

19.02.11 CodeEngn Basic RCE L04

Tree to Tree

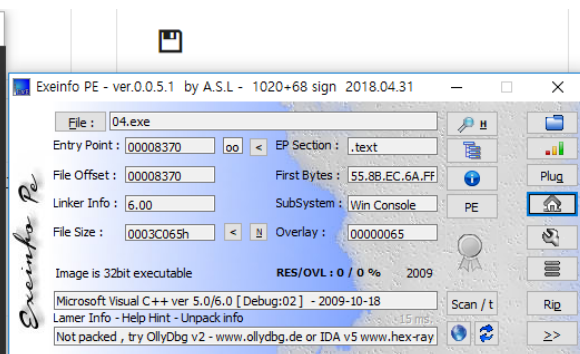
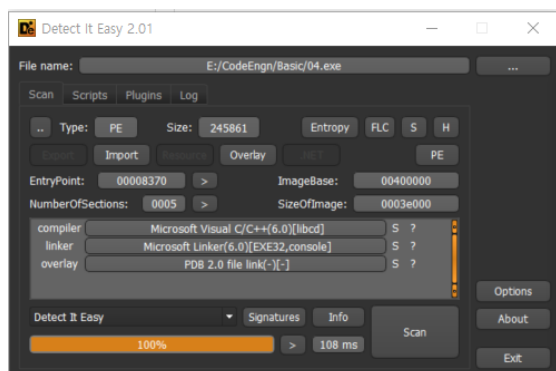
Basic RCE L04

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

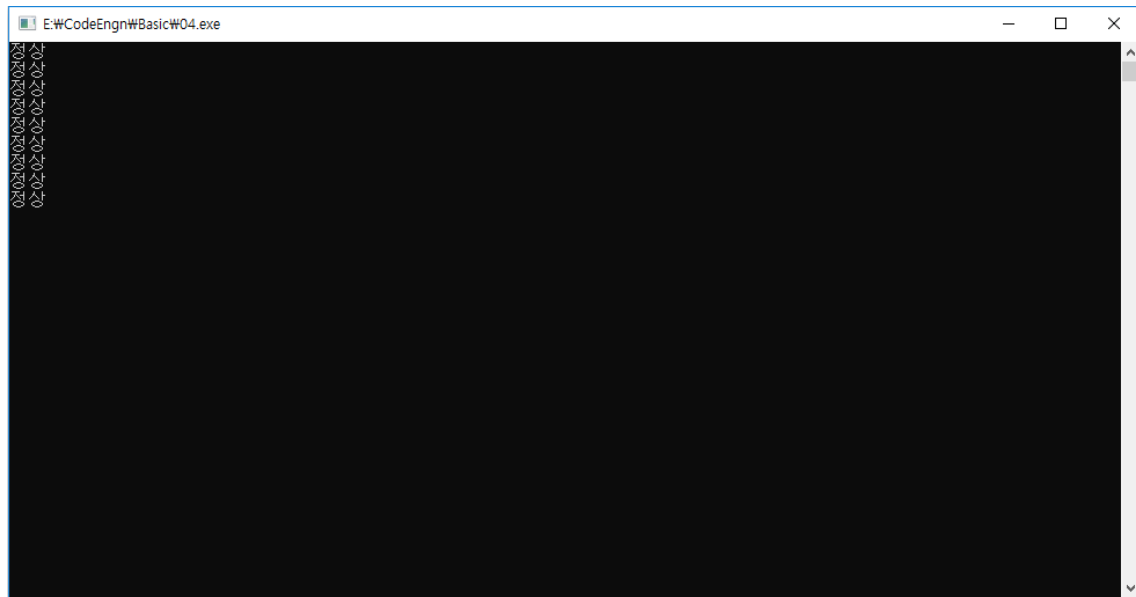
— Author: CodeEngn
— File Password: codeengn



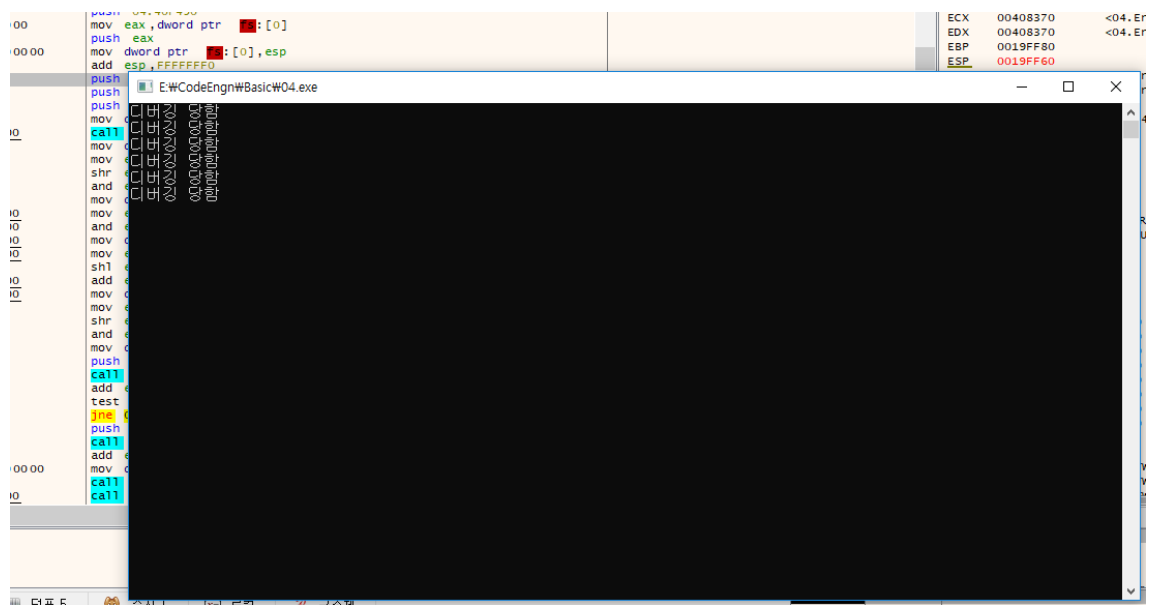
우선 PE분석기로 분석 해보니까 별다른 패킹은 되어있지 않다.



실행하니 정상이라는 문구가 계속 나옴
계속 체크한다는 것을 알 수 있음



디버거로 실행하니 디버깅 당함이라는 문구가 계속 나온다.



PE view로 Section .idata IMPORT Name Table을 보니
PEB값을 활용하는 기본 디버깅 API IsDebuggerPresent()가 보인다.

pFile	Data	Description	Value
00039C00	00039C00	HintName RVA	022A IsDebuggerPresent
00039C0C	00039C0A	HintName RVA	0345 Sleep
00039C30	00039C2A	HintName RVA	026B MultiByteToWideChar
00039C34	00039C29	HintName RVA	0108 GetCommandLineA
00039C38	00039C2F	HintName RVA	010E GetVersion
00039C3C	00039C30	HintName RVA	00AF ExitProcess
00039C40	00039C3E	HintName RVA	02CC RollWindow
00039C44	00039C3A	HintName RVA	0200 RaiseException
00039C48	00039C2C	HintName RVA	022C SetLastErrorPtr
00039C4C	00039C3C	HintName RVA	0229 SetLastErrorPtr
00039C50	00039C4C	HintName RVA	0216 HeapValidate
00039C54	00039C5C	HintName RVA	0351 TerminateProcess
00039C58	00039C70	HintName RVA	013A GetCommProcess
00039C5C	00039C84	HintName RVA	0073 DebugBreak
00039C60	00039C92	HintName RVA	01B1 GetStdHandle
00039C64	00039C92	HintName RVA	0297 WaitFor
00039C68	00039C9E	HintName RVA	021E InterlockedDecrement
00039C6C	00039C9E	HintName RVA	0283 OutputDebugStringA
00039C70	00039C9C	HintName RVA	0198 GetProcAddress
00039C74	00039C9E	HintName RVA	0240 LoadLibraryA
00039C78	00039C9E	HintName RVA	0222 InterlockedIncrement
00039C7C	00039C9E	HintName RVA	0175 GetModuleFileNameA
00039C80	00039C9C	HintName RVA	03C2 UnhandledExceptionFilter
00039C84	00039C9E	HintName RVA	00ED FreeEnvironmentStringsA
00039C88	00039C9E	HintName RVA	00EC FreeEnvironmentStringsW
00039C8C	00039C9C	HintName RVA	0389 WideCharToMultiByte
00039C90	00039C9E	HintName RVA	014D GetEnvironmentStrings
00039C94	00039C9E	HintName RVA	014F GetEnvironmentStringsW
00039C98	00039C9C	HintName RVA	0119 SelfLockCount
00039C9C	00039C9E	HintName RVA	015E GetFileType
00039CA0	00039C9E	HintName RVA	014F GetStartupInfoA
00039CA4	00039C9E	HintName RVA	0177 GetModuleHandleA
00039CA8	00039C9E	HintName RVA	0150 GetEnvironmentVariableA
00039CAC	00039C9E	HintName RVA	01DF GetVersionExA
00039CAE	00039C9E	HintName RVA	0204 HeapDestroy
00039CB0	00039C9E	HintName RVA	0208 HeapCreate
00039CB4	00039C9E	HintName RVA	020C HeapFree
00039CB8	00039C9E	HintName RVA	0178 VirtualFree
00039CB8	00039C9E	HintName RVA	0169 GetLastError
00039CB8	00039C9E	HintName RVA	0110 SelfFlush
00039CB8	00039C9E	HintName RVA	00EC FlushFileBuffers
00039CB8	00039C9E	HintName RVA	002E CloseHandle
00039CB8	00039C9E	HintName RVA	0330 SetUnhandledExceptionFilter
00039CB8	00039C9E	HintName RVA	0206 HeapAlloc
00039CB8	00039C9E	HintName RVA	0210 HeapReAlloc
00039CB8	00039C9E	HintName RVA	0215 VirtualAlloc
00039CB8	00039C9E	HintName RVA	00E3 GetConsoleCtrlHandler
00039CB8	00039C9E	HintName RVA	00FC GetCPInfo
00039CB8	00039C9E	HintName RVA	00F5 GetACP
00039CB8	00039C9E	HintName RVA	018B GetOEMCP
00039CB8	00039C9E	HintName RVA	0226 SetLastErrorPtr

바로 따라가보자

00401000	CC	int3		EAX	0034D000
00401001	CC	int3		EBX	0034D000
00401002	CC	int3		ECX	00A51735
00401003	CC	int3		EDX	00000000
00401004	CC	int3		EBP	0019FF40
00401005	64: A1. 30.00.00.00	mov eax, dword ptr [30]		ESP	0019FEF0
00401006	0F 64 02	movzx eax, byte ptr [eax+2]	IsDebuggerPresent	ESI	0019FEF4
00401007	C3	ret		EDI	0019FF40
00401008	CC	int3			
00401009	CC	int3			
0040100A	CC	int3			

PEB structure

12/05/2018 • 2 minutes to read

[This structure may be altered in future versions of Windows.]

Contains process information.

Syntax

C++Copy

```
typedef struct _PEB {
    BYTE Reserved1[2];
    BYTE BeingDebugged;
    BYTE Reserved2[1];
    PVOID Reserved3[2];
    PPEB_LDR_DATA Ldr;
    PRTL_USER_PROCESS_PARAMETERS ProcessParameters;
    PVOID Reserved4[3];
    PVOID AtlThunkSListPtr;
    PVOID Reserved5;
    ULONG Reserved6;
    PVOID Reserved7;
    ULONG Reserved8;
    ULONG AtlThunkSListPtr32;
    PVOID Reserved9[45];
    BYTE Reserved10[96];
    PPS_POST_PROCESS_INIT_ROUTINE PostProcessInitRoutine;
    BYTE Reserved11[128];
    PVOID Reserved12[1];
    ULONG SessionId;
} PEB, *PPEB;
```