IR-3

분야	포렌식
문제 파일 (zip)	https://drive.google.com/file/d/1KhkiZXagtpBXRQ63et2ZCyDtpvAIko87/view?usp=sharing
배포 완료	☐
출제자	이현

문제

지금까지 분석하면서 확인된 RAT, 랜섬웨어 악성코드의 이름을 적어라.

이름은 소문자로 입력한다.

ex: KEEPER{RAT이름_랜섬웨어이름}

답

KEEPER{quasar_hiddentear}

풀이 과정

IR-2에 풀이를 너무 자세하게 적어서 IR-2를 참고하면 된다.

IR-2까지 추측성으로 충분히 풀 수 있어서 IR-3에 어떤 파일이 RAT인지 랜섬웨어인지 virustotal에 올려서 확인하는 작업을 통해 두 악성코드의 존재 유무 파악