코드엔진 Basic RCE L09

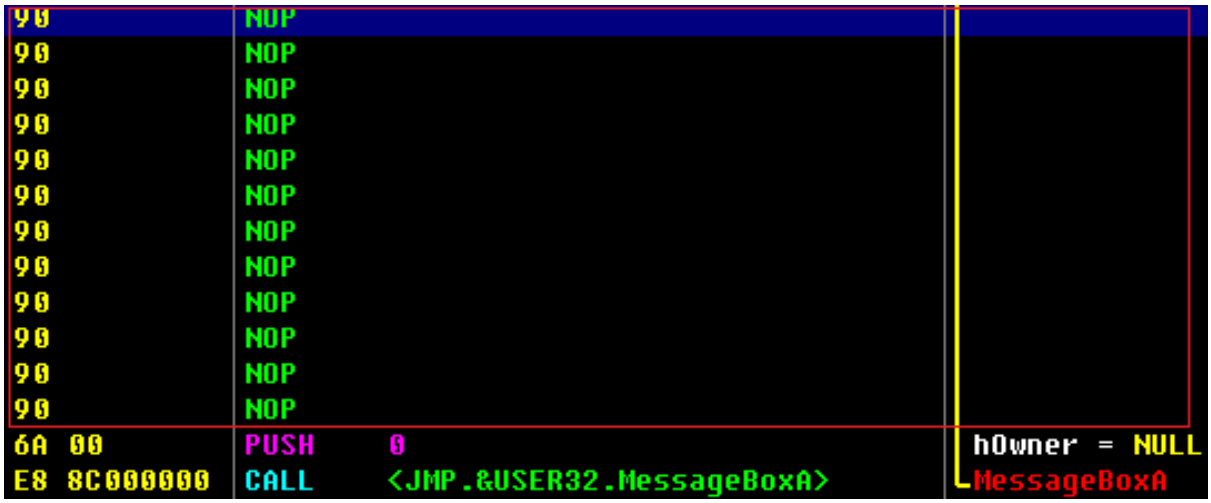
문제

> 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 L09

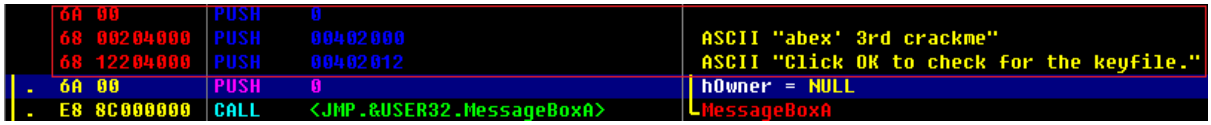
해결 과정

- upx로 패킹된 실행 파일을 언패킹
- 실행파일을 ollyDbg에 올리면 MessageBoxA 함수를 위한 인자가 몇 개 부족함을 확인 가능



빨간 줄 상자 안에 MessageBoxA 함수를 위해 필요한 인자들을 채우는 코드가 없음

- MessageBoxA 함수를 사용하는 실행파일의 다른 코드 부분을 참조하여 부족한 인자들을 채움



빨간 줄 상자안에 MessageBoxA 함수의 필요한 인자들을 채우는 코드들이 추가됨

- 실제 잘 동작하는 것을 확인

잘 표시되고 있는 메시지박스의 문자열들

- ollyDbg에 있는 바이트 코드를 확인해서 깨진 부분의 바이트 코드들을 합하여 해결

빨간 줄 상자안에 있는 HEX들은 추가한 코드들을 바이트로 나타낸 것

실행 흐름

- Keyfile을 체크하겠다는 메시지 박스 출력
- abex.12c라는 파일을 열어보고자 하는 함수(CreateFileA) 수행
- abex.12c라는 파일이 없을 경우 파일이 없다는 메시지 박스 출력
- abex.12c라는 파일이 존재할 경우 그 파일의 파일 크기를 알아내는 함수(GetFileSize) 수행
- 파일의 크기가 특정 크기일 경우 keyfile을 찾았다는 메시지박스를 출력
- 그렇지 않을 경우 찾은 파일이 올바른 Keyfile이 아니라는 메시지박스를 출력
- 위의 모든 로직이 종료되었으면 프로그램 종료