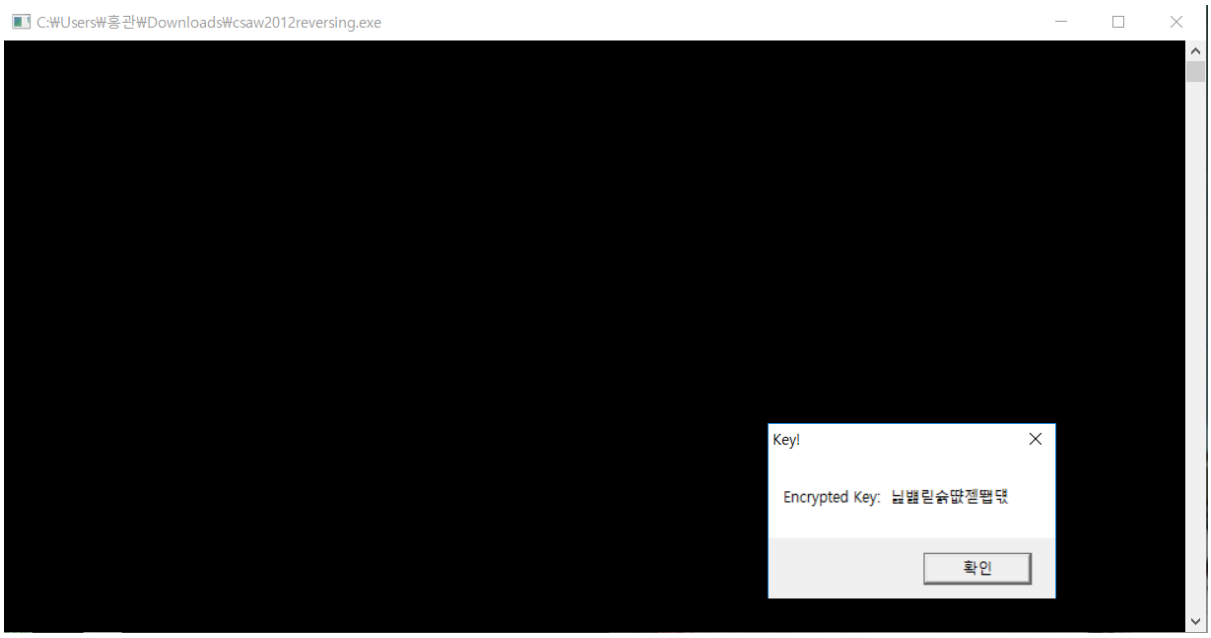
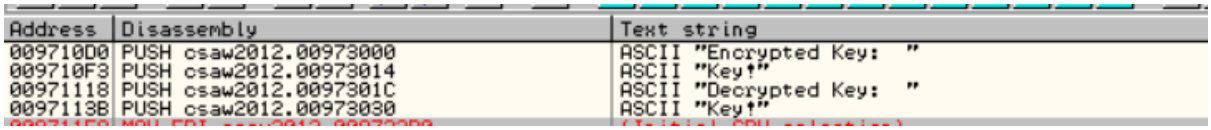
CSAW 2012 Reversing 100

윤홍관



실행하면 Encrypted Key라고 이상한 문자열이 뜬다.

decrypted key를 찾으면 될 것 같은 문제다! 올리 디버거로 열어보자



string을 검색해보니 Encrypted와 Decrypted를 출력해주는 부분이 있다.

Encrypted 부분을 우리는 보았으니 그 부분으로 이동해 보자

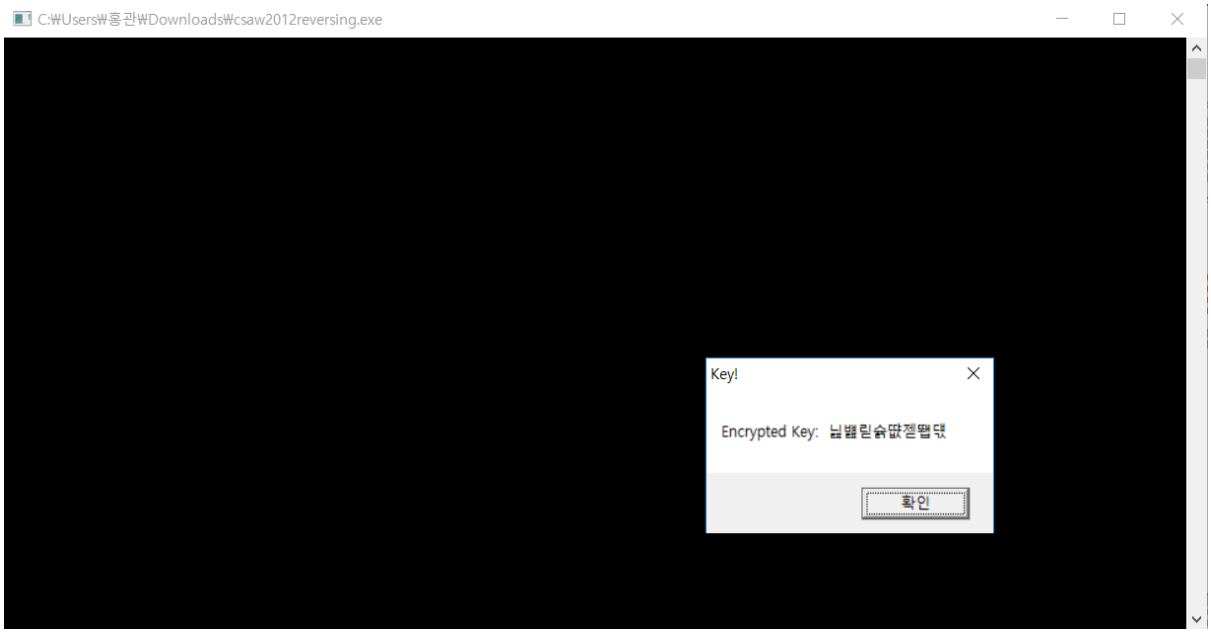
```
8945 FC        MOV [LOCAL.1],EAX
C645 E8 88     MOV BYTE PTR [EBP-18],88
C645 E9 9A     MOV BYTE PTR [EBP-17],9A
C645 EA 93     MOV BYTE PTR [EBP-16],93
C645 EB 9C     MOV BYTE PTR [EBP-15],9C
C645 EC 90     MOV BYTE PTR [EBP-14],90
C645 ED 92     MOV BYTE PTR [EBP-13],92
C645 EE 9A     MOV BYTE PTR [EBP-12],9A
C645 EF A0     MOV BYTE PTR [EBP-11],0A0
C645 F0 8B     MOV BYTE PTR [EBP-10],8B
C645 F1 90     MOV BYTE PTR [EBP-F],90
C645 F2 A0     MOV BYTE PTR [EBP-E],0A0
C645 F3 9C     MOV BYTE PTR [EBP-D],9C
C645 F4 8C     MOV BYTE PTR [EBP-C],8C
C645 F5 9E     MOV BYTE PTR [EBP-B],9E
C645 F6 88     MOV BYTE PTR [EBP-A],88
C645 F7 DE     MOV BYTE PTR [EBP-9],0DE
C645 F8 00     MOV BYTE PTR [EBP-8],0
8D45 E8        LEA EAX,[LOCAL.6]
50             PUSH EAX                          Arg1
E8 33FFFFFF    CALL csaw2012.00971000            csaw2012.00971000
83C4 04        ADD ESP,4
68 00309700    PUSH csaw2012.00973000            src = "Encrypted Key:  "
8D4D A8        LEA ECX,[LOCAL.22]
51             PUSH ECX                          dest
E8 8A000000    CALL <JMP.&MSVCR100.strcpy>       strcpy
83C4 08        ADD ESP,8
8D55 E8        LEA EDX,[LOCAL.6]
52             PUSH EDX                          src
8D45 A8        LEA EAX,[LOCAL.22]
50             PUSH EAX                          dest
E8 74000000    CALL <JMP.&MSVCR100.strcat>       strcat
83C4 08        ADD ESP,8
6A 00          PUSH 0                            Style = MB_OK|MB_APPLMODAL
68 14309700    PUSH csaw2012.00973014            Title = "Key!"
8D4D A8        LEA ECX,[LOCAL.22]
51             PUSH ECX                          Text
6A 00          PUSH 0                            hOwner = NULL
FF15 AC209700  CALL [<&USER32.MessageBoxA>]      MessageBoxA
6A FF          PUSH -1                           status = FFFFFFFF (-1.)
FF15 A0209700  CALL [<&MSVCR100.exit>]           MSVCR100.exit
8D55 E8        LEA EDX,[LOCAL.6]
52             PUSH EDX                          Arg1
E8 1BFFFFFF    CALL csaw2012.00971030            csaw2012.00971030
83C4 04        ADD ESP,4
68 1C309700    PUSH csaw2012.0097301C            src = "Decrypted Key:  "
8D45 A8        LEA EAX,[LOCAL.22]
50             PUSH EAX                          dest
E8 42000000    CALL <JMP.&MSVCR100.strcpy>       strcpy
83C4 08        ADD ESP,8
```

무엇인가 많이 넣어놓고 00971000을 call하는데 저 부분을 들어가보니 암호화 해주는 부분인 것 같았다. 딱히 비교해서 들어가는 것도 없어서 멍하니 보고있다가 버튼을 누르면 꺼져서 뒤에 부분이 실행되지 않는 다는 생각이 들었다.

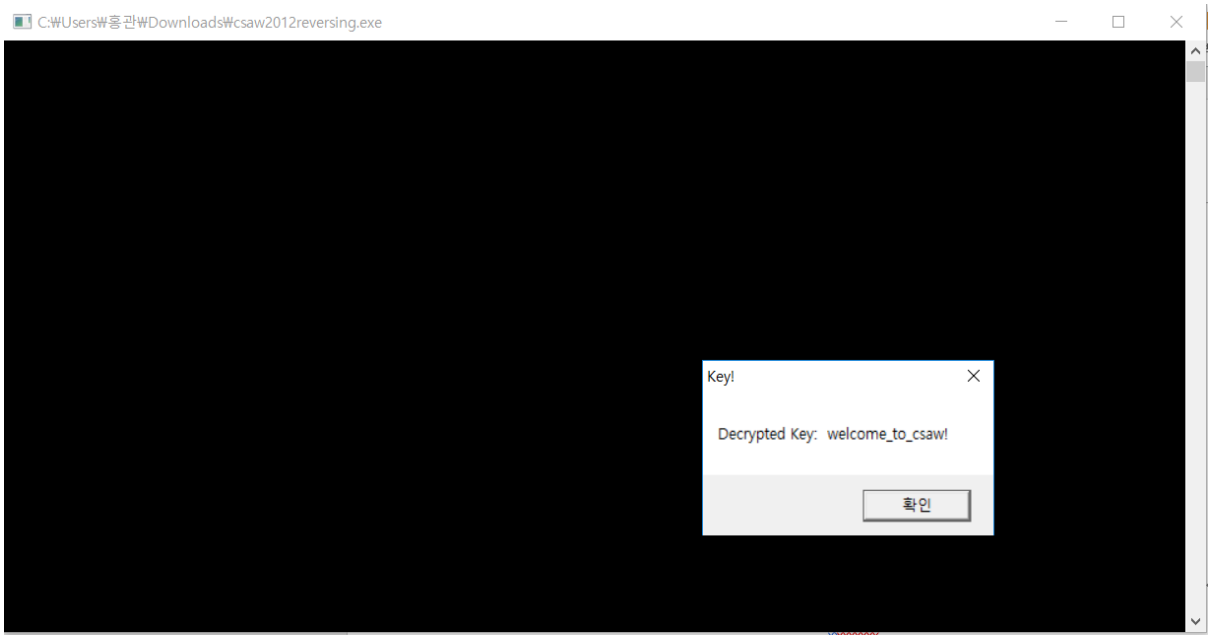
MSVCR100.exit 부분이 아마 확인을 누르면 꺼지는 부분일 것이므로 exit 부분을 그냥 바로 다음 주소로 패치해주면 되겠다고 생각했다!

```
009710EE  . 83C4 08      ADD ESP,8
009710F1  . 6A 00        PUSH 0                            Style = MB_OK|MB_APPLMODAL
009710F3  . 68 14309700  PUSH csaw2012.00973014            Title = "Key!"
009710F8  . 8D4D A8      LEA ECX,[LOCAL.22]
009710FB  . 51           PUSH ECX                          Text
009710FC  . 6A 00        PUSH 0                            hOwner = NULL
009710FE  . FF15 AC209700 CALL [<&USER32.MessageBoxA>]     MessageBoxA
00971104  . 6A FF        PUSH -1                           status = FFFFFFFF (-1.)
00971106    EB 04        JMP SHORT csaw2012.0097110C
00971108    90           NOP
00971109    90           NOP
0097110A    90           NOP
0097110B    90           NOP
0097110C  . 8D55 E8      LEA EDX,[LOCAL.6]
0097110F  . 52           PUSH EDX                          Arg1
00971110  . E8 1BFFFFFF  CALL csaw2012.00971030            csaw2012.00971030
00971115  . 83C4 04      ADD ESP,4
00971118  . 68 1C309700  PUSH csaw2012.0097301C            src = "Decrypted Key:  "
```

패치해준 후 실행을 해보면



처음엔 Encrypted Key가 뜨나 당황하지 않고 확인을 누르면



정상적으로 우리가 원하는 창을 띄워준다.

Key : welcome_to_csaw!