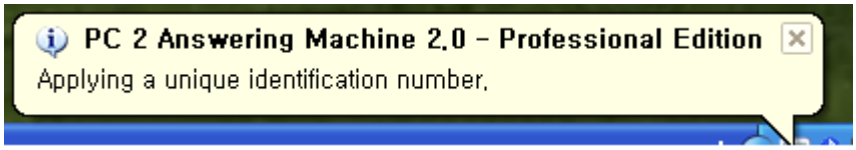
악성코드 분석 보고서

(sand-reversingwithlena-tutorials)

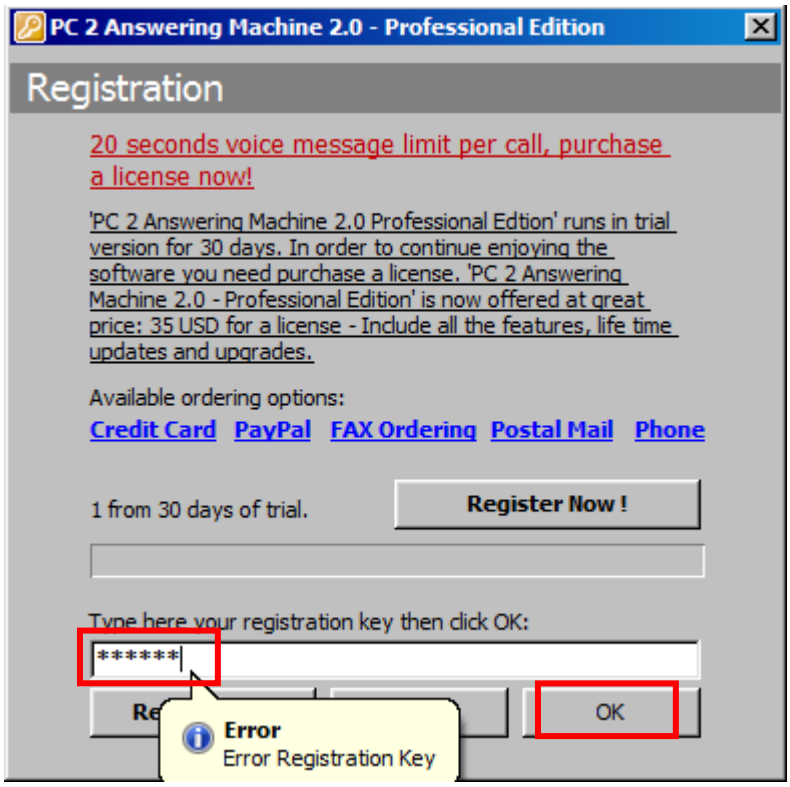
2025.07.01

0 9

1. 문제

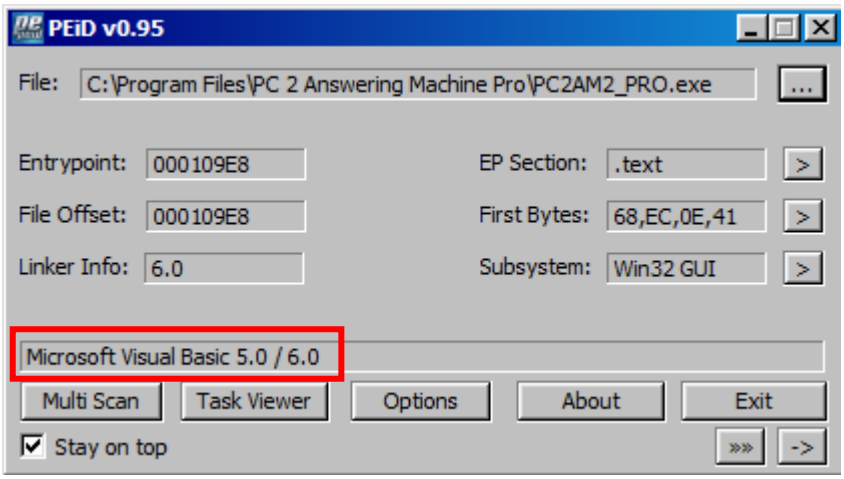


처음 설치할 때 유일한 시리얼 넘버를 사용하는 것을 알 수 있다.



Help > Registraion에 들어가서 시리얼 넘버를 알아내야한다.

2. 해결 방법



PEID로 분석 시 비쥬얼베이직(VB)로 만들어진 걸 볼 수 있다.

VB에서는 프로그램 등록 여부 확인 작업이 DLL의 API에서 수행된다고 한다.

VB에서 쓰이는 가장 유명한 비교 API함수는 아래와 같다.

__vbaVarTstEq

__vbaVarTstNe

__vbaVarCmpEq

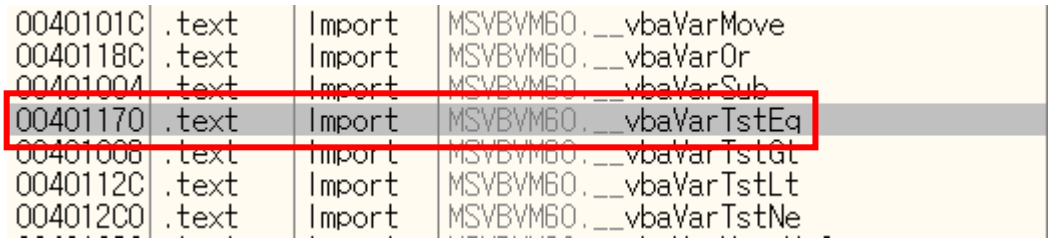
__vbaStrCmp

__vbaStrCmp

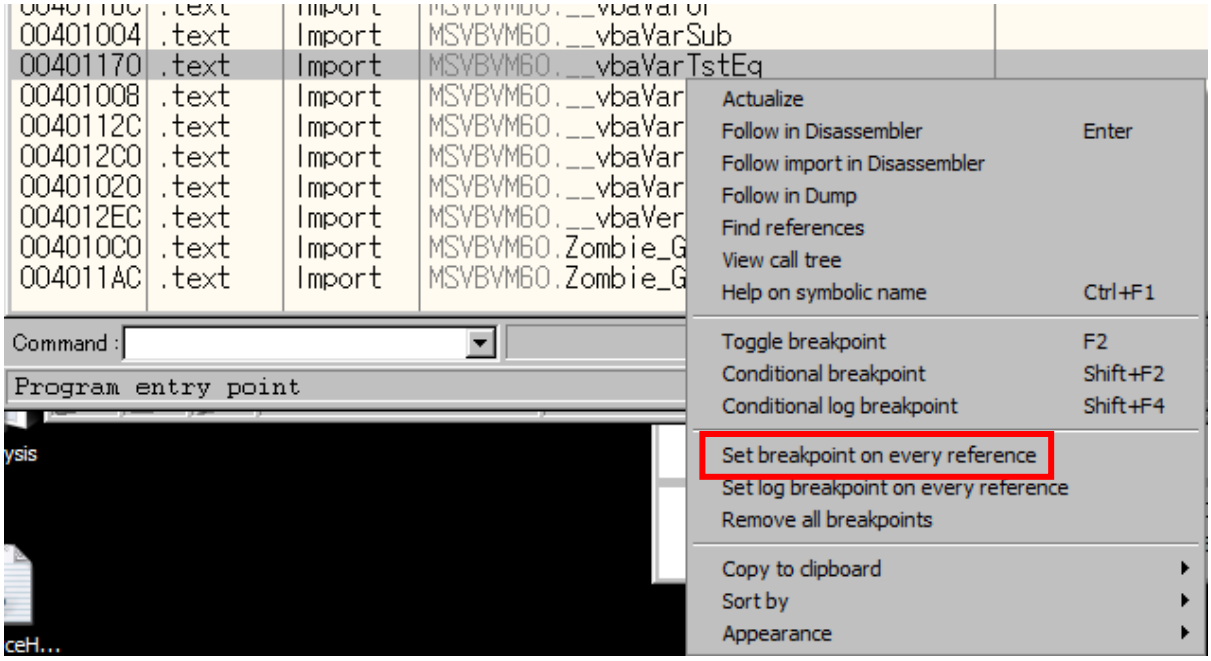
__vbaStrCompVar

'Ctrl+n'을 누르면 import 및 export된 함수를 다 볼 수 있다.

6개의 함수들을 차례대로 검색해 볼 거다.

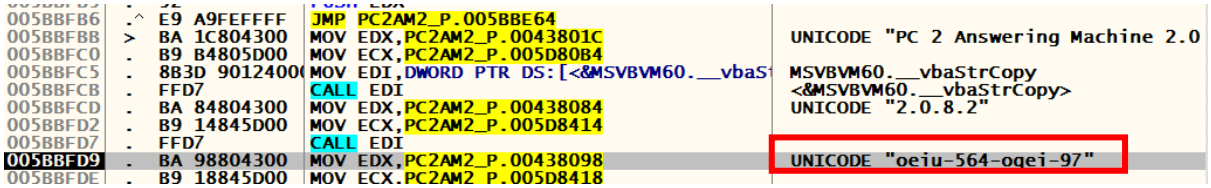


첫 번째로 '__vbaVarTstEq' 를 찾아본다.

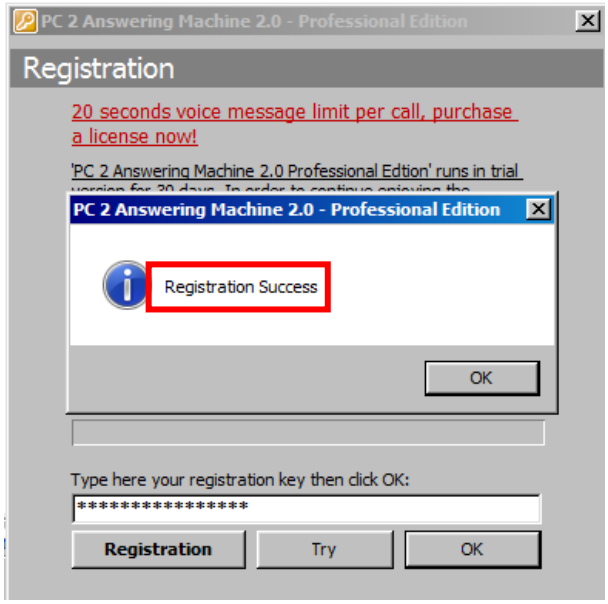


마우스 오른쪽 키 > Set breakpoint on every reference 누르면 이 함수가 사용하는 모든 코드에 브레이크가 걸리게 된다.

누른 후 'F9'를 누르고 'F8'로 하나씩 눌러서 검색해본다



하나씩 내려가다보면 문자가 시리얼 넘버 같은 구문이 하나 검색된다.



이 시리얼 넘버를 넣고 'Ok' 누르면 등록되는 것을 볼 수 있다.

문제 해결!

이거는 문제가 어렵지 않아서 간단히 해결이 되었지만 원래는 다 찾아봐야한다.