

2019.02.17. CodeEngn Basic RCE L14

Tree to Tree

Basic RCE L14

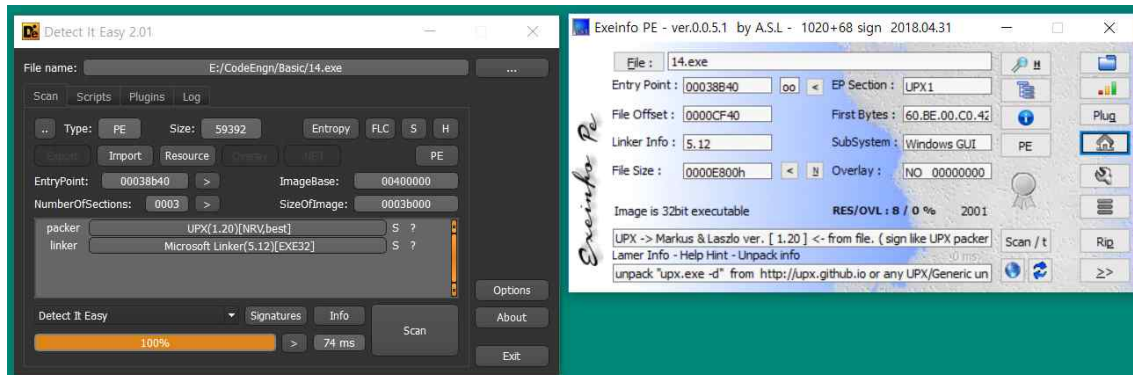
Name이 CodeEngn 일때 Serial을 구하시오
(이 문제는 정답이 여러개 나올 수 있는 문제이며 5개의 숫자로 되어있는 정답을 찾아야함, bruteforce 필요)
Ex) 11111

— Author: BENGALY

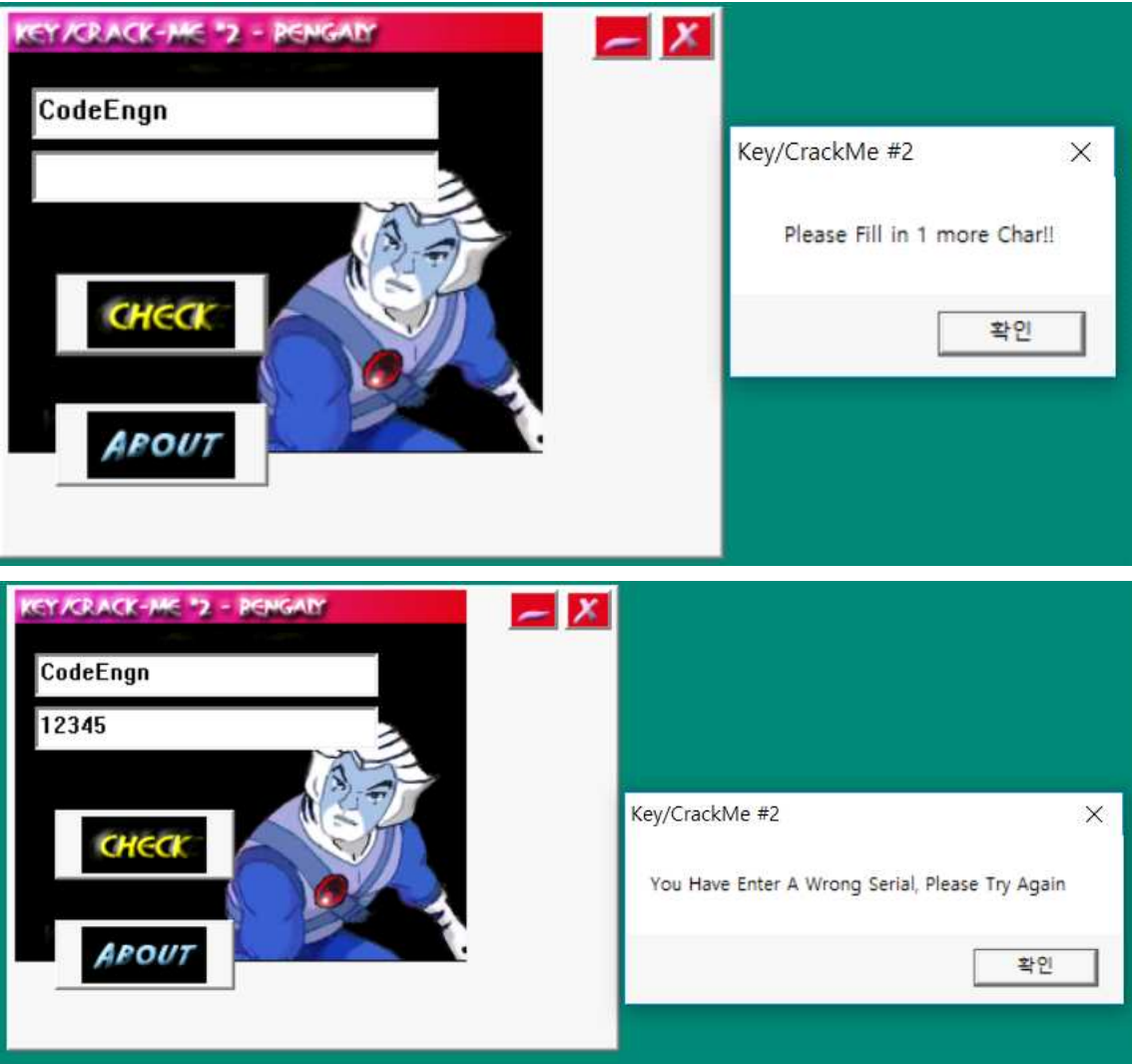
— File Password: codeengn



PE분석기로 보니 UPX패커로 패킹되어있다.



일반적으로 실행했을 때 문자열들을 확인했고 칸을 꼭 채워야 한다.



브레이크 포인트로 pushad와 popad바로 하단 jmp문에 걸고

유형	주소	Module/Label/Exception	상태	디스어셈블리
소프트웨어	00438B40	<14.exe.EntryPoint>	One-time	pushad
	00438C8F	14.exe	활성화됨	jmp 14.401000

OEP를 발견 00401000

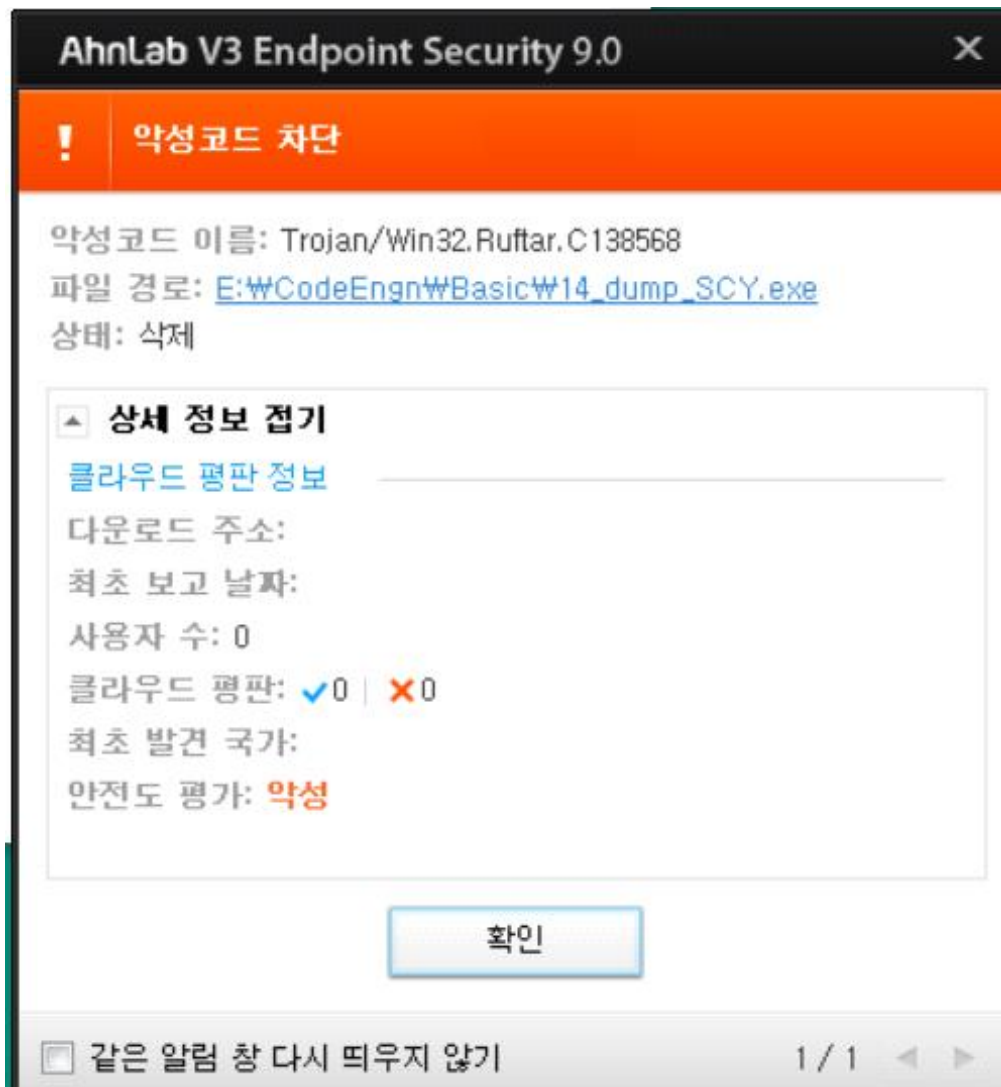
덤프했는데...

악성코드??

Trojan/Win32.Ruftar.C138568

망했다 이미 실행시켰는데..

악성코드 분석으로 바뀌야하는거 아닌가요...?



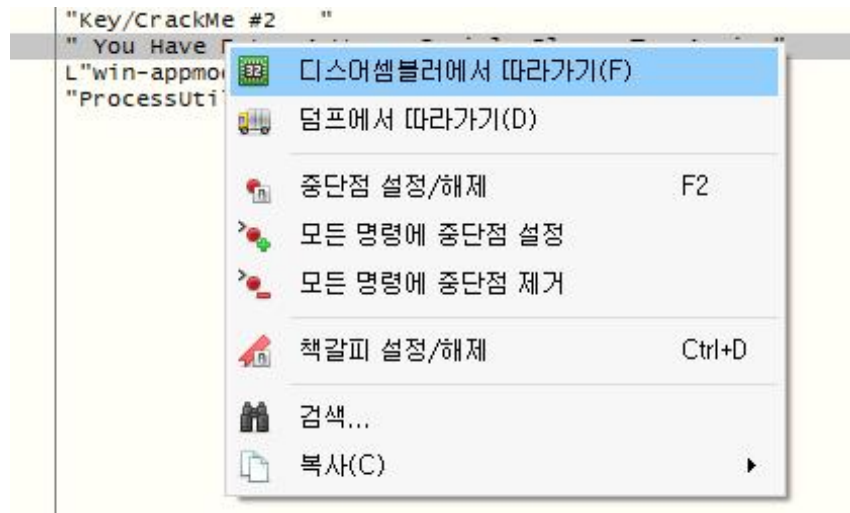
우선 문제를 풀기위해 OEP지점에서 현재모듈 문자열들을 살펴봤습니다.

The screenshot shows the OllyDbg interface. The menu path is: View -> Disassembly -> Follow in Disassembler. The main window displays assembly code. A search for 'kernel32.77888484' is performed, and a list of strings found in the current module is shown. The strings include 'Bengali', 'Mainwindow', 'key/CrackMe - #2', 'Key/CrackMe #2', 'Please Fill in 1 more Char!!', 'Key/CrackMe #2', '& kto', 'Key/CrackMe #2', 'You Have Enter A Wrong Serial, Please Try Again', 'win-appmodel-runtime-11-1-2', and 'ProcessUtilityStruct'.

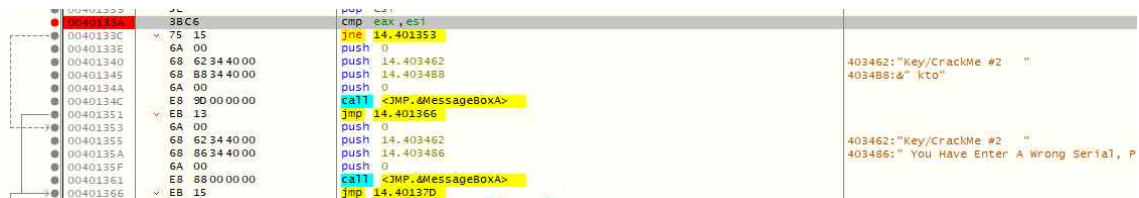
성공문구가보입니다.

주소	디스어셈블리	문자열
00401072	mov dword ptr ss:[ebp-8],14.40302C	"Bengali"
004010A4	push 14.403021	"Mainwindow"
00401179	push 14.40340C	"key/CrackMe - #2"
0040127A	push 14.403462	"Key/CrackMe #2"
004012E1	push 14.403462	"Key/CrackMe #2"
004012E6	push 14.403500	"Please Fill in 1 more Char!!"
00401340	push 14.403462	"Key/CrackMe #2"
00401345	push 14.403488	"& kto"
00401355	push 14.403462	"Key/CrackMe #2"
0040135A	push 14.403486	"You Have Enter A Wrong Serial, Please Try Again"
0040873F	xor dword ptr ds:[ebx-76487A7A],ucrtbase.777DAC86	"win-appmodel-runtime-11-1-2"
00411701	test eax,kernebase.77958389	"ProcessUtilityStruct"

바로 디스어셈블러에서 따라가기



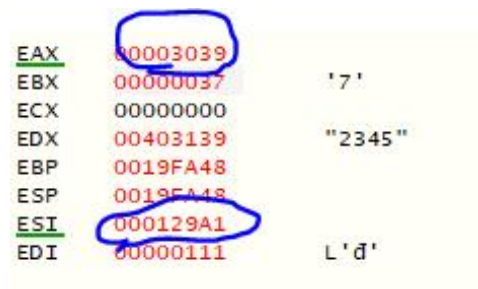
분기문 바로 위쪽 비교구문에서 레지스터의 변화를 관찰해보면

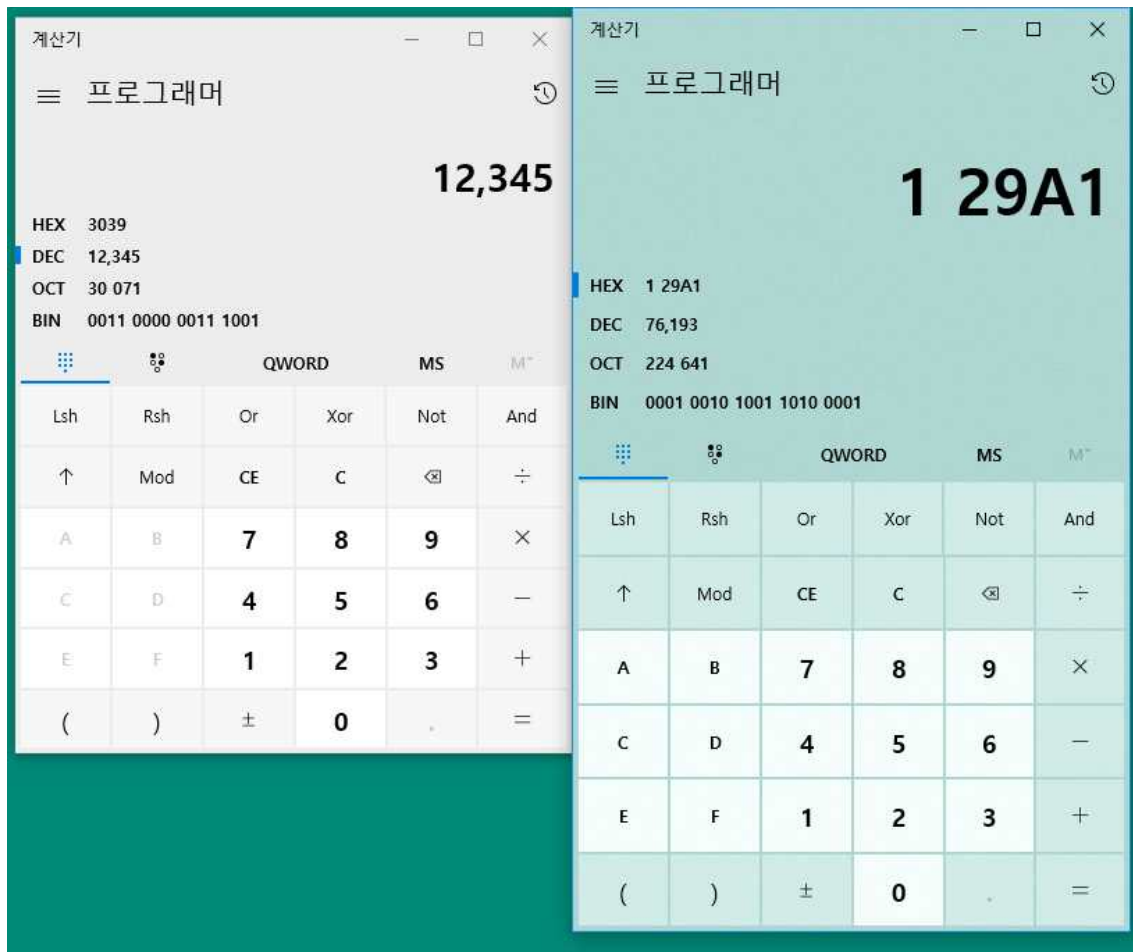


입력값 "12345"가 문자열 -> 숫자로 변환 16진수 3039 EAX

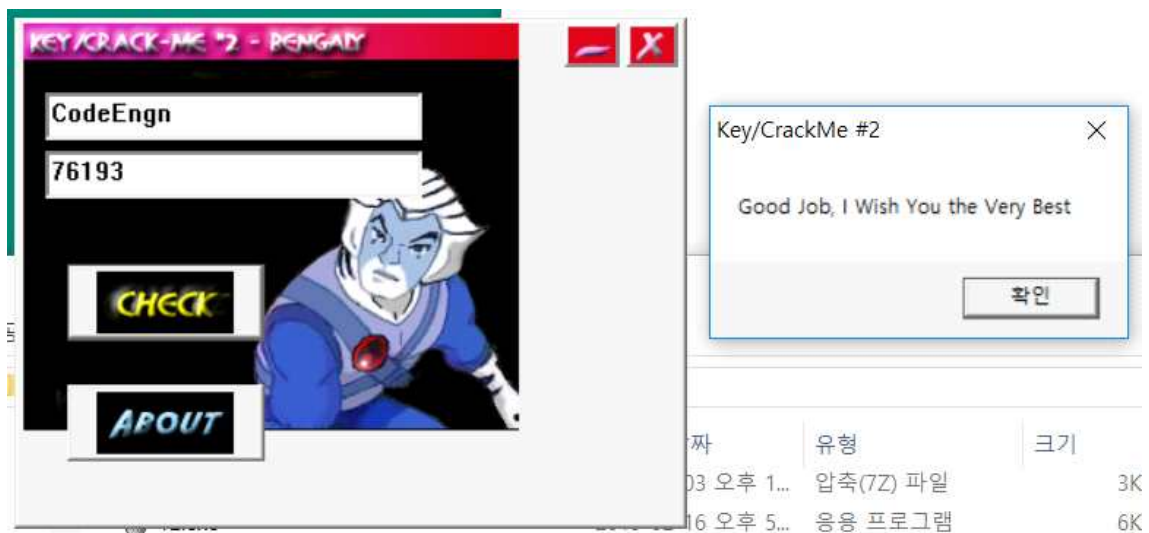
비교하는 값은 16진수 129A1이므로

정답은 10진수 76193으로 예상





CodeEngn과 76193을 넣어보니



Clear.... 그나저나 악성코드.....