CodeEngn
ReverseEngineering Conference

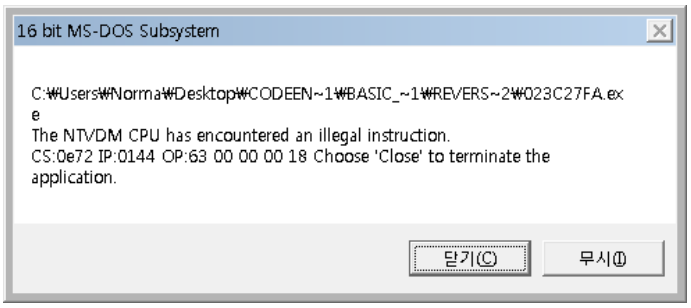
FIRST CREATION	2012-08-28
LAST MODIFICATION	2012-08-28
NAME	CENTY

Type & Problem

✓ BASIC RCE
✓ Reverse L02
✓ 패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

Solution L01

0. 프로그램을 실행하면 아래와 같은 에러가 발생



첫 번째 원인으로는 16비트 실행 파일을 16비트 실행 파일을 지원하지 않는 환경에서 실행하였을 경우 발생 될 수 있고, 다른 이유로는 실행 파일의 변조되어 에러가 발생할 수 있다. 본 문제에서는 실행파일이 손상되어 실행이 안되었다고 언급했기 때문에 두 번째 경우이다.

1. 먼저 실행 파일의 구조를 보기 위해 Hex 프로그램으로 파일을 연다 [01].

023C27FA.exe

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010   B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030   00 0A 00 00 00 00 00 00 00 10 00 00 00 10 00 00  ................
00000040   00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00  . ....@.........
00000050   04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00  ................
00000060   00 50 00 00 00 04 00 00 00 00 00 00 02 00 00 00  .P..............
00000070   00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
00000080   00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000090   2C 20 00 00 3C 00 00 00 00 40 00 00 18 03 00 00  , ..<....@......
000000A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0   00 00 00 00 00 00 00 00 00 20 00 00 2C 00 00 00  ......... ..,...
000000F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

기본적으로 32bit 실행 파일 (Portable Executable)은 간략히 다음과 같이 구성되어 있다 [02].

- IMAGE_DOS_HEADER
- DOS Stub Code
- PE HEADER

하지만 본 파일에서는 IMAGE_DOS_HEADER의 시작부분인 MZ (DOS 개발자 가운데 한명인 Mark Zbikowski

의 이니셜로 DOS Header의 시그니쳐로 사용되고 있음 [02])만 볼 수 있고 다른 부분은 알기가 힘든 것으로 보아 파일이 잘못되었다고 생각할 수 있다.

2. HEX 코드는 보기 힘들지만 오른쪽에 ASCII로 나타난 부분은 읽을 수 있기 때문에 코드를 내려 힌트가 될만한 문자열을 검색

```
00000710  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000720  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000730  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000740  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000750  41 44 44 69 61 6C 6F 67 00 41 72 74 75 72 44 65  ADDialog.ArturDe
00000760  6E 74 73 20 43 72 61 63 6B 4D 65 23 31 00 00 00  nts CrackMe#1...
00000770  00 00 00 00 00 4E 6F 70 65 2C 20 74 72 79 20 61  .....Nope, try a
00000780  67 61 69 6E 21 00 59 65 61 68 2C 20 79 6F 75 20  gain!.Yeah, you
00000790  64 69 64 20 69 74 21 00 43 72 61 63 6B 6D 65 20  did it!.Crackme
000007A0  23 31 00 4A 4B 33 46 4A 5A 68 00 00 00 00 00 00  #1.JK3FJZh......
000007B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000007C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000007D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000007E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000007F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

이곳에서 다음과 같은 문자열을 볼 수 있다.

- CrackMe#1
- Nope, try again!
- Yeah, you did it!
- CrackMe#1
- JK3FJZh

이 중 마지막 문자열이 (7Byte)가 패스워드이다.

References

[01] HxD, Freeware Hex Editor and Disk Editor, http://mh-nexus.de/en/hxd/
[02] codeengn.com, PE 구조 분석,
http://codeengn.com/archive/Reverse%20Engineering/File%20Structure/PE%20%EA%B5%AC%EC%A1%B0%20%EB%B6%84%EC%84%9D%20%5Bcari2052%5D.pdf