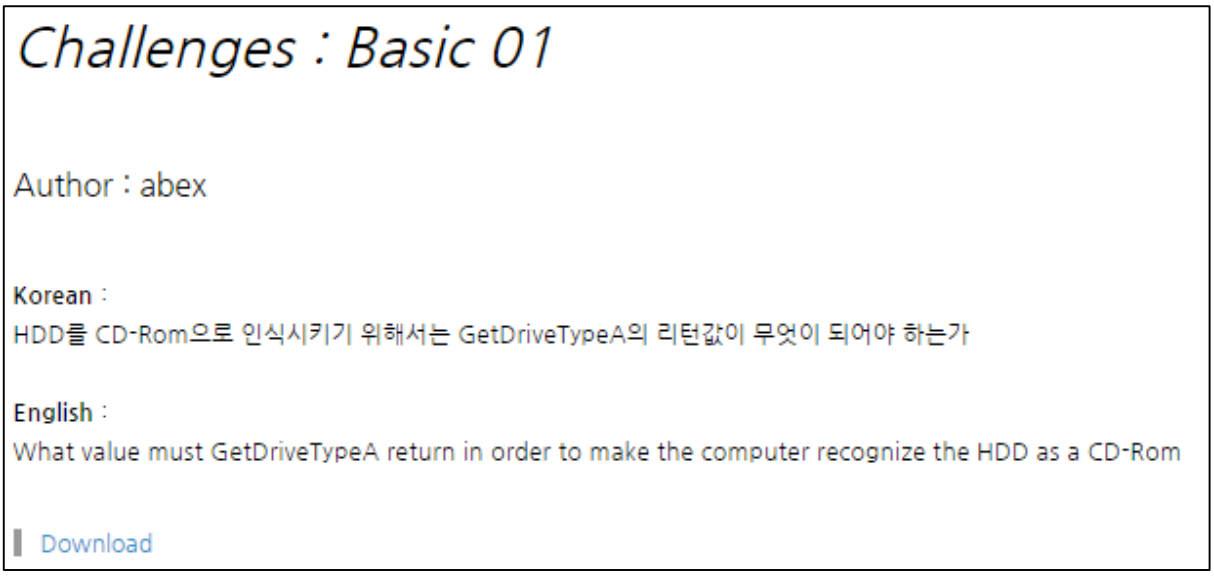
Code Engn Challenges : Basic 01 풀이 보고서

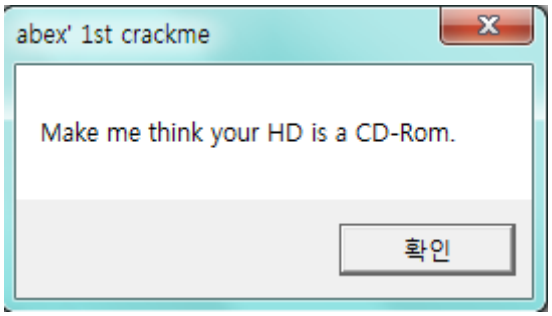
blinglnav

문제



풀이

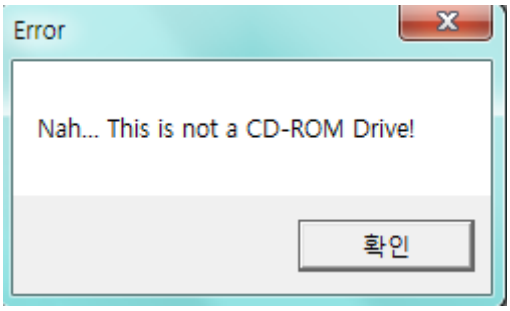
멀웨어 분석이 아닌 이상 리버싱 문제의 경우는 main 함수 또는 이벤트 핸들러를 찾는데 있어 프로그램 상에 출력되는 문자열은 좋은 힌트가 되기 때문에 일단 실행해봅니다.



<너의 HD를 CD-Rom으로 인식하게 만들어라>

HD는 CD-Rom으로 추정해보건데 아마도 Hard Disk 같군요.

여기서 확인 버튼을 누르면



<나...*(?)* 이건 CD-ROM 드라이버 아님>

CD-Rom이 아니라면서 찡찡댑니다.

확인 버튼을 누르면 꺼집니다.

이제 OllyDBG로 열어서 분석을 해보도록 하겠습니다.

어셈블리로 프로그래밍 되었는지 코드가 굉장히 깔끔합니다.

```
$  6A 00          PUSH 0                          Style = MB_OK|MB_APPLMODAL
.  68 00204000    PUSH 00402000                   Title = "abex' 1st crackme"
.  68 12204000    PUSH 00402012                   Text = "Make me think your HD is a CD-Rom."
.  6A 00          PUSH 0                          hOwner = NULL
.  E8 4E000000    CALL <JMP.&USER32.MessageBoxA>  MessageBoxA
.  68 94204000    PUSH 00402094                   RootPathName = "c:\\"
.  E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>  GetDriveTypeA
.  46             INC ESI
.  48             DEC EAX                         kernel32.BaseThreadInitThunk
.  EB 00          JMP SHORT 00401021
>  46             INC ESI
.  46             INC ESI
.  48             DEC EAX                         kernel32.BaseThreadInitThunk
.  3BC6           CMP EAX,ESI
.  74 15          JE SHORT 0040103D
.  6A 00          PUSH 0                          Style = MB_OK|MB_APPLMODAL
.  68 35204000    PUSH 00402035                   Title = "Error"
.  68 3B204000    PUSH 0040203B                   Text = "Nah... This is not a CD-ROM Drive!"
.  6A 00          PUSH 0                          hOwner = NULL
.  E8 26000000    CALL <JMP.&USER32.MessageBoxA>  MessageBoxA
.  EB 13          JMP SHORT 00401050
>  6A 00          PUSH 0                          Style = MB_OK|MB_APPLMODAL
.  68 5E204000    PUSH 0040205E                   Title = "YEAH!"
.  68 64204000    PUSH 00402064                   Text = "Ok, I really think that your HD is a CD-ROM! :p"
.  6A 00          PUSH 0                          hOwner = NULL
.  E8 11000000    CALL <JMP.&USER32.MessageBoxA>  MessageBoxA
>  E8 06000000    CALL <JMP.&KERNEL32.ExitProcess>  ExitProcess
$- FF25 50304000  JMP [<&KERNEL32.GetDriveTypeA>]  kernel32.GetDriveTypeA
.- FF25 54304000  JMP [<&KERNEL32.ExitProcess>]  kernel32.ExitProcess
$- FF25 5C304000  JMP [<&USER32.MessageBoxA>]  USER32.MessageBoxA
   00             DB 00
```

00401013~00401018을 보면 "C:₩₩"를 GetDriveTypeA() 함수의 Parameter로 주어 실행하는 것을 볼 수 있습니다.

```
0040100E  .  E8 4E000000    CALL <JMP.&USER32.MessageBoxA>  MessageBoxA
00401013  .  68 94204000    PUSH 00402094                   RootPathName = "c:\\"
00401018  .  E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>  GetDriveTypeA
0040101D  .  46             INC ESI
```

GetDriveTypeA()는 어떤 함수인지 MSDN(~~MSDN는 개발자의 영원한 친구~~)에 검색해봅니다.

GetDriveType function

Determines whether a disk drive is a removable, fixed, CD-ROM, RAM disk, or network drive.

To determine whether a drive is a USB-type drive, call **SetupDiGetDeviceRegistryProperty** and specify the **SPDRP_REMOVAL_POLICY** property.

<GetDriveType 함수: 디스크 드라이브가 removable인지, fixed인지, CD-ROM인지, RAM 디스크인지, Network 드라이브인지 결정한다>

Parameter는 아래와 같습니다.

C++

```
UINT WINAPI GetDriveType(
  _In_opt_  LPCTSTR lpRootPathName
);
```

Parameters

lpRootPathName [in, optional]

The root directory for the drive.

A trailing backslash is required. If this parameter is **NULL**, the function uses the root of the current directory.

<lpRootPathName. Root Directory를 parameter로 받습니다>

올리로 봤을 때, "C:₩₩"를 parameter로 주었으므로 Virtual Addr 00401013~00401018에서 호출하는 GetDriveTypeA()는 결국 C: 드라이브의 드라이브 타입을 얻는 함수입니다.

문제에서는 HDD를 CD-ROM으로 인식시키기 위한 GetDriveTypeA()의 리턴값을 요구하고 있습니다.
MSDN GetDriveTypeA() Return 항목을 보면 아래와 같이 잘 정리되어있습니다.

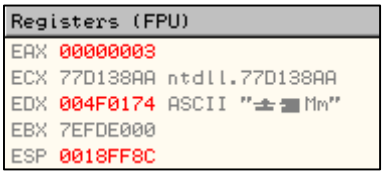
Return value

The return value specifies the type of drive, which can be one of the following values.

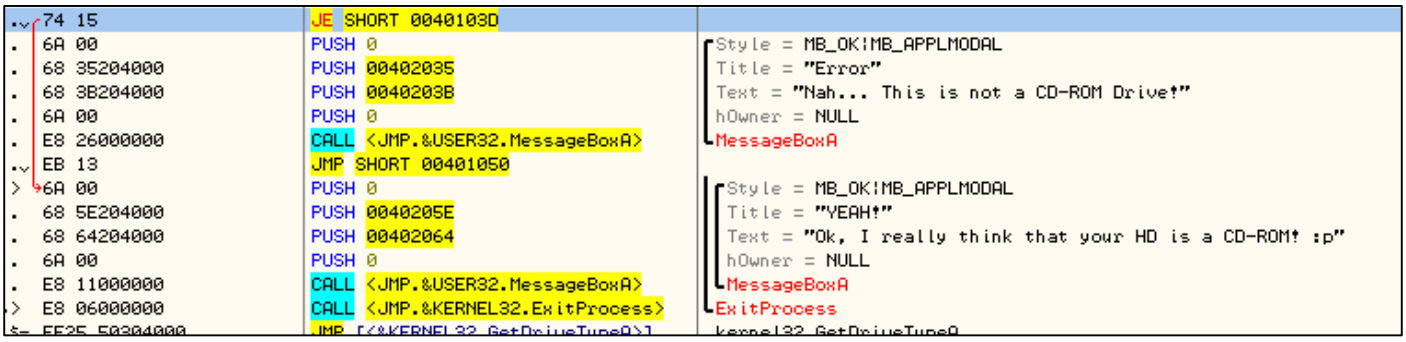
Return code/value	Description
DRIVE_UNKNOWN 0	The drive type cannot be determined.
DRIVE_NO_ROOT_DIR 1	The root path is invalid; for example, there is no volume mounted at the specified path.
DRIVE_REMOVABLE 2	The drive has removable media; for example, a floppy drive, thumb drive, or flash card reader.
DRIVE_FIXED 3	The drive has fixed media; for example, a hard disk drive or flash drive.
DRIVE_REMOTE 4	The drive is a remote (network) drive.
DRIVE_CDROM 5	The drive is a CD-ROM drive.
DRIVE_RAMDISK 6	The drive is a RAM disk.

따라서 문제의 답은 5가 되긴 하는데요...
여기서 끝내면 재미가 없으니까 여러가지 방법을 통해 CD-ROM으로 인식하도록 해보겠습니다.

1) 리턴값 수정
문제에서 요구한 풀이 방법입니다. GetDriveTypeA() 함수의 리턴값을 수정하여 CD-ROM으로 인식하게 하는 것입니다.



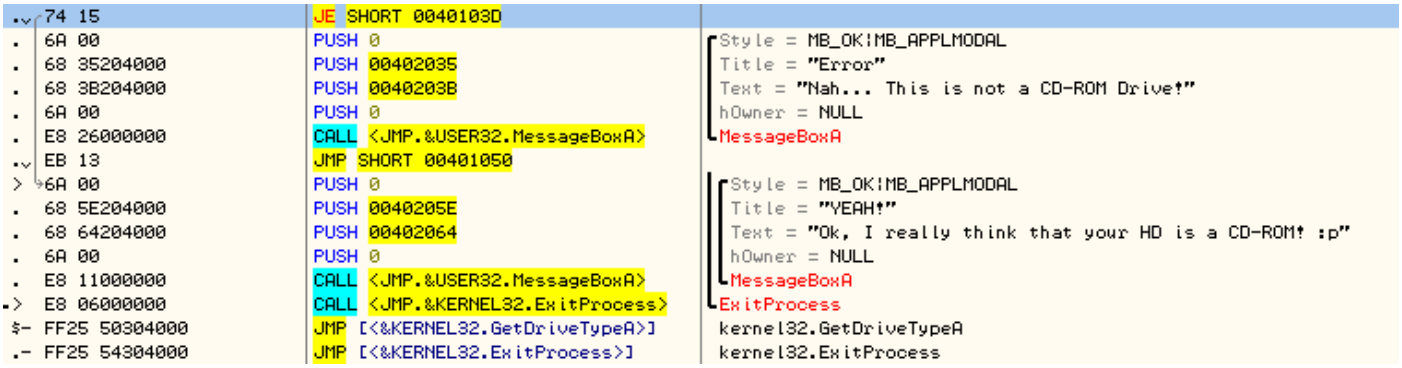
GetDriveTypeA() 함수를 통과한 직후 Registers의 모습입니다.
EAX가 3으로 바뀐 것을 알 수 있습니다. 위에서 본 MSDN GetDriveTypeA() Return에 의하면 3은 DRIVE_FIXED를 의미합니다. C:는 고정된 드라이브이니 올바른 리턴값입니다.
이제 EAX를 더블클릭하여 5(DRIVE_CDROM)로 바꾸어줍니다.



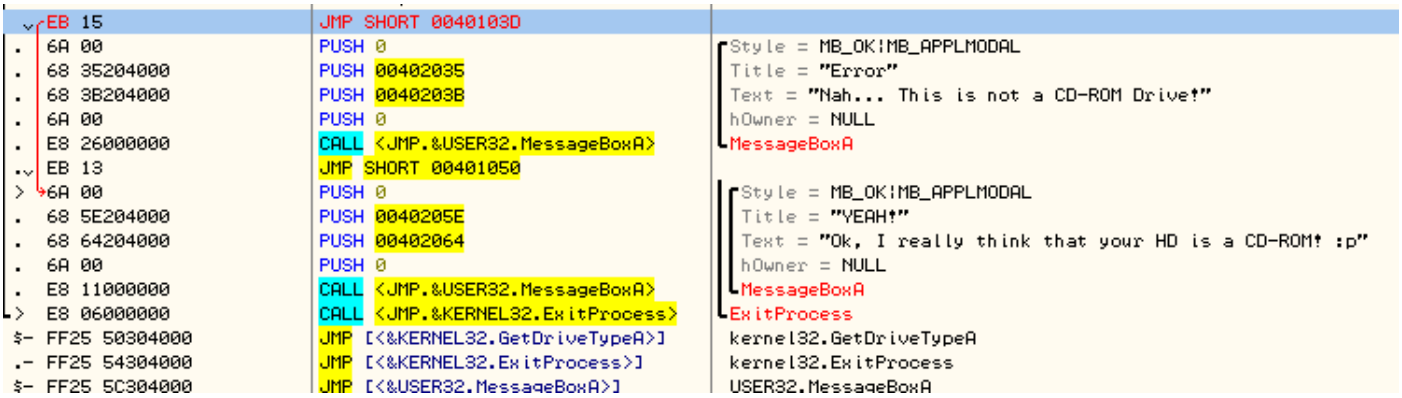
이제 아래쪽으로 분기되는 것을 확인할 수 있습니다.

2) JE 수정
2번은 단순 무식한 방법입니다. 어셈블리 코드를 수정하는 방법이라 보통 리버싱 문제에서는 잘 쓰이지 않습니다. (프로그램 크랙 만들때나 간간히 쓰일 듯 합니다. 근데 크랙은 불법ㅋ)

그냥 쭉쭉 내려오면 분기되지 않고 바로 다음 명령어가 수행되는 것을 볼 수 있습니다.



해당 JE 명령어 위치에서 [SPACE] 키를 눌러 JE를 JMP로 수정합니다.



이제 분기됩니다.

어쨌든 Auth Key는 5