

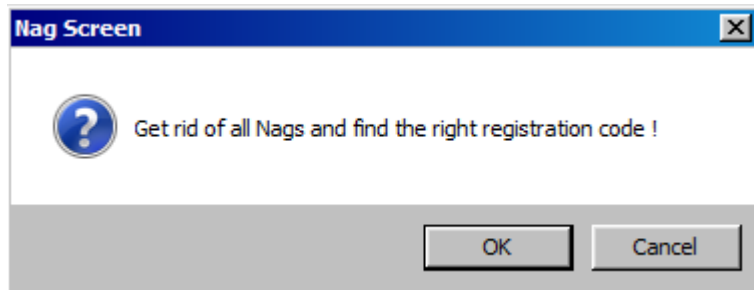
악성코드 분석 보고서

(sand-reversingwithlana-tutorials)

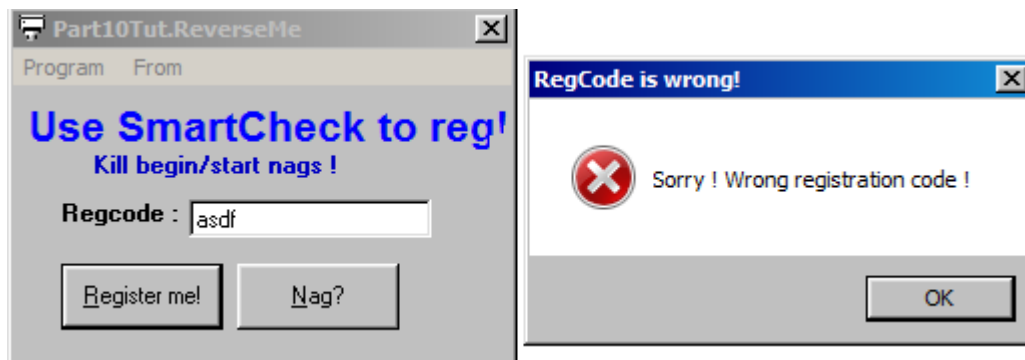
2025.07.01

1. 문제

1) Tut ReverseMe1

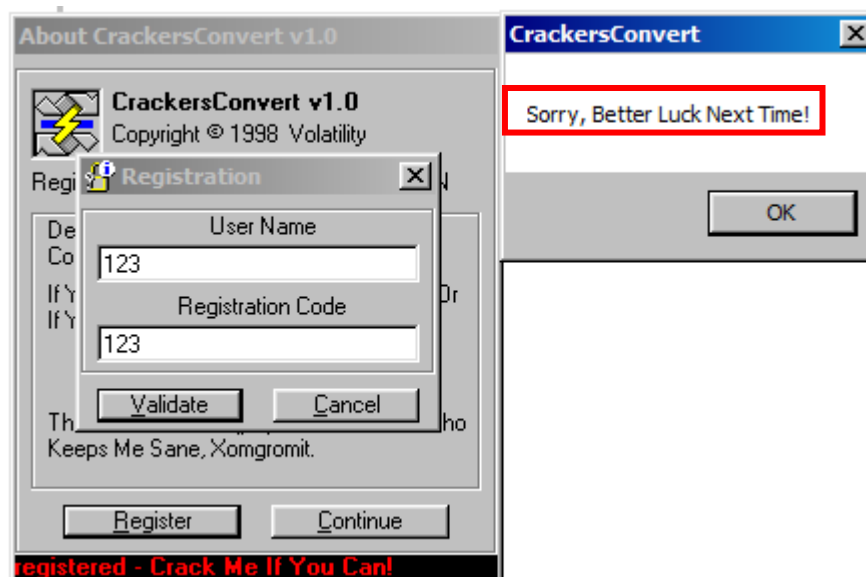


> Nag 다 제거하기



> 레지스터 키 등록하기

2) CConvert



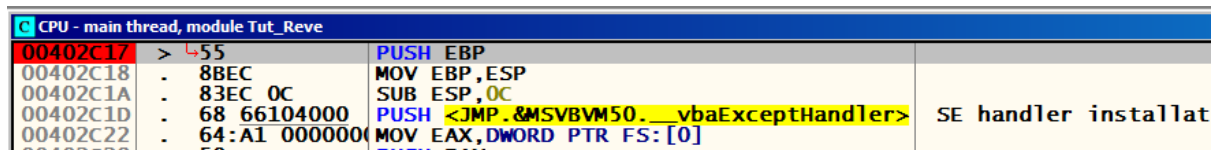
키 값을 찾아줘야한다.

3) ReverseMe2 해결 못함.

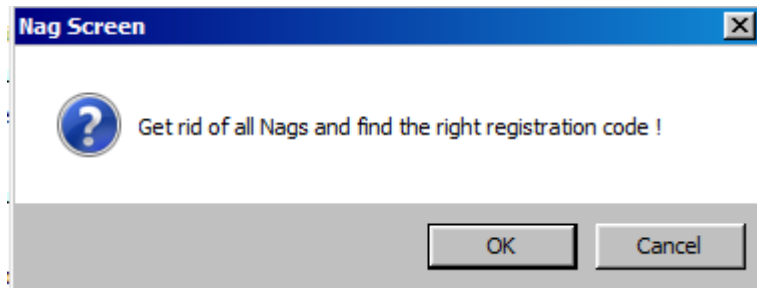
하나씩 보면서 내려가다보면 'l'mlena151' 키 같이 생긴 문자열을 볼 수 있다. 그리고 위 아래를 보면 성공했을 때 나오는 문자열과 실패했을 때 나오는 문자열을 볼 수 있다. 그래서 이 값이 키 값이라는 것을 유추할 수 있다.



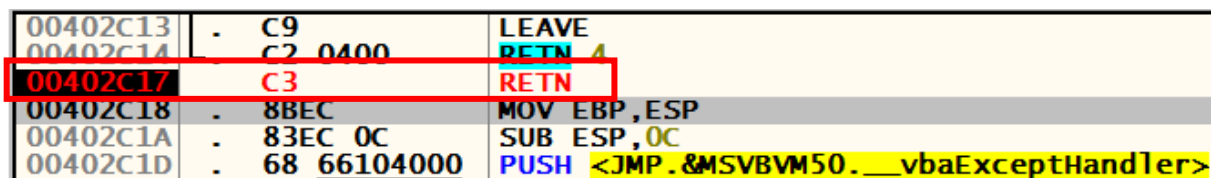
Nag를 끄기 위해서는 VB디컴파일러로 보면 commad2가 이름인 걸 볼 수 있고 시작하는 주소가 402C17인 걸 알 수 있다.



402C17에 브레이크를 걸어주고 다시 실행해본다.

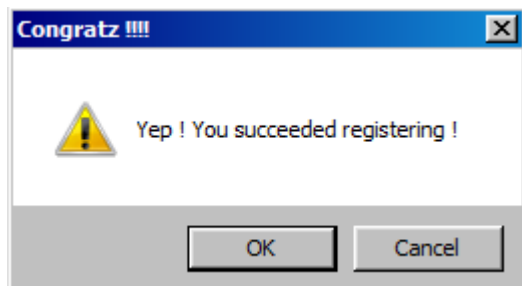


원래 처음에 Nag가 하나 나오는데 주소가 402C17이고 폼에 Nag를 눌렀을 때도 똑 같은 주소를 공유한다는 것을 알 수 있다.



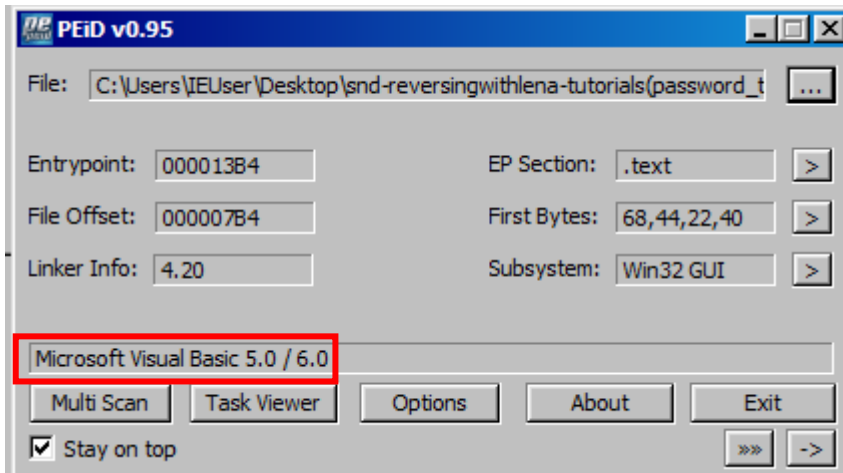
이 창이 안나오게 하기 위해서는 이 구간이 아예 끝나게 'RETN'으로 바꿔주면된다.

바꿔서 저장 후 실행하면 Nag창이 안나오는 걸 볼 수 있다.

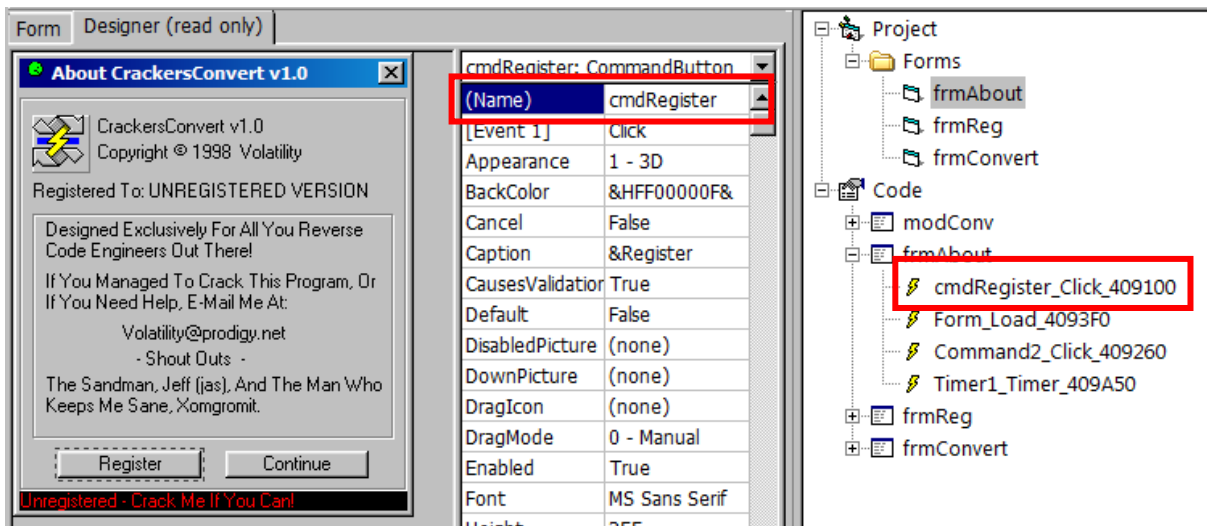


키 값인 'mlena151'을 넣어주면 성공했다는 창이 나오는 걸 볼 수 있다.

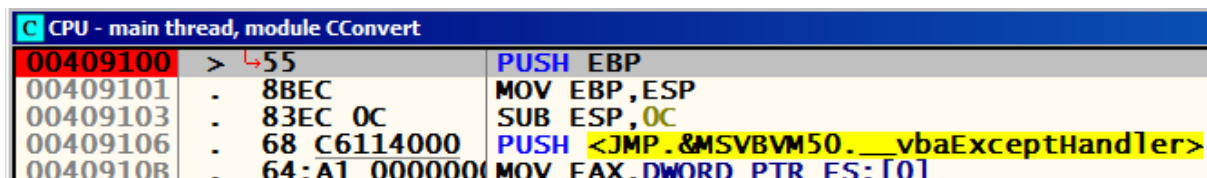
2) CConvert



PEID로 확인 시 비주얼 베이직으로 만든 파일이라는 것을 알 수 있다.

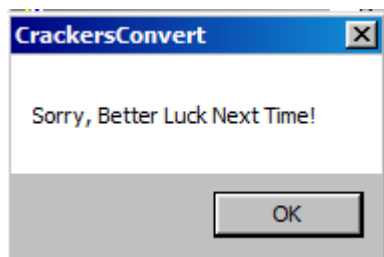


VB디컴파일러로 열어보면 'Register' cmdRegister라는 이름을 갖고 있다는 것을 알 수 있고 주소가 409100로 시작하는 것을 볼 수 있다.



409100에 브레이크를 걸어주고 다시 실행해본다.

'F9'으로 몇 번 눌러주다보면 이름이랑 키를 입력할 수 있는 창이 나온다.



이름이랑 키를 입력하고 눌러보면 이 창이 나오고 중간으로 돌아간다.

'Sorry, Better Luck Next Time!' 해당 문자열 참조위치를 찾아준다,

R Text strings referenced in CConvert.text		
Address	Disassembly	Text string
004042E0	UNICODE "am",0	
004042EC	UNICODE "Sorry, B"	
004042FC	UNICODE "etter Lu"	
0040430C	UNICODE "ck Next "	
0040431C	UNICODE "Time!",0	

차례로 참조하는 것을 볼 수 있고 들어가본다.

CPU - main thread, module CConvert		
004042EB	00	DB 00
004042EC	. 5300 6F00 7200	UNICODE "Sorry, B"
004042FC	. 6500 7400 7400	UNICODE "etter Lu"
0040430C	. 6300 6B00 2000	UNICODE "ck Next "
0040431C	. 5400 6900 6D00	UNICODE "Time!",0
00404328	. 5F 5F 76 62 00	ASCII "__vbaEnd",0

이렇게 나오고 이 구간을 참조하는 함수를 찾아준다.

R References in CConvert.text to 004042EC		
Address	Disassembly	Comment
004042EC	UNICODE "Sorry, B"	(Initial CPU selection)
0040A10A	MOV DWORD PTR SS:[EBP-A4],CConvert.004042EC	UNICODE "Sorry, Better Luck Next Time!"

Find references to > Selected address 들어가면 참조하는 함수를 찾았다.

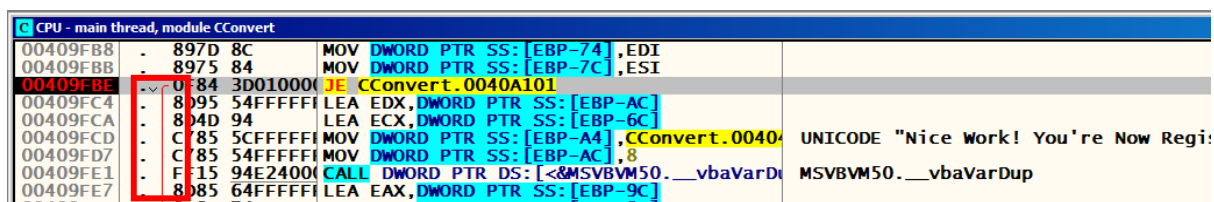
CPU - main thread, module CConvert		
0040A101	> 8D95 54FFFFFF LEA EDX,DWORD PTR SS:[EBP-AC]	
0040A107	. 8D4D 94 LEA ECX,DWORD PTR SS:[EBP-6C]	
0040A10A	. C785 5CFFFFFF MOV DWORD PTR SS:[EBP-A4],CConvert.004042EC	UNICODE "Sorry, Better Luck Next Time!"
0040A114	. C785 54FFFFFF MOV DWORD PTR SS:[EBP-AC],8	
0040A11E	. FF15 94E24000 CALL DWORD PTR DS:[<&MSVBVM50.__vbaVarDup]	MSVBVM50.__vbaVarDup

우선 브레이크 걸고 위아래 함수를 찾아본다.

CPU - main thread, module CConvert		
00409FB8	. 897D 8C MOV DWORD PTR SS:[EBP-74],EDI	
00409FB8	. 8975 84 MOV DWORD PTR SS:[EBP-7C],ESI	
00409FBE	. 0F84 3D010000 JE CConvert.0040A101	
00409FC4	. 8D95 54FFFFFF LEA EDX,DWORD PTR SS:[EBP-AC]	
00409FCA	. 8D4D 94 LEA ECX,DWORD PTR SS:[EBP-6C]	
00409FCD	. C785 5CFFFFFF MOV DWORD PTR SS:[EBP-A4],CConvert.004042EC	UNICODE "Nice Work! You're Now Registered"
00409FD7	. C785 54FFFFFF MOV DWORD PTR SS:[EBP-AC],8	
00409FE1	. FF15 94E24000 CALL DWORD PTR DS:[<&MSVBVM50.__vbaVarDup]	MSVBVM50.__vbaVarDup

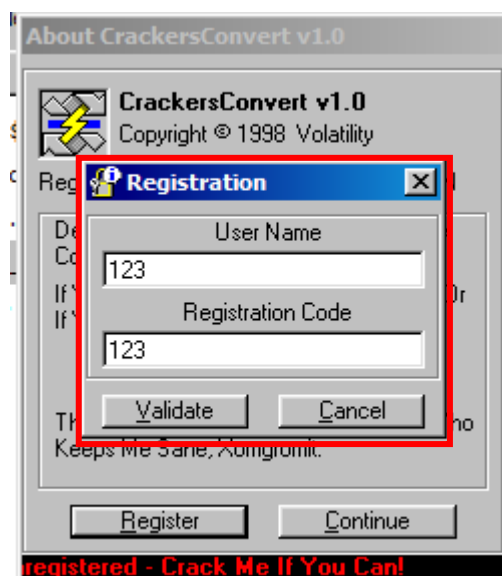
성공했을 때 나오는 문자열을 찾았고 문자열 위에 비교문도 찾았다. 브레이크 걸고 실행

해본다.

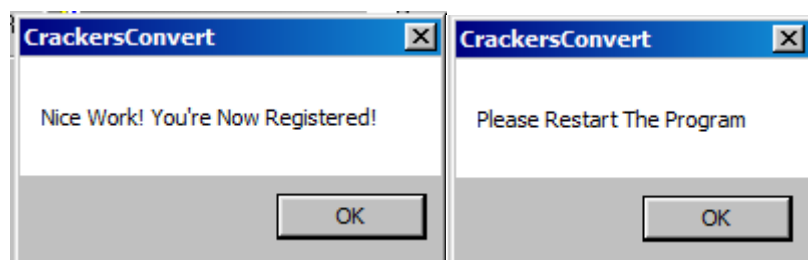


해당 조건문에서 브레이크가 걸리고 활성화된게 보인다.

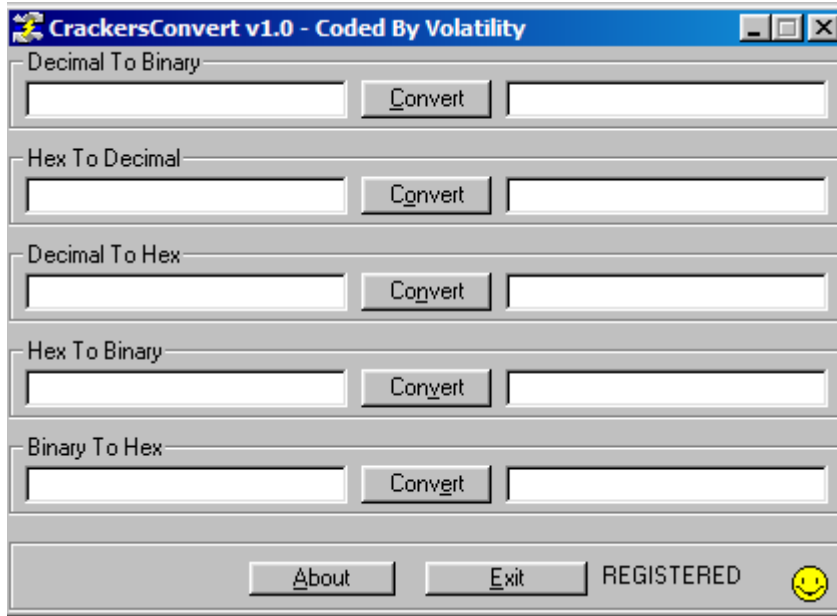
이렇게 되면 점프되서 실패로 뜨니까 이 조건문을 NOP으로 바꿔주고 저장한다.



아무 값이나 입력하고 Validate를 눌러준다.



성공했다는 창과 프로그램을 다시 시작해달라는 창이 발생한다.



다시 실행해보면 REGISTERED가 뜬 걸 볼 수 있다.

3) ReverseMe2 해결 못함.