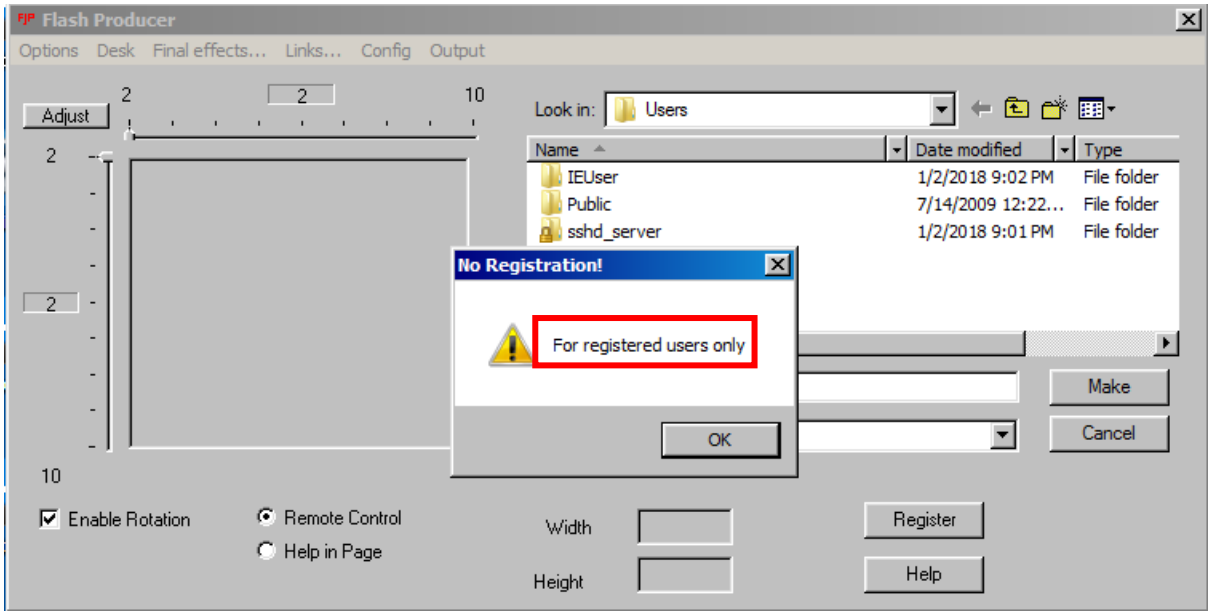
악성코드 분석 보고서

(sand-reversingwithlena-tutorials)

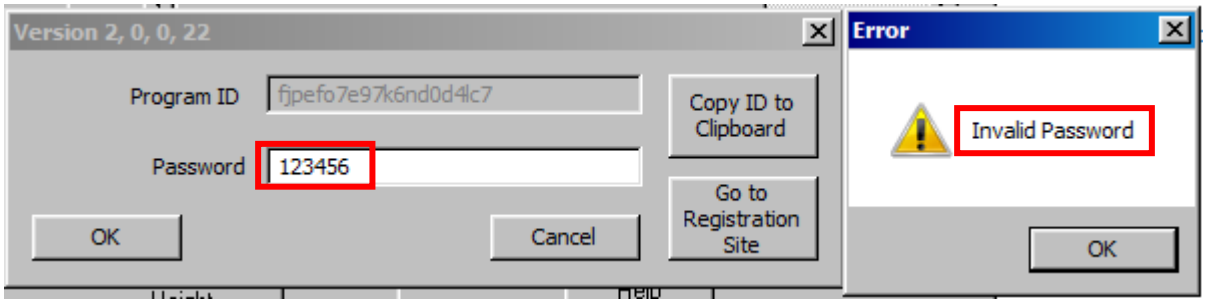
2025.07.01

11

1. 문제



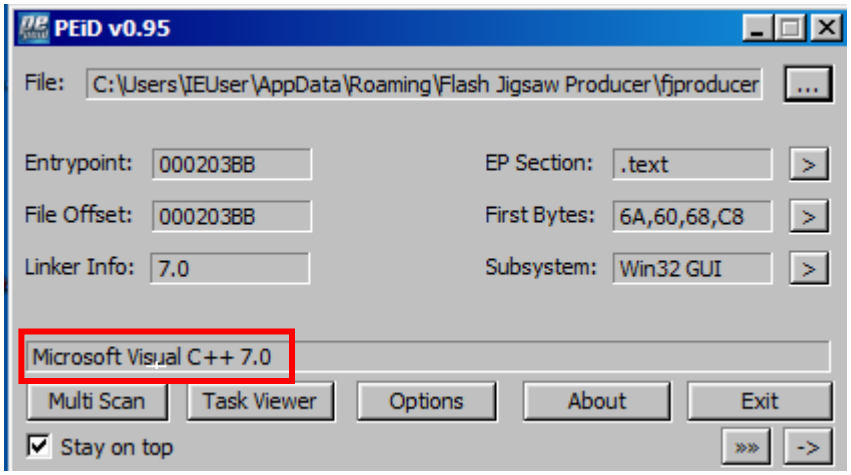
Desk > Select... 들어가면 경고 창이 뜸



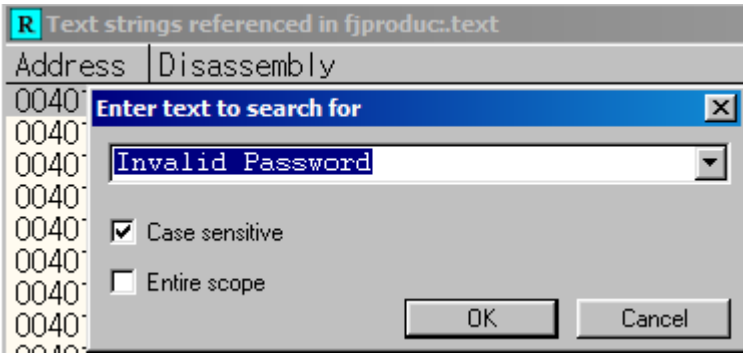
Register 들어가서 비밀번호 입력하고 'OK'버튼 누르면 패스워드가 유효하지 않다고 나옴

레지스터 키 등록해서 전부 사용할 수 있게 해야함.

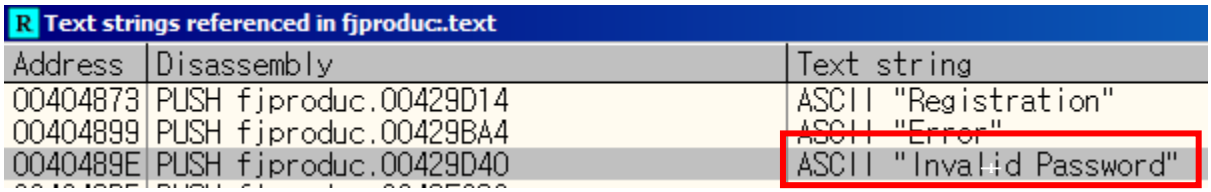
2. 해결 방법



PEID로 확인 시 C++로 만든 파일이라는 것을 알 수 있다.



Search for > All referenced text strings 눌러서 Invalid Password 해당 구문을 찾아준다.

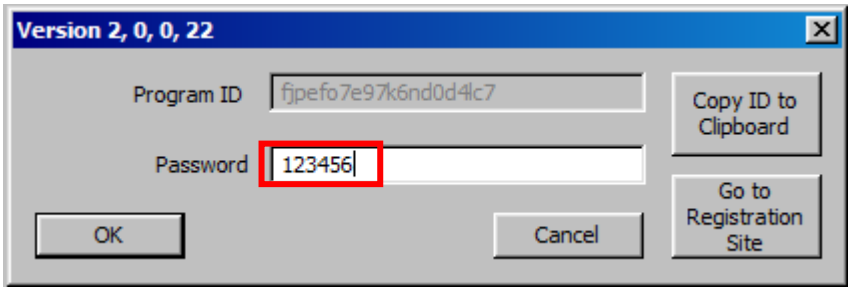


나오는 걸 볼 수 있고 들어가서 브레이크를 걸고 주변 분기문을 찾아본다.

```
0040484F  .v 74 37        JE SHORT fjproduc.00404888
00404856  .  E8 E5FDFFFF  CALL fjproduc.00404640
0040485E  .  84C0         TEST AL,AL
00404860  .v 74 35        JE SHORT fjproduc.00404897
00404862  .  8B0D ACE3420( MOV ECX,DWORD PTR DS:[42E3AC]      fjproduc.00429EBC
00404868  .  68 60034300  PUSH fjproduc.00430360              FileName = ""
0040486D  .  68 34034300  PUSH fjproduc.00430334              String = ""
00404872  .  51           PUSH ECX                            Key => "Password"
00404873  .  68 149D4200  PUSH fjproduc.00429D14              Section = "Registration"
00404878  .  FF15 2890420( CALL DWORD PTR DS:[<&KERNEL32.WritePriv  WritePrivateProfileStringA
0040487E  .  6A 01        PUSH 1
00404880  .  E8 5BFEFFFF  CALL fjproduc.004046E0
00404885  .  83C4 04      ADD ESP,4
00404888  >  6A 01        PUSH 1                              Result = 1
0040488A  .  56           PUSH ESI                            hWnd
0040488B  .  FF15 2C92420( CALL DWORD PTR DS:[<&USER32.EndDialog>]  EndDialog
00404891  .  33C0         XOR EAX,EAX
00404893  .  5E           POP ESI
00404894  .  C2 1000      RETN 10
00404897  >  6A 30        PUSH 30                             Style = MB_OK|MB_ICONEXCLAMATI
0040489E  .  68 409D4200  PUSH fjproduc.00429D40              Text = "Invalid Password"
004048A4  .  FF15 4892420( CALL DWORD PTR DS:[<&USER32.MessageBoxA  MessageBoxA
```

0x00404860에 JE분기문을 찾을 수 있고 'TEST AL, AL'을 비교하는 걸 볼 수 있다.

AL은 0x00404856 함수에서 정의되니까 브레이크를 걸어주고 다시 실행해본다.

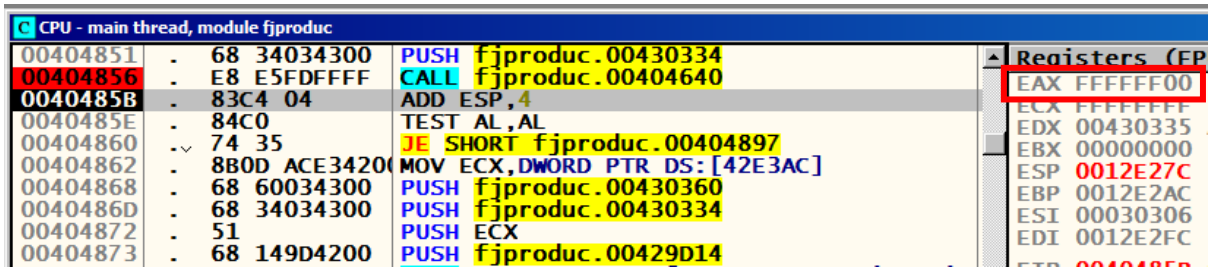


입력하면 브레이크 건 0x00404856에 멈추는 걸 볼 수 있고 'F7'을 눌러 함수 안으로 들어가서 분석해본다.

```
00404640  $  83EC 2C      SUB ESP,2C
00404643  .  56           PUSH ESI
00404644  .  8B7424 34    MOV ESI,DWORD PTR SS:[ESP+34]
00404648  .  8BC6         MOV EAX,ESI
0040464A  .  8D50 01      LEA EDX,DWORD PTR DS:[EAX+1]
0040464D  .  8D49 00      LEA ECX,DWORD PTR DS:[ECX]
00404650  >  8A08         MOV CL,BYTE PTR DS:[EAX]            pw compare
00404652  .  40           INC EAX
00404653  .  84C9         TEST CL,CL
00404655  .^ 75 F9        JNZ SHORT fjproduc.00404650
00404657  .  2BC2         SUB EAX,EDX
00404659  .  83F8 04      CMP EAX,4
0040465C  .v 73 07        JNB SHORT fjproduc.00404665
0040465E  >  32C0         XOR AL,AL
00404660  .  5E           POP ESI
00404661  .  83C4 2C      ADD ESP,2C
00404664  .  C3           RETN
```

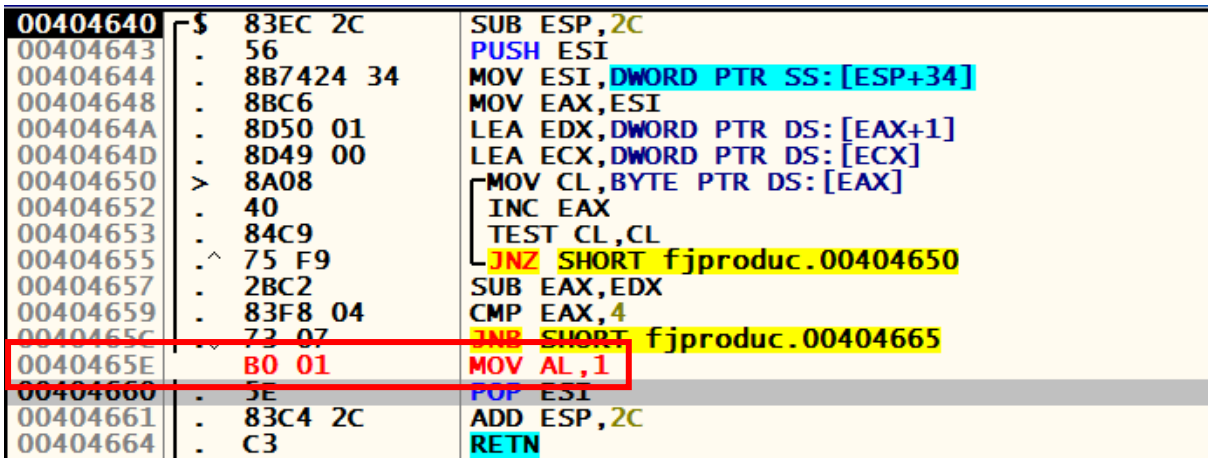
패스워드를 비교하는 코드를 볼 수 있다.

실행하다보면 0x00404664에서 빠져나오고 AL이 XOR에 의해서 초기화된다,

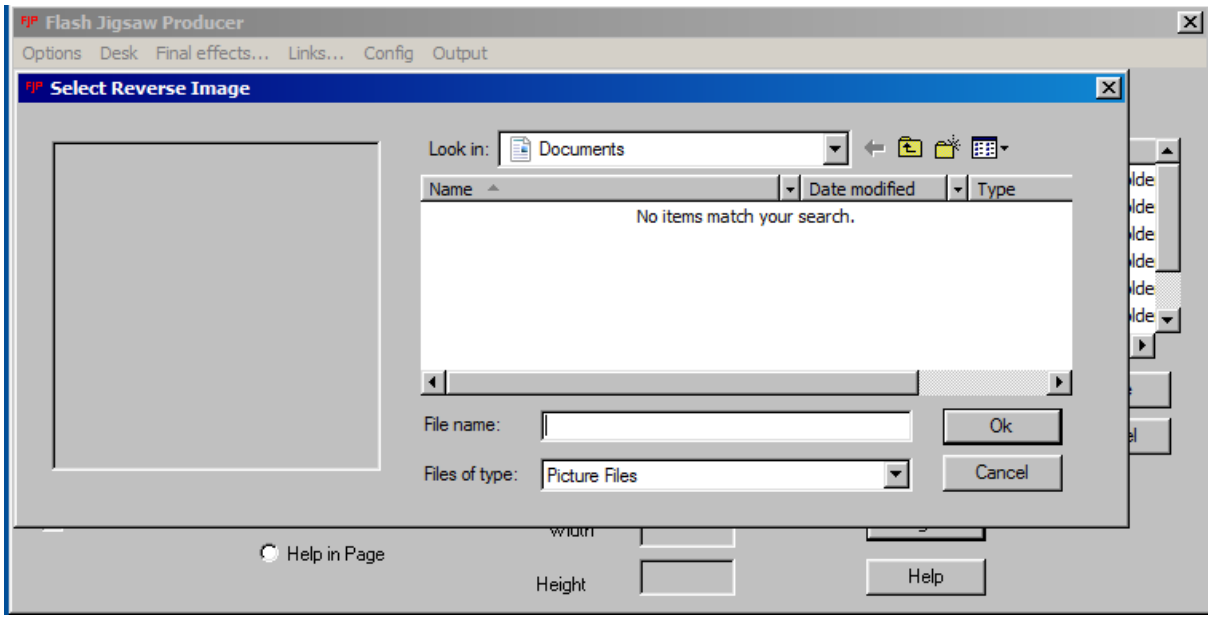


그럼 JE가 실행되면서 패스워드가 유효하지 않다는 창이 나오게된다.

그럼 JE가 점프 안하게 하려면 AL != 0이 되게 해야한다.



그럼 전에 있던 함수로 되돌아가서 0x0040465E를 'MOV AL, 1'로 바꿔주고 저장한다.



그럼 키를 등록하지 않아도 Desk > Select Reverse Image에 들어갈 수 있게 된다.

문제 해결!