Reverse L02

2012년 7월 17일 화요일
오후 12:02

Reverse L02 Start

Author : ArturDents

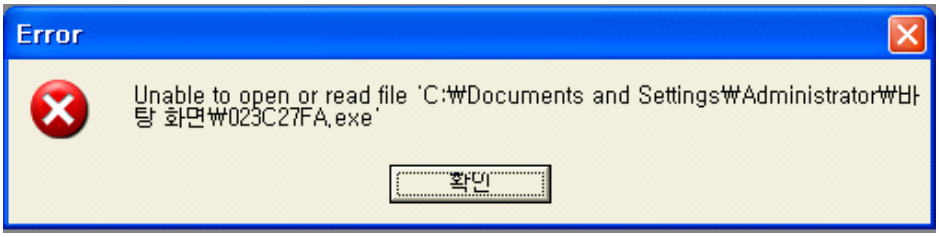
Korea :

패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

English :

The program that verifies the password got messed up and ceases to execute. Find out what the password is.

Down

- http://codeengn.com/continue
  - L01 의 답인 5 입력 시 문제 확인 가능
- 파일의 정보를 확인하기 위해서 OllyDBG로 파일을 열었으나 아래와 같은 메시지 출력된다.
  - 

- PE구조를 확인하기 위해서 Hex 편집기로 열어보니 시작 오프셋이 비정상적인 것을 확인할 수 있다.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00
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

- 다른 정보를 얻을 수 없을까라는 생각에 하단으로 내려보니 사용되는 API가 확인된다.

000005E0	00	00	00	00	92	00	44	69	61	6C	6F	67	42	6F	78	50	' DialogBoxP
000005F0	61	72	61	6D	41	00	B8	00	45	6E	64	44	69	61	6C	6F	aramA ¸ EndDialo
00000600	67	00	00	01	47	65	74	44	6C	67	49	74	65	6D	00	00	g GetDlgItem
00000610	02	01	47	65	74	44	6C	67	49	74	65	6D	54	65	78	74	GetDlgItemText
00000620	41	00	BB	01	4D	65	73	73	61	67	65	42	6F	78	41	00	A » MessageBoxA
00000630	10	02	53	65	6E	64	4D	65	73	73	61	67	65	41	00	00	SendMessageA
00000640	2B	02	53	65	74	46	6F	63	75	73	00	00	55	53	45	52	+ SetFocus USER
00000650	33	32	2E	64	6C	6C	00	00	75	00	45	78	69	74	50	72	32.dll u ExitPr
00000660	6F	63	65	73	73	00	11	01	47	65	74	4D	6F	64	75	6C	ocess GetModul
00000670	65	48	61	6E	64	6C	65	41	00	00	4B	45	52	4E	45	4C	eHandleA KERNEL
00000680	33	32	2E	64	6C	6C	00	00	00	00	00	00	00	00	00	00	32.dll

- 조금 더 하단으로 내려보니 사용되는 String이 확인되며 패스워드로 의심되는 문자열이 보여진다.

```
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
```

- 답은 JK3FJZh로 의심된다.