Challenges : Basic 07

Author : abex

Korean :
컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 "어떤것"으로 변경되는가

English :
Assuming the drive name of C is CodeEngn, what does CodeEngn transform into in the process of the serial construction

Download

<문제>

```
0040106C  >  6A 25        PUSH 25                          Count = 25 (37.)
0040106E  .  68 24234000  PUSH 07.00402324                 Buffer = 07.00402324
00401073  .  6A 68        PUSH 68                          ControlID = 68 (104.)
00401075  .  FF75 08      PUSH [ARG.1]                     hWnd = 003D8000
00401078  .  E8 F4000000  CALL <JMP.&USER32.GetDlgItemTextA>  GetDlgItemTextA
0040107D  .  6A 00        PUSH 0                           pFileSystemNameSize = NULL
0040107F  .  6A 00        PUSH 0                           pFileSystemNameBuffer = NULL
00401081  .  68 C8204000  PUSH 07.004020C8                 pFileSystemFlags = 07.004020C8
00401086  .  68 90214000  PUSH 07.00402190                 pMaxFilenameLength = 07.00402190
0040108B  .  68 94214000  PUSH 07.00402194                 pVolumeSerialNumber = 07.00402194
00401090  .  6A 32        PUSH 32                          MaxVolumeNameSize = 32 (50.)
00401092  .  68 5C224000  PUSH 07.0040225C                 VolumeNameBuffer = 07.0040225C
00401097  .  6A 00        PUSH 0                           RootPathName = NULL
00401099  .  E8 B5000000  CALL <JMP.&KERNEL32.GetVolumeInformatio  GetVolumeInformationA
0040109E  .  68 F3234000  PUSH 07.004023F3                 StringToAdd = "4562-ABEX"
004010A3  .  68 5C224000  PUSH 07.0040225C                 ConcatString = ""
004010A8  .  E8 94000000  CALL <JMP.&KERNEL32.lstrcatA>    lstrcatA
```

문제를 OllyDbg로 연 후 밑으로 조금 내리다보면 위 사진과 같은 어셈블리를 볼 수 있다.
여기서 GetDlgItemTextA 함수는 이름에서 느껴지듯이 텍스트에서 문자를 읽는다.

GetDlgItemText QuickInfo Overview Group

The **GetDlgItemText** function retrieves the title or text associated with a control in a dialog box.

함수가 어떤 행동을 하는지 모를 때 MSDN과 같은 사이트에서 함수에 대해 알아볼 수 있지만 가끔 귀찮을 때가 있다. 그럴때 위에 첨부된 Win32.hlp 파일을 올리디버거 폴더에 넣고 Help메뉴 -> Select API help file을 누른 후 Win32.hlp 를 선택하고 프로그램을 재시작한다.
그리고 내가 궁금한 함수를 클릭한 후 오른쪽 버튼을 누르고 Help on symbolic name을 눌러보면 해당 함수에 대해 자세히 알 수 있다.

GetVolumeInformationA는 파일시스템의 정보를 얻는데 사용되는 함수인데 이 함수에는 위에서 볼 수 있는것처럼 8개의 파라미터가 있다. Help on symbolic name을 눌러보면

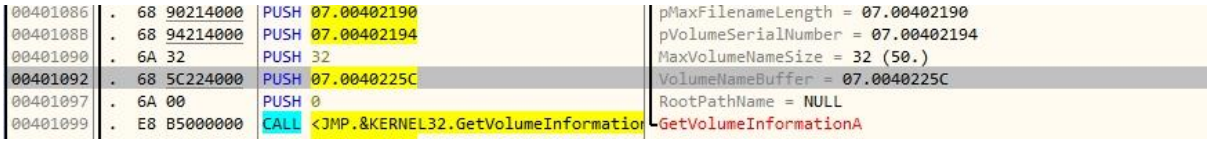
Parameters

lpRootPathName
Points to a string that contains the root directory of the volume to be described. If this parameter is NULL, the root of the current directory is used.

lpVolumeNameBuffer
Points to a buffer that receives the name of the specified volume.

이런 내용을 볼 수 있는데 읽어보면 RootPathName은 NULL값을 받을 때 지금 폴더의 루트디렉토리, 즉 C드라이브를 가리키게 된다. 그리고 VolumeNameBuffer이 가리키는 주소로 C드라이브의 이름을 가져온다.

생각해보면 VolumeNameBuffer에서 가져온 값을 CodeEngn으로 바꿔주게 된다면 인증에 성공할 것이다.



RootPathName에 NULL이 들어가있고, VolumeNameBuffer에는 0040225C라는 주소값이 들어가있다. 이 말은 0040225C에 C드라이브의 이름이 들어간다는 뜻이다. 함수를 실행하고 저 위치로 가서 값을 CodeEngn으로 바꿔주게 된다면 시리얼 값을 얻을 수 있다.

밑으로는 이제 문자열을 뒤에 이어붙이고 CodeEngn이라는 문자열을 다른 문자열로 바꾸는 루틴이 있고 내가 입력한 값과 같는지 확인한다.
이건 뭐 F8만 눌러봐도 알 수 있기에 여기서 다루지는 않겠다.