

5**조** assist

손현기 김주환 김호준 오예린 이동윤 Ruslan 윤명근 교수님

으프로젝트 개요



보안 전문가 보조도구의 부족

정보보호 전문 기업 AhnLab에 따르면 전문가가 하나의 파일을 분석 하는 데는 적게는 몇시간, 많게는 몇 주가 걸리곤 합니다.

하지만 정보보호에 대한 지원은 턱없이 부족하며 자동 분석 도구의 연구 만 진행될 뿐,전문가를 위한 분석 보조도구에 대한 연구는 전무합니다. 그래서 저희는 보안 전문가의 분석 시간을 단축 시켜주기 위한 악성코드 분석 도구 'asi'를 개발하였습니다.

○시스템 흐름도

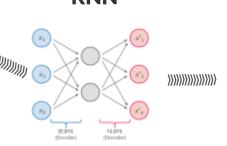




disassemble

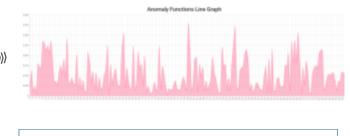
RNN MINIMINI

CNN



이상 탁지

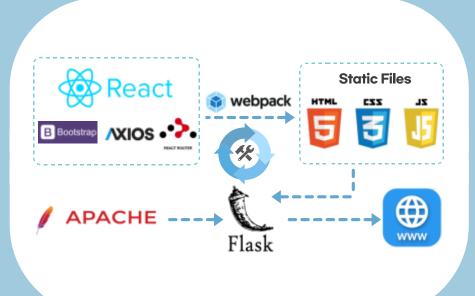




38b5a1e13bc796f7f7a06651fe656572 (2b3e3e8c9c7e11e8b1aedeaede3989)	0.93604	0.92105
2b2d8d5a0fea23990609f544872a9ee0 (#808248713el2/s48satelet5satel22)	0.93539	0.95775
071895421ca6baaa5b7f89fabbf85033 (32387148847344604988711848)	0.93427	0.91935
03fec7d8d5068877c2fbec926683166a aakseodccsalraeee071643cc3fft	0.93371	0.85075
009fc7850d06f63c9da487a1d3461db1 (N00227dbocc54d8b7katc1189464)	0.93281	0.97917

○웹 구조

○ 웹 결과물







7677843 2385167



<이상 탐지>

<상세 정보>

익기대 효과



asi를 사용하면 더 적은 인력으로 더 많은 악성코드를 분석할 수 있습 니다. 따라서 악성코드 분석에 소요 되는 비용을 감소시킬 수 있습니 다.



asi를 사용하면 우선적으로 분석해 야 하는 함수를 추출할 수 있으므로 새로운 악성코드에 대한 분석 시간 을 줄일 수 있습니다. 따라서 악성 코드에 빠르게 대응할 수 있습니다.



asi를 사용하면 악성코드로 의심되 는 파일에 대하여 함수단위 분석결 과, 스트링, 임포트, 익스포트 등 다 양한 결과를 제공합니다. 따라서 입 문자에게 도움이 될 수 있습니다.