A Security Insight

5조 assist

손현기 김주환 김호준 오예린 이동윤 Ruslan
윤명근 교수님

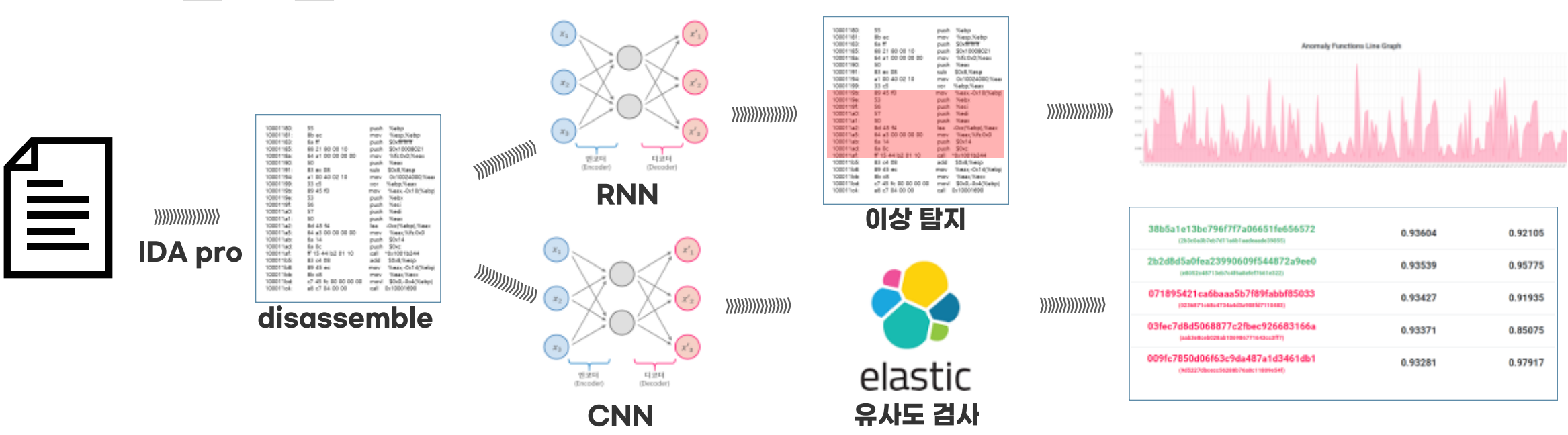
프로젝트 개요

[기사 1]드라마 유령 ' 속 악성코드 , 실제로는? [3]

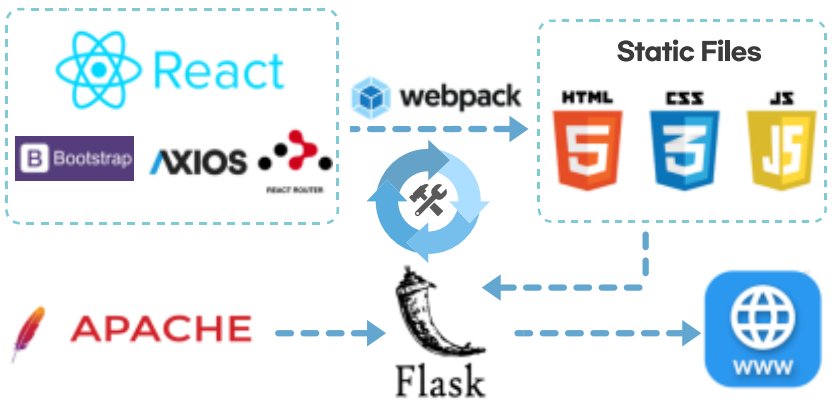
보안 전문가 보조도구의 부족

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 연구만 진행될 뿐,전문가를 위한 분석 보조도구에 대한 연구는 전무합니다.
그래서 저희는 보안 전문가의 분석 시간을 단축 시켜주기 위한 악성코드 분석 도구 'asi'를 개발하였습니다.

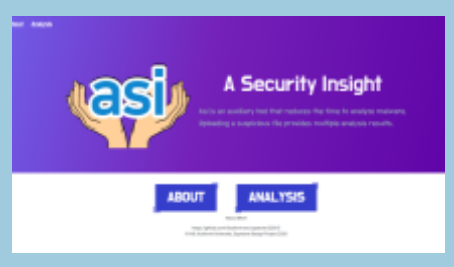
시스템 흐름도



웹 구조

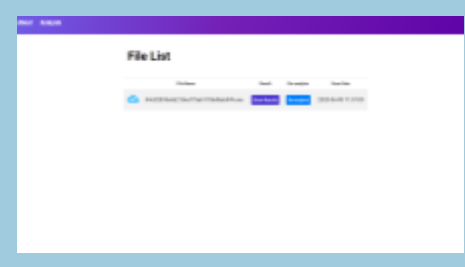


웹 결과물



<메인 페이지>

<파일 업로드>



<업로드 목록>

<유사도 검사 결과>

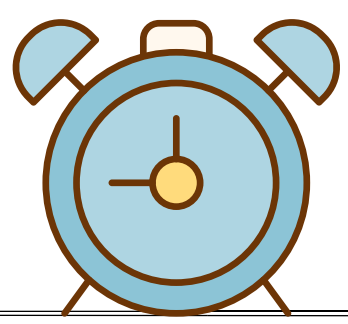
<이상 탐지>

<상세 정보>

기대 효과

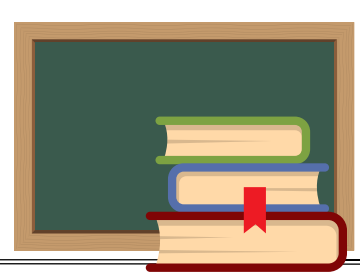
비용절약

asi를 사용하면 더 적은 인력으로 더 많은 악성코드를 분석할 수 있습니다. 따라서 악성코드 분석에 소요되는 비용을 감소시킬 수 있습니다.



시간절약

asi를 사용하면 우선적으로 분석해야 하는 함수를 추출할 수 있으므로 새로운 악성코드에 대한 분석 시간을 줄일 수 있습니다. 따라서 악성코드에 빠르게 대응할 수 있습니다.



교육효과

asi를 사용하면 악성코드로 의심되는 파일에 대하여 함수단위 분석결과, 스트링, 임포트, 익스포트 등 다양한 결과를 제공합니다. 따라서 입문자에게 도움이 될 수 있습니다.