

코드엔진 Basic RCE L10

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 L10

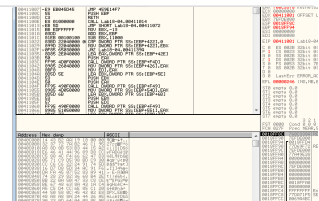
해결 과정

- PEiD를 통해 실행파일이 ASPack으로 패킹된 것을 파악

Category:Digital-Forensics/Computer-Forensics/Anti-Reverse-Engineering/Packers/ASPack

ASPack can be difficult to unpack because it uses self-modifying code. Hence, you should use hardware breakpoints rather than software breakpoints. Given a malware packed with ASPack (idenyified as "ASPack 2.12 -> Alexey Solodovnikov" by PEiD). The malware starts at 0x41001 with a

 <https://www.aldeid.com/wiki/Category:Digital-Forensics/Computer-Forensics/Anti-Reverse-Engineering/Packers/ASPack>



- 위의 사이트에서 알려주는 방법을 통해 OEP를 구하고 패킹된 실행파일을 언패킹
- 언패킹된 실행파일에서 결과를 출력하는 문자열을 찾아 그 문자열을 출력하는 함수 위에 있을 분기점의 코드를 찾아 해결