REPORT:

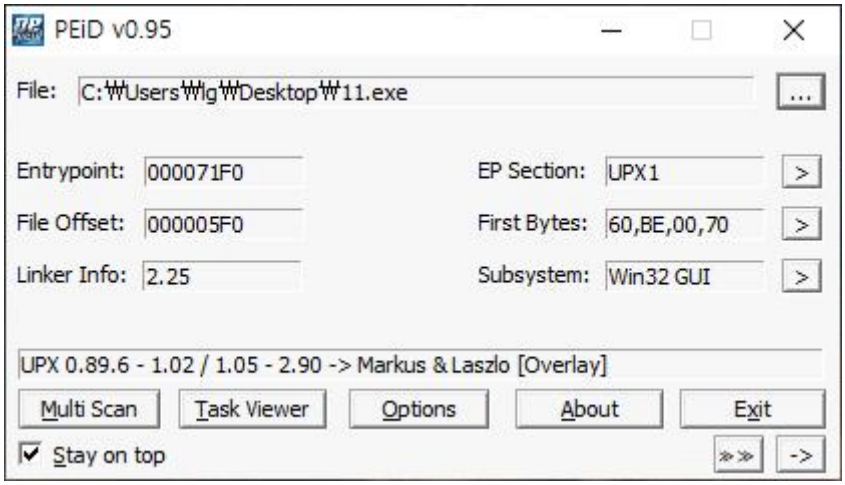
코드엔진 Basic RCE 11 Writeup

COLONY
1824275 정상지

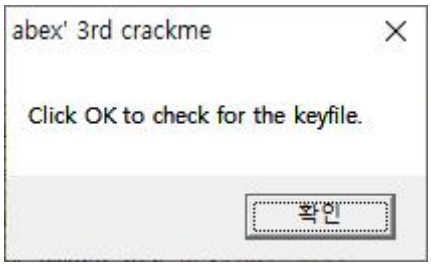
2021.05.30

OEP를 찾으시오. Ex) 00401000 / Stolenbyte 를 찾으시오.

해당 프로그램을 PEiD로 분석 시 UPX로 패킹되어있다

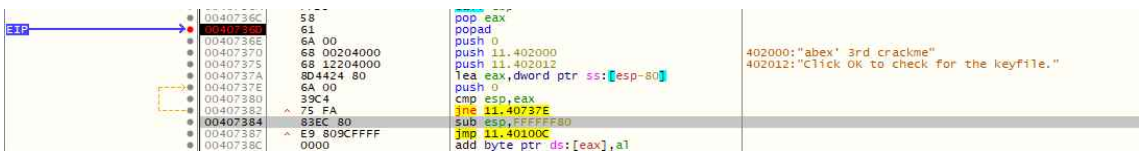


프로그램 실행시



언패킹후 프로그램 실행시

위와 같은 오류가 발생하며 codeengn basic 09번에서 StolenByte를 확인한 것처럼



popad 이후에 있는 push를 통해 값이 입력되는 것을 알 수 있다

StolenByte는 6A006800204000681220400 0

이후 OEP 값을 확인해보면 0040100C로 나온다

정답은 0040100C6A00680020400068122040000