코드엔진 Basic RCE L18

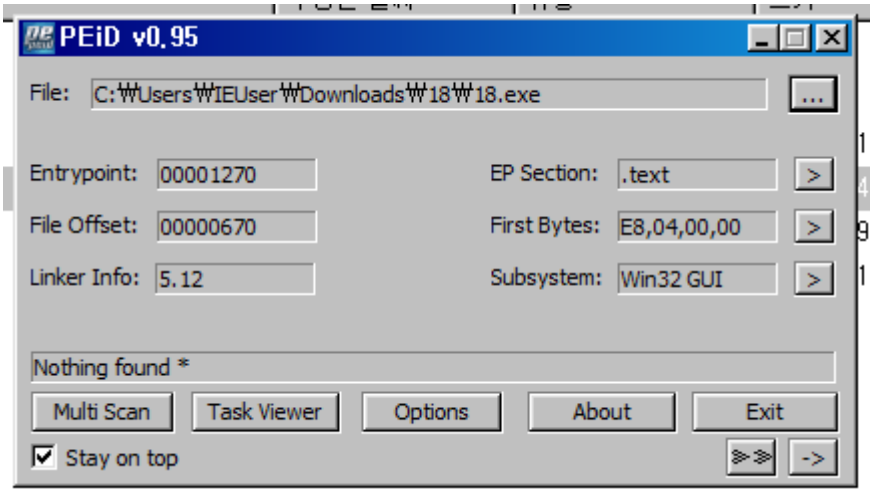
문제

> CodeEngn.com [코드엔진]
>
> 코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을 현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.
>
> https://ch.codeengn.com/

의 Basic RCE L18

해결 과정

- PEiD를 통해 실행파일의 정보를 파악합니다.



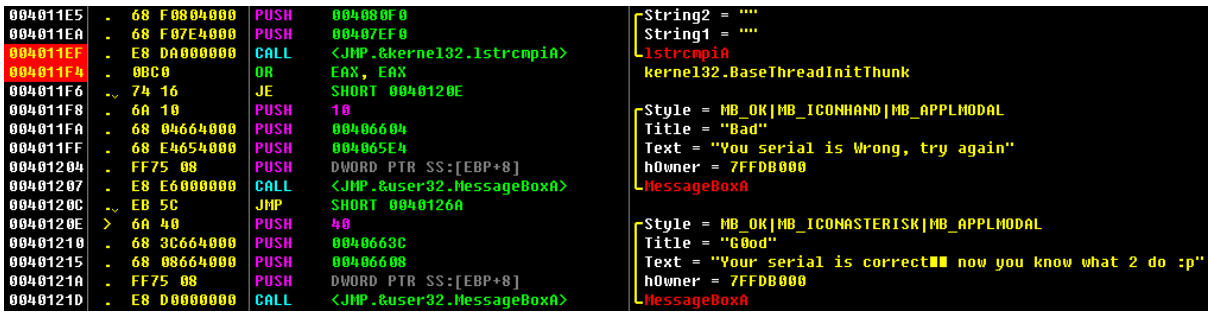
PEiD를 통해 보는 실행파일의 정보들

- ollyDbg를 통해 실행파일 분석을 시작합니다.
- ollyDbg에서 모든 레퍼런스 되는 문자열들을 검색하면 성공시 출력되는 것으로 보이는 문자열들을 볼 수 있습니다.

```
PUSH    004065E4                ASCII "You serial is Wrong, try again"
PUSH    0040663C                ASCII "G0od"
PUSH    00406608                ASCII "Your serial is correct now you know what 2 do :p"
```

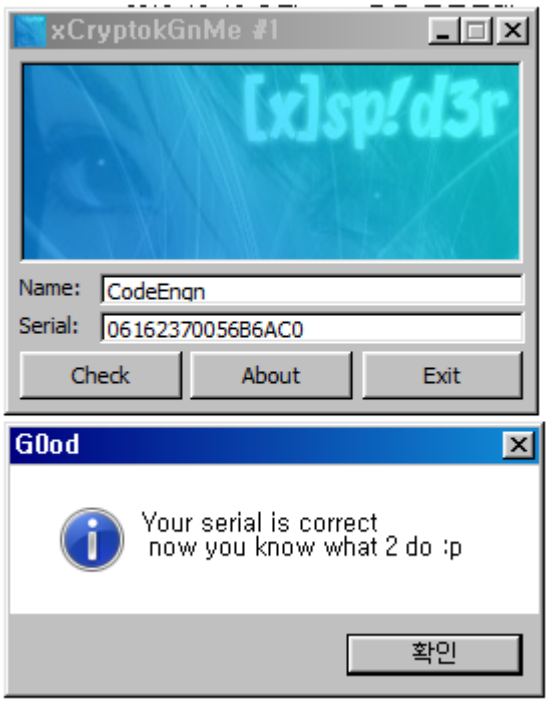
성공시 출력되는 것으로 추정되는 문자열들을 확인가능

- 문자열을 클릭하면 그 문자열을 레퍼런스 하는 코드로 이동할 수 있습니다.



클릭한 문자열을 레퍼런스 하는 코드와 그 주변의 코드들

- 위 코드들을 보면 성공이나 실패 메시지 박스를 출력하는 코드와 JE SHORT 0040120E(계산 결과가 0일 때 0040120E로 점프) 그리고 OR EAX, EAX(EAX 값이 0인지 확인)코드를 볼 수 있습니다.
- 그리고 맨 위에서는 String 두개를 인자로 받는 lstrcmpiA 라는 함수를 볼 수 있는데 이 함수는 두 문자열을 비교하여 같으면 0을 리턴(EAX 레지스터에 저장)하는 함수입니다.
- 참고로, 실행파일을 동작시켜 Name과 Serial을 넣어보면 lstrcmpiA의 두개의 인자 중 String2는 Name을 변형한 문자열이고 String1은 Serial을 그대로 받는다는 것을 확인할 수 있습니다.
- 따라서 CodeEngn을 Name으로 넣었을 때 나오는 String2가 올바른 Serial임을 알 수 있습니다.
- 실제로 Name을 CodeEngn으로 하고 정답이라고 추정한 Serial을 넣어보면 성공 메시지 박스가 출력되는 것을 확인할 수 있습니다.



성공 메시지 박스를 출력하는 실행파일

실행 구조

- 사용자로부터 Name과 Serial을 받습니다.
- Name의 길이가 5미만이면 Serial을 입력하는 칸에 Name의 길이는 5이상이어야 한다고 알려줍니다.
- Name의 길이가 5이상이면 Name에 어떠한 처리를 수행하여 새로운 값을 생성합니다.
- Serial값을 가져와 새롭게 생성한 값과 비교합니다.
- 같으면 점프하여 성공 메시지 박스를 출력합니다.
- 다르면 점프하지 않고 실패 메시지 박스를 출력합니다.
- 프로그램을 종료합니다.