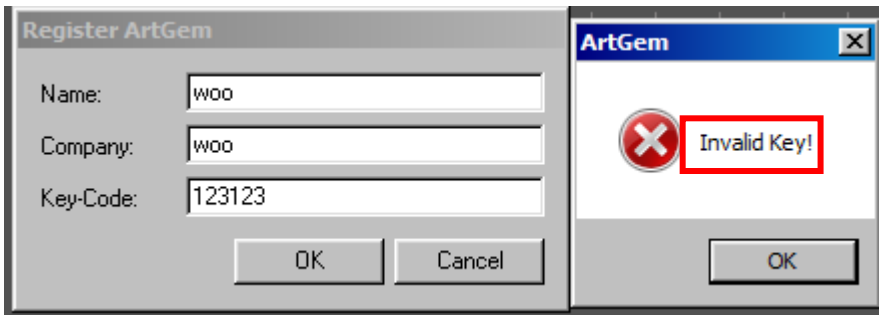
악성코드 분석 보고서

(sand-reversingwithlena-tutorials)

2025.07.01

0 8

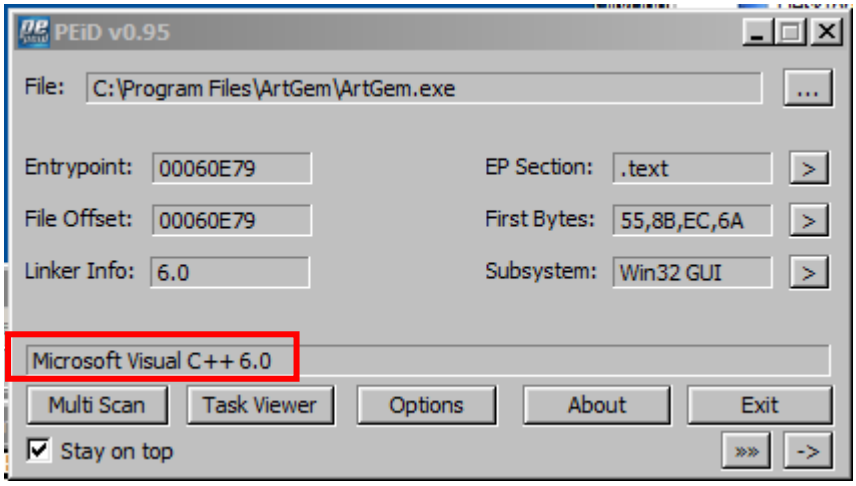
1. 문제



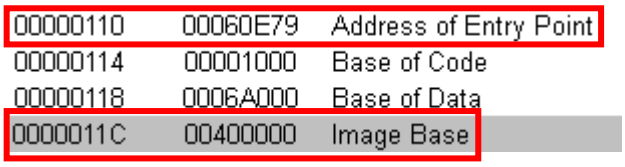
Info > register 들어가면 키 입력하라고 나온다. 키가 다르면 Invalid Key! 발생

위에 'UNREGISTERED! REGISTER NOW!'는 키 문제가 해결되면 없어질 가능성이 있어서 이것부터 해결해본다.

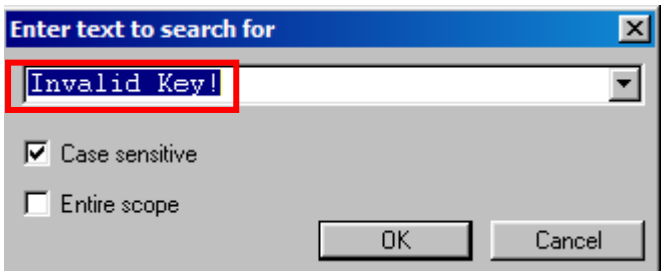
2. 해결 방법



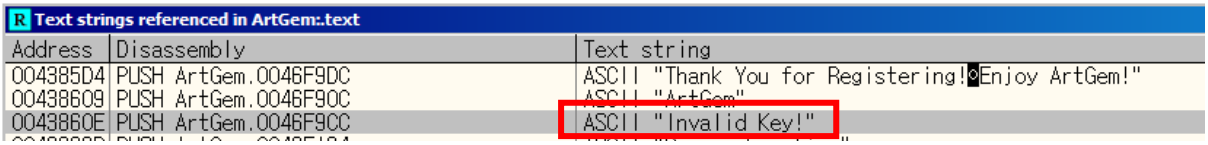
PEID로 먼저 분석 시 압축되어 있지 않은 걸 확인할 수 있다.



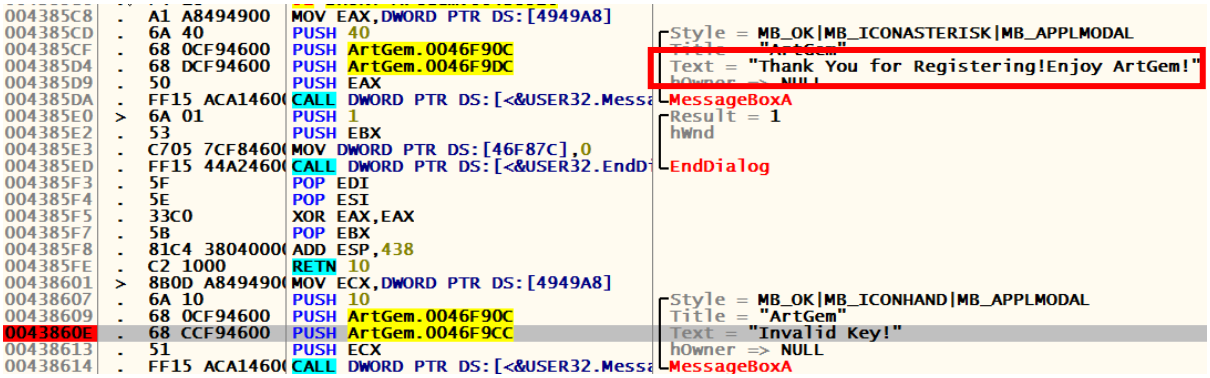
PEview로 확인 시 00460E79에서 시작하는 걸 확인할 수 있다. 코드 주소 확인 시 같은 주소에서 시작하는 것을 확인



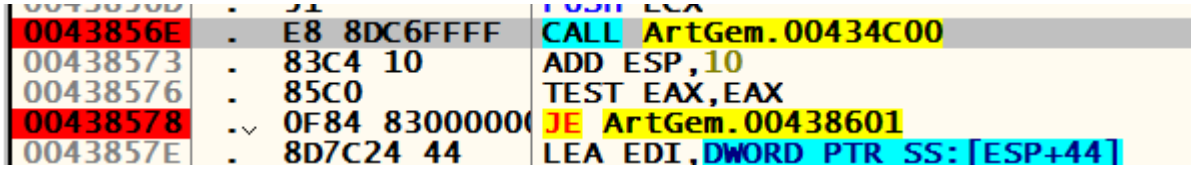
Search for > All referenced text strings 눌러서 Invalid Key! 해당 구문을 찾아준다.



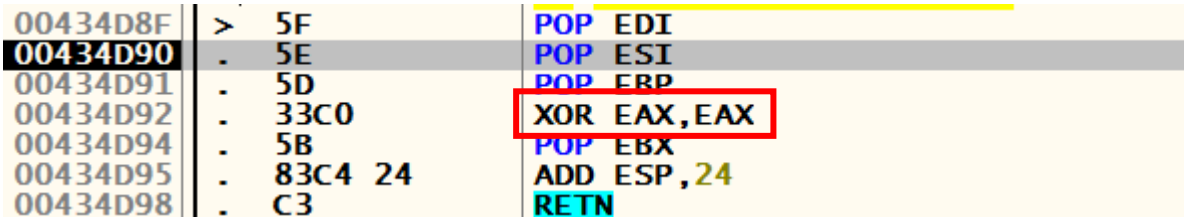
나오는 걸 볼 수 있고 클릭해서 들어가서 그 조건에 해당하는 분기문을 찾아준다.



근데 위에를 보면 레지스터 키를 등록되었다는 구문이 보인다. 그럼 등록되었다는 구문은 지나고 'Invaild Key!'는 지나지 않는 분기문을 찾아준다.

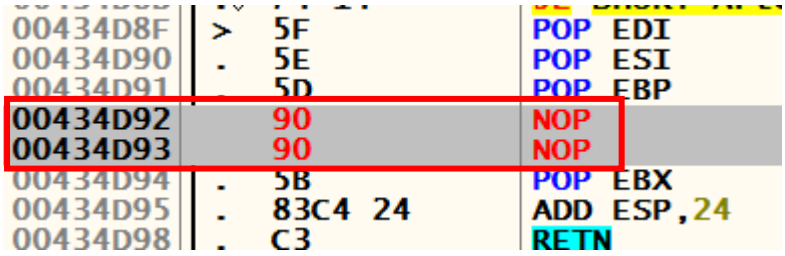


많은 분기문이 있는데 그 중 0x00438578이 어떤 메시지 박스를 보낼지 정하는 분기문이다. 그래서 위에 TEST 함수를 보면 EAX를 비교하는 함수가 있고 EAX는 위에 CALL 함수에서 나오는 걸 볼 수 있다. 이 함수로 들어가본다.

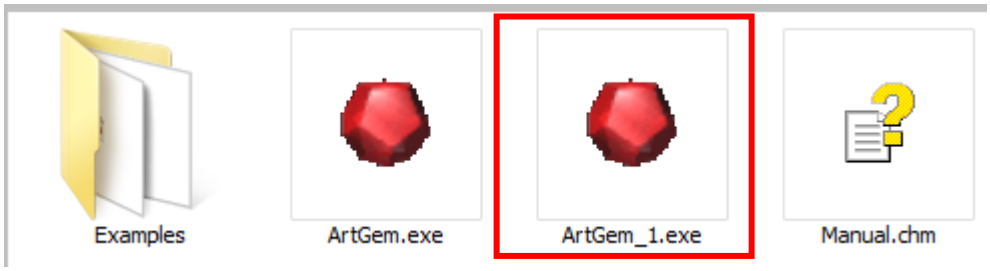


함수에 들어가서 실행하다보면 'XOR EAX EAX' EAX를 초기화하는 것을 볼 수 있다.

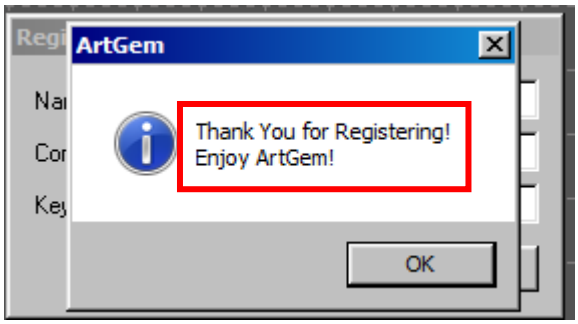
초기화를 하면 당연히 EAX=0, ZF=1 0x00438578이 JE이니까 점프를 하게되고 그럼 'Invaild Key!' 구문 쪽으로 이동하는 것을 볼 수 있다.



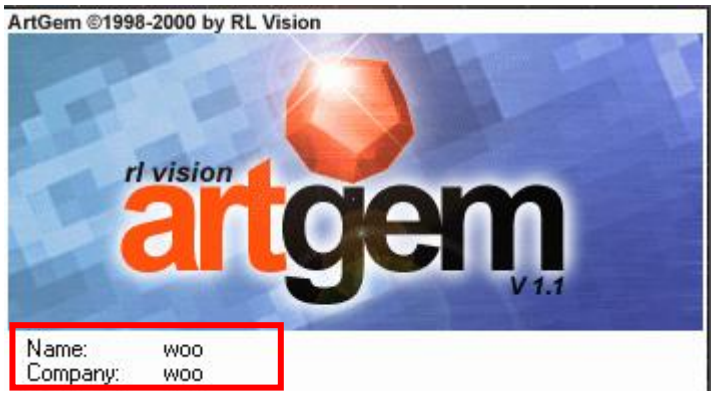
그렇게 안되긴 위해서 'XOR EAX EAX' 를 NOP으로 바꿔주줘서 초기화를 안시켜줘야한다. Binary > Fill with NOPs로 해주고 저장해준다.



ArtGem_1.exe로 저장한다.



실행 후 레지스터 키 등록하면 키 등록이 완료되었다는 창이 발생한다.



다시 실행하면 처음에 떴던 'UNREGISTERED! REGISTER NOW!'가 변경된 것을 볼 수 있다.

문제 해결!