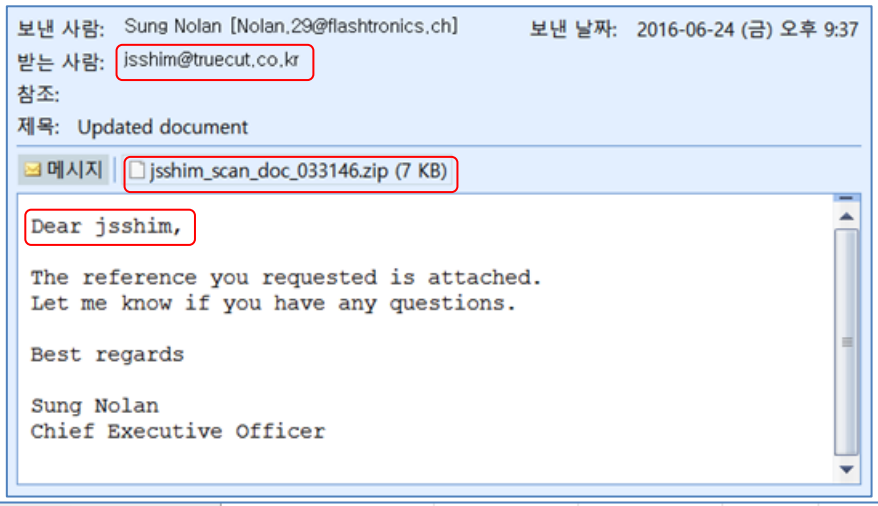
랜섬프리에 의한 자바스크립트 록키랜섬 차단 분석

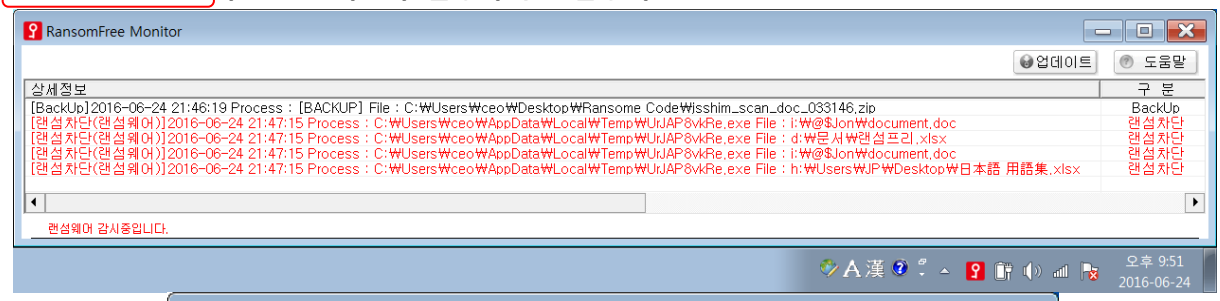
차단일시 : 2016년 6월 24일 21:47:15초

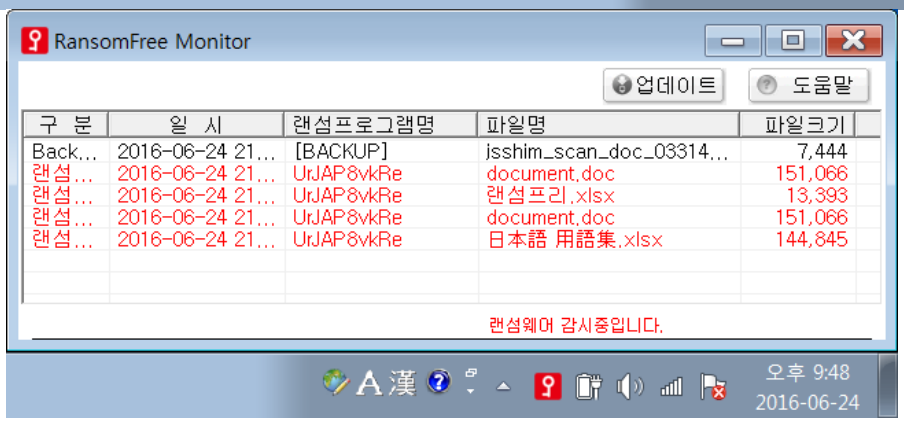
자바스크립트 스팸을 통한 록키 랜섬웨어 : 2016년 5월말경 유럽을 강타한 최신의 랜섬공격

악성코드 배포 : jsshim(메일ID)_scan_doc_033146.zip =>압축을 풀면 unpaid_5d93.js



자바 스크립트 파일을 실행시키면, C:₩Users₩ceo(로그인 계정)₩AppData₩Local₩Temp₩ UrJAP8vkRe.exe라는 프로세스가 실행하여 랜섬공격





랜섬프리가 보호하지 않는 파일 한 개가 랜섬공격을 당한 모습/보호대상 파일은 모두 안전