

Reverse_L01.exe 문제

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가?

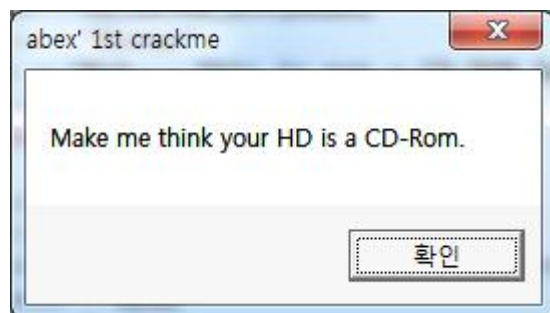
Address	Disassembly	Comment
00401000	PUSH 0	
00401002	PUSH Reverse_.00402000	
00401007	PUSH Reverse_.00402012	
0040100C	PUSH 0	
0040100E	CALL <JMP.&USER32.MessageBox>	
00401013	PUSH Reverse_.00402094	
00401018	CALL <JMP.&KERNEL32.GetDriveTypeA>	
0040101D	INC ESI	
0040101E	DEC EAX	
0040101F	JMP SHORT Reverse_.00401021	
00401021	INC ESI	
00401022	INC ESI	
00401023	DEC EAX	
00401024	CMP EAX, ESI	
00401026	JE SHORT Reverse_.0040103D	
00401028	PUSH 0	
0040102A	PUSH Reverse_.00402035	
0040102F	PUSH Reverse_.0040203B	
00401034	PUSH 0	
00401036	CALL <JMP.&USER32.MessageBox>	
0040103B	JMP SHORT Reverse_.00401050	
0040103D	PUSH 0	
0040103F	PUSH Reverse_.0040205E	
00401044	PUSH Reverse_.00402064	
00401049	PUSH 0	
0040104B	CALL <JMP.&USER32.MessageBox>	
00401050	CALL <JMP.&KERNEL32.ExitProcess>	
00401055	JMP DWORD PTR DS:[&KERNEL32.GetDriveTypeA]	
0040105B	JMP DWORD PTR DS:[&KERNEL32.ExitProcess]	
00401061	JMP DWORD PTR DS:[&USER32.MessageBox]	
00401067	DB 00	
00401068	DB 00	

Register	Value
EAX	74E53378
ECX	00000000
EDX	00401000
EBX	7EFD0000
ESP	0010FF0C
EBP	0010FF94
ESI	00000000
EDI	00000000
EIP	00401000
EFL	00000246

[그림 1] OllyDbg로 Open한 모습

위 코드를 분석해보면

- 0040100E에서 MessageBoxA를 CALL한다.
Title : "abex' 1st crackme"
Text : "Make me think your HD is a CD-Rom."



[그림 2] MessageBoxA

2. 00401018에서 GetDriveTypeA 함수를 CALL한다.

RootPathName : "c:\\"

GetDriveTypeA 함수의 리턴값은 다음과 같다

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.

[그림 3] GetDriveType 함수의 리턴 값⁽¹⁾

내 컴퓨터의 c:\는 HDD이기 때문에 위 내용에 따르면 리턴 값은 3이 되어야 한다

Registers (FPU)
EAX 00000003

[그림 4] 리턴값 레지스터 EAX

위 그림은 GetDriveType 함수를 CALL하고 난 뒤의 EAX가 변경된 값이다

0040101D	. 46	INC ESI
0040101E	. 48	DEC EAX
0040101F	~ EB 00	JMP SHORT Reverse_.00401021
00401021	> 46	INC ESI
00401022	. 46	INC ESI
00401023	. 48	DEC EAX
00401024	. 3BC6	CMP EAX,ESI

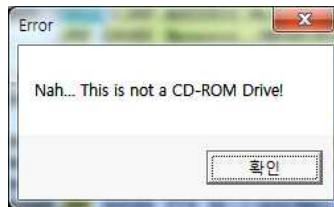
[그림 5] 리턴 값과 비교 값 연산

이후의 코드 내용은 ESI값을 3번 1씩 증가(INC ESI)시키고, EAX값을 2번 1씩 감소(DEC EAX)시킨다.

HDD를 CD-ROM으로 인식한다면 GetDriveType 함수의 리턴 값은 5가 될 것이고, 이것을 위 코드 내용에 대입하면 $EAX = 5 - 2 = 3$, $ESI = 0 + 3 = 3$ 이 된다.

EAX와 ESI를 비교하여 값이 같다면 0040103D로 점프 그렇지 않으면 Error 호출한다

00401024	. 3BC6	CMP EAX,ESI	
00401026	~ 74 15	JE SHORT Reverse_.0040103D	
00401028	. 6A 00	PUSH 0	
0040102A	. 68 35204000	PUSH Reverse_.00402035	
0040102C	. 68 3B204000	PUSH Reverse_.0040203B	
0040102E	. 6A 00	PUSH 0	
00401030	. E8 26000000	CALL <JMP.&USER32.MessageBoxA>	Style = MB_OK!MB_APPLMODAL Title = "Error" Text = "Nah... This is not a CD-ROM Drive!" hOwner = NULL MessageBoxA



[그림 6] Error

지금은 HDD로 인식하기 때문에 에러 메시지가 호출된다.

CD-ROM으로 인식 시키기 위해 RootPathName을 내 PC의 CD-ROM인 "d:\"로 변경해 보겠다.

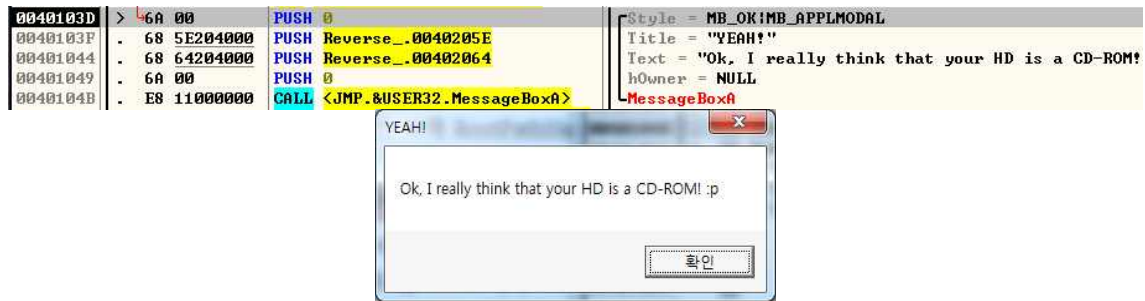
Address	Hex dump	ASCII
00402074	64 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00	d:\w.....

Dump창에서 직접 "c:\"에서 "d:\"로 변경해 보았다

변경하자 리턴값이 다음과 같이 5로 변경되었다.

Registers (FPU)	
EAX	00000005

리턴값이 5가 되자 정상 메시지가 호출되었다.



따라서, HDD를 CD-ROM으로 인식되게 하려면 리턴 값이 5가 되어야 함을 알 수 있다.