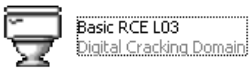
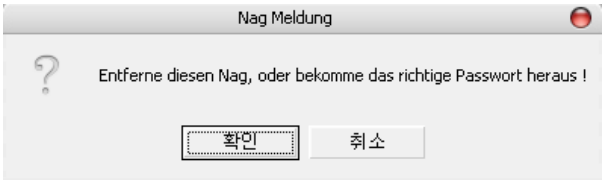
Reverse L03

2009년 12월 22일 화요일
오후 4:26

파일 확인



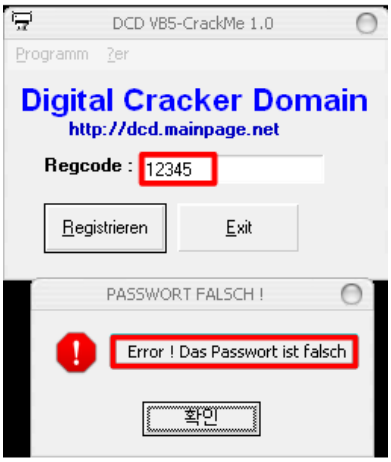
프로그램 실행



독일에서 만든 Crack me 라고 생각된다.

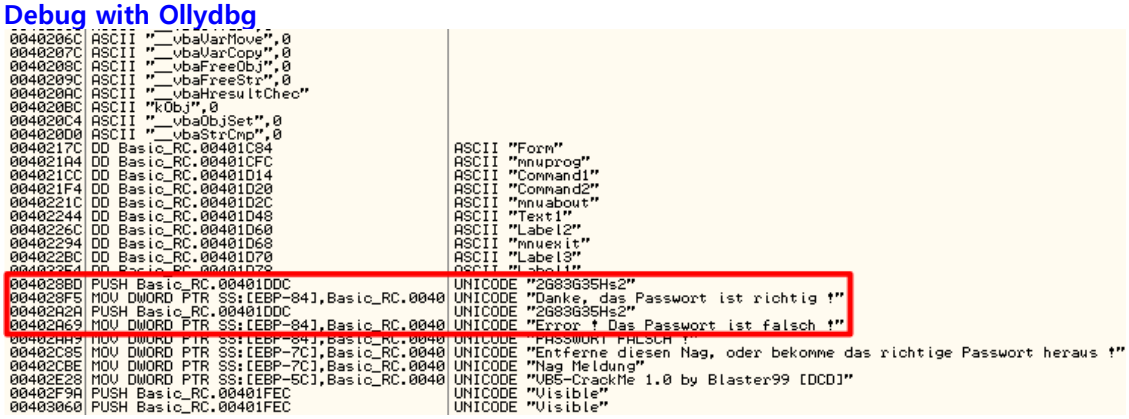
- 실제 구글 번역기를 돌려본 결과, **이 성가신 잔소리 하거나, 올바른 암호를 꺼내 제거!** 라고 번역 되었다.

확인 클릭



확인을 누르면 regcode 를 입력하라는 입력창이 뜨게 되고, 아무 값 (12345) 를 대입하니, **Error Messagebox 가 호출**되었다.

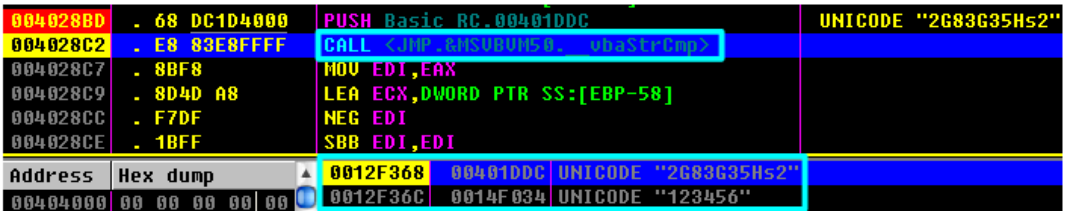
Debug with Ollydbg



마우스 우클릭 -> Search for -> All referenced text strings 를 통해 출력된 string 을 확인 할 수 있었다.

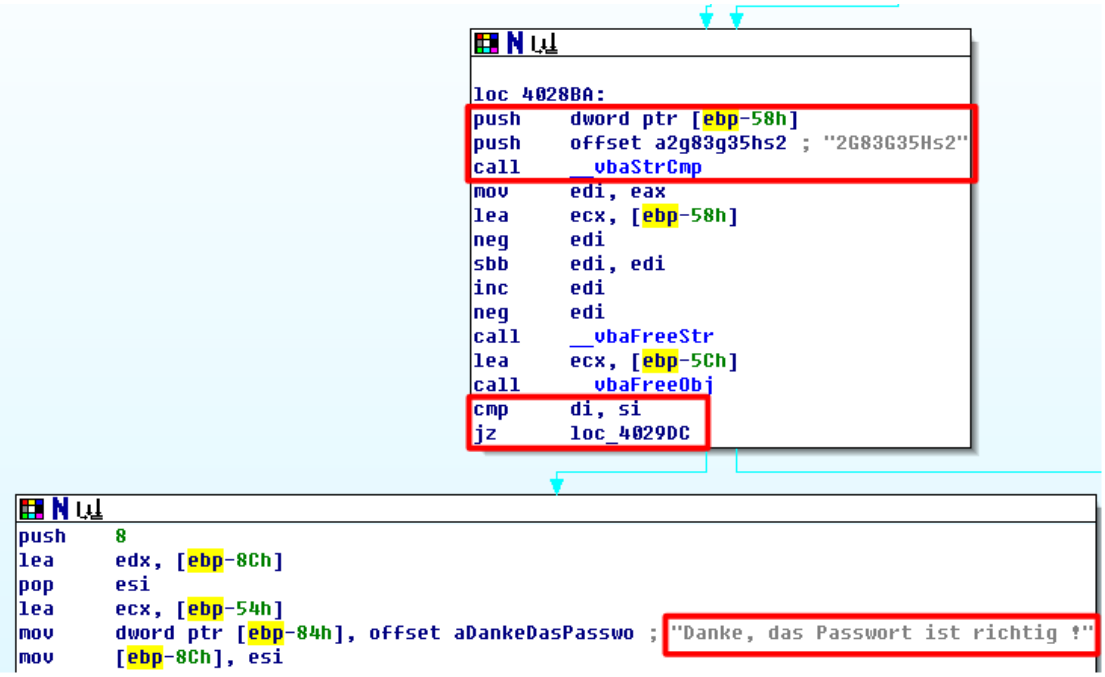
- 2G83G35Hs2 가 richtig 와 falsch 가 포함된 문장 사이에 있는 것으로 보아 **KEY 라고 추측**

004028BD 에 **Breakpoint 를 설정한 후, 실행**을 시켜 보았다.



바로 아래에 **vbaStrCmp** 라는 함수가 보이고 **Stack 영역에 입력한 값과, KEY 값**이 들어가 있는 것을 확인 하였다.

With IDA Pro



입력한 값 **ebp-58h 와 KEY 값을 push** 한 후 , **vbaStrCmp** 함수를 실행 후, **cmp (di - si) 작업을 통해 참 거짓 출력 문**으로 **jmp** 한다.

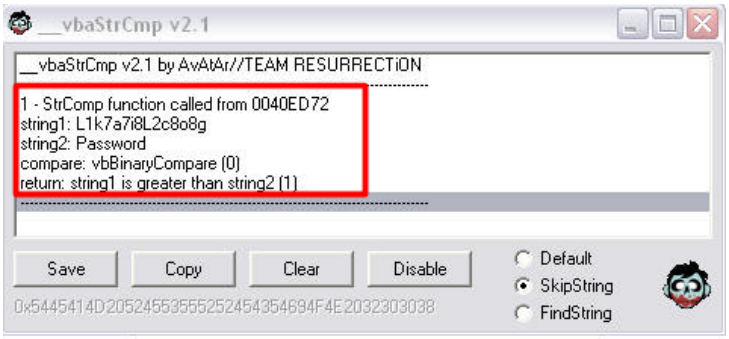
문제 해결

입력된 값 과 비교하게되는 값 (**2G83G35Hs2**) 이 같으면 **"Danke, das Passwort ist richting !" 출력구문으로 jmp** 되므로, 입력후 확인

보충 설명

실제로 **vbastrcmp 라는 crack tool** 도 있다.

- visual basic 폴더에, 해당 crack tool 의 파일을 넣으면 **vbastrcmp 함수가 실행될때 값을 획득해서 KEY 를 획득하는 Tool** 이다.


__vbaStrCmp v2.1
__vbaStrCmp v2.1 by AvAtAr//TEAM RESURRECTiON
1 - StrComp function called from 0040ED72
string1: L1k7a7i8L2c8o8g
string2: Password
compare: vbBinaryCompare (0)
return: string1 is greater than string2 (1)
Save
Copy
Clear
Disable
Default
SkipString
FindString
0x5445414D2052455355525245435469F4E2032303038


CrackMe V 7.0
By Dark-Graveyard
NickName
Password
Registra
www.inj3ct-it.org
www.ogmdevelopment.com

답

vbaStrCmp