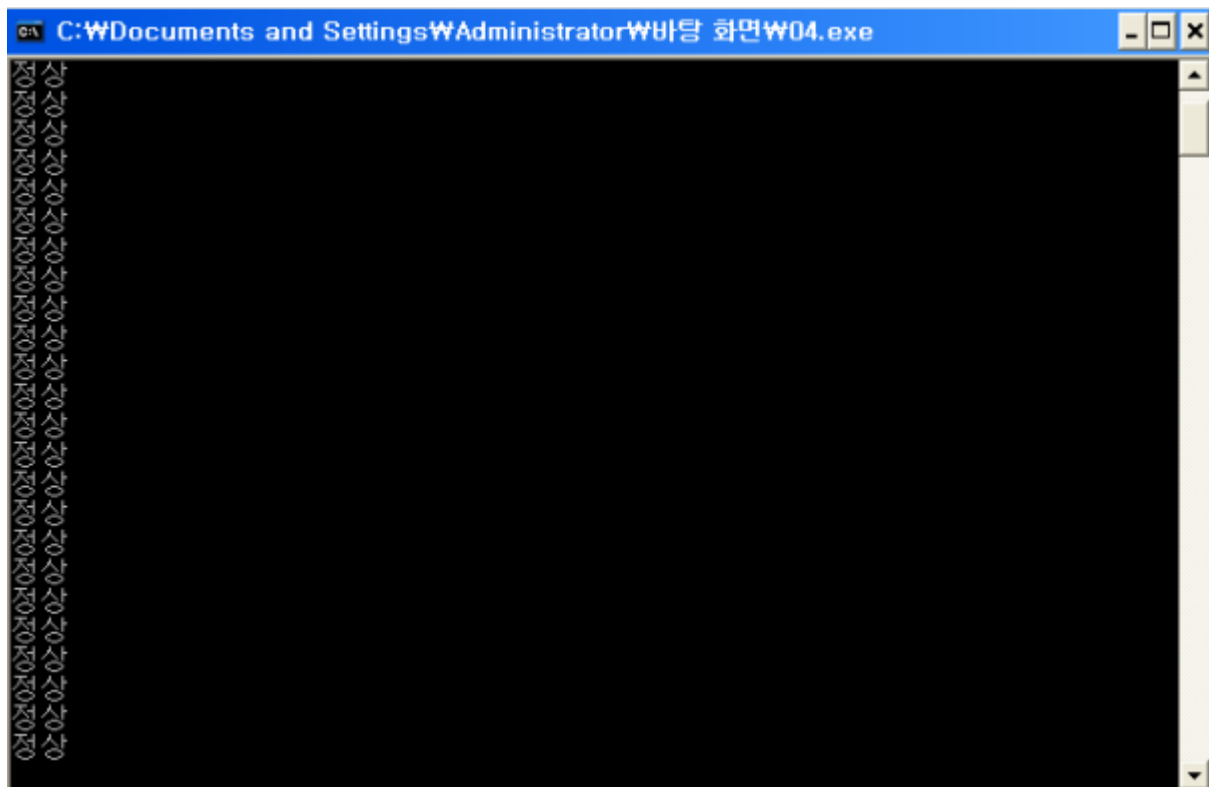
Korea :

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



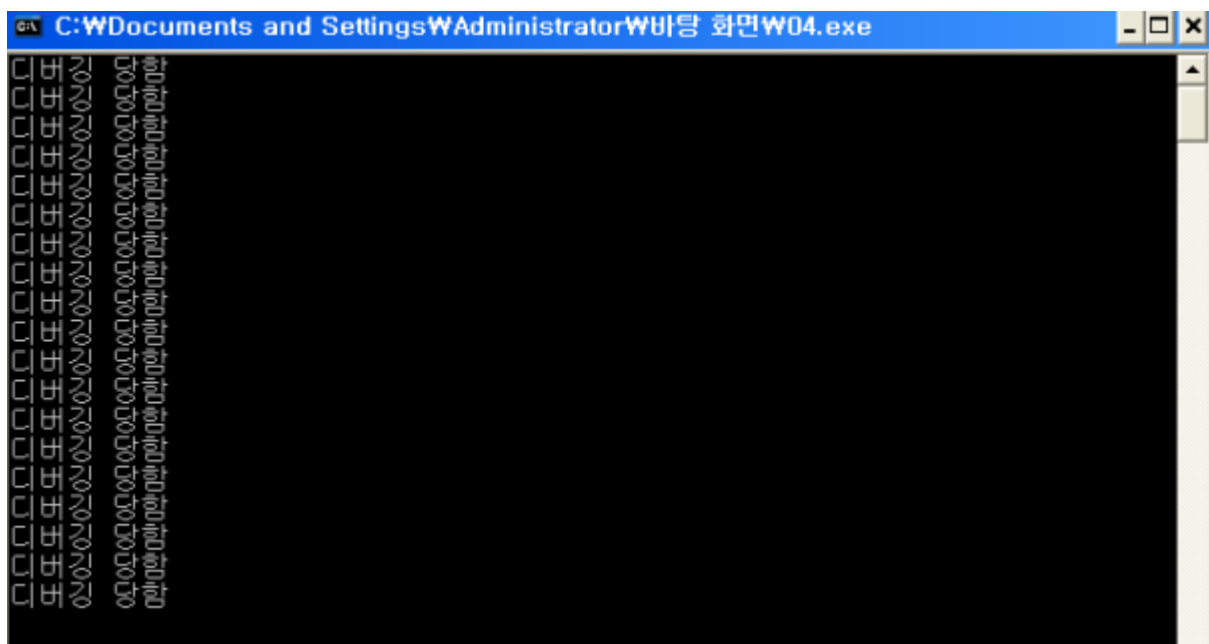
이처럼 매 초마다 '정상' 이라는 문자값을 출력하고 있다.

0040842F	. E8 7C430000	CALL 04.0040C7B0
00408434	. 8B0D 48894301	MOV ECX,DWORD PTR DS:[438948]
0040843A	. 890D 4C894301	MOV DWORD PTR DS:[43894C],ECX
00408440	. 8B15 48894301	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 3C894301	MOV ECX,DWORD PTR DS:[43893C]
00408453	. 51	PUSH ECX
00408454	. E8 B68BFFFF	CALL 04.0040100F
00408457	. 83C4 0C	ADD ESP,0C
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]

OlyDBG 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

0040102C	CC	INT3	
0040102D	CC	INT3	
0040102E	CC	INT3	
0040102F	CC	INT3	
00401030	> 55	PUSH EBP	
00401031	. 8BEC	MOV EBP,ESP	
00401033	. 83EC 40	SUB ESP,40	
00401036	. 53	PUSH EBX	
00401037	. 56	PUSH ESI	
00401038	. 57	PUSH EDI	
00401039	. 8D7D C0	LEA EDI,DWORD PTR SS:[EBP-40]	
0040103C	. B9 10000000	MOV ECX,10	
00401041	. B8 CCCCCCCC	MOV EAX,CCCCCCCC	
00401046	. F3:AB	REP STOS DWORD PTR ES:[EDI]	
00401048	> 8BF4	MOV ESI,ESP	
0040104A	. 68 E8030000	PUSH 3E8	[Timeout = 1000. ms Sleep
0040104F	. FF15 68B14300	CALL DWORD PTR DS:[&KERNEL32.Sleep]	
00401055	. 3BF4	CMP ESI,ESP	
00401057	. E8 B4710000	CALL 04.004008210	
0040105C	. 8BF4	MOV ESI,ESP	
0040105E	. FF15 64B14300	CALL DWORD PTR DS:[&KERNEL32.IsDebuggerPresent]	[IsDebuggerPresent
00401064	. 3BF4	CMP ESI,ESP	
00401066	. E8 A5710000	CALL 04.004008210	
0040106B	. 85C0	TEST EAX,EAX	
0040106D	> 74 0F	JE SHORT 04.0040107E	
0040106F	. 68 24104300	PUSH 27.00731027	[Arg1 = 00431024 04.004008190
00401074	. E8 17710000	CALL 04.004008190	
00401079	. 83C4 04	ADD ESP,4	
0040107C	> EB 0D	JMP SHORT 04.0040108B	
0040107E	. 68 1C104300	PUSH 04.0043101C	[Arg1 = 0043101C 04.004008190
00401083	. E8 08710000	CALL 04.004008190	
00401088	. 83C4 04	ADD ESP,4	
0040108B	> EB BB	JMP SHORT 04.00401048	
0040108D	CC	INT3	
0040108E	CC	INT3	
0040108F	CC	INT3	
00401090	CC	INT3	
00401091	CC	INT3	
00401092	CC	INT3	
00401093	CC	INT3	

스크롤을 조금 내리다 보면 다음과 같은 코드들이 보입니다.

문제에서 찾고자 하는 답인 [IsDebuggerPresent] 라는 함수가 보이네요

또한 Sleep 함수를 사용하여 매 초마다 출력하는 것을 알수 있고,

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

본 지문에서 찾고자 하는 것은 아니기에.. 생략하겠습니다 ^^;