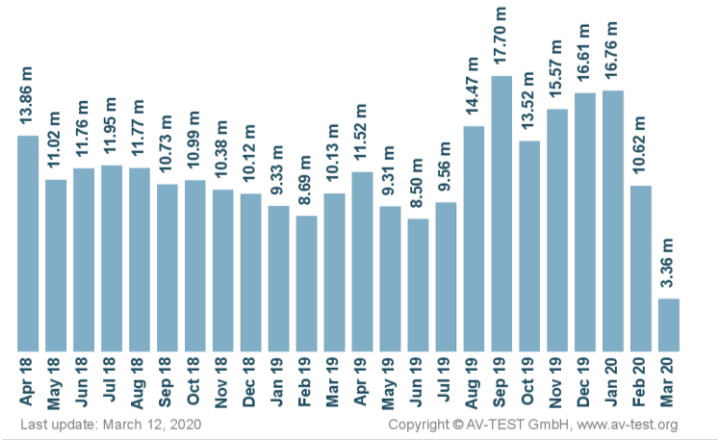
5조 assist
손현기 김주환 김호준 오예린 이동윤 Ruslan
윤명근 교수님

a security insight

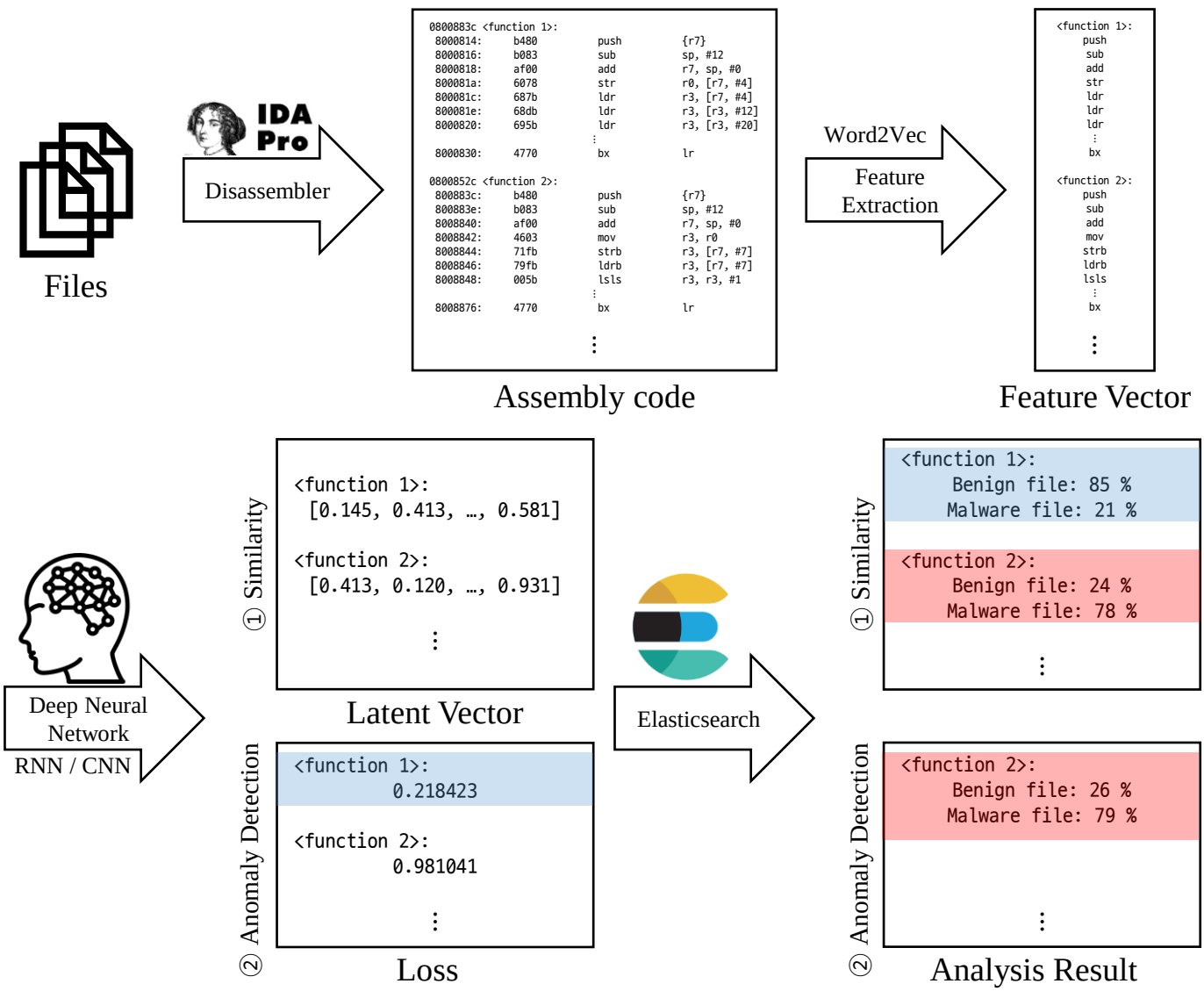
I. 프로젝트 소개



정보 보안 전문 기업 AV-Test에 따르면 매일 약 350,000개의 악성코드가 새로 생성되고 있습니다. 그러나, 새로운 악성코드를 분석할 수 있는 전문가의 수는 한정적이고, 전문가의 악성코드 분석에는 최소 몇 시간에서 최대 몇 주가 소요됩니다.

asi는 악성코드 전문가의 분석 시간을 줄일 수 있는 보조 프로그램입니다. 이 프로그램은 입력 파일의 각 함수 별 악성/정상 여부를 점수화 함으로써, 전문가가 살펴야 할 함수의 수를 줄이는 것을 목표로 합니다.

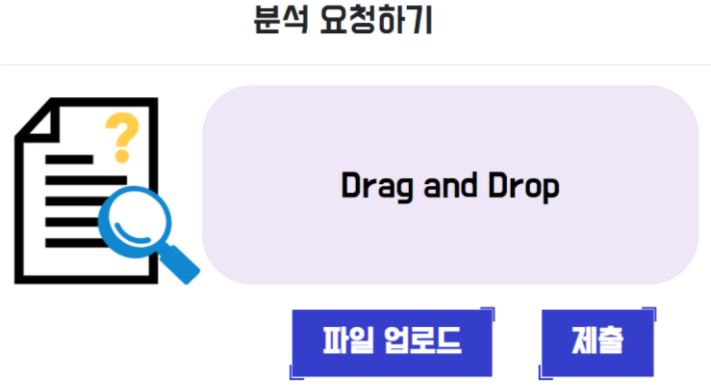
II. 시스템 흐름도



III. 사용 방법

asi는 웹 기반 환경으로 분석자의 컴퓨팅 성능에 관계 없이, 언제 어디서나 편리하게 분석을 수행할 수 있습니다. 접속을 위한 링크는 다음과 같습니다. [http://203.246.112.132:10888/]

1. 파일 업로드



분석자는 웹에 분석하고자 하는 파일을 업로드합니다. 이때 분석자는 다량의 파일을 한 번에 분석할 수 있습니다.

2. 분석 종류 선택

각 파일에 대한 유사도 검사 결과와 이상탐지 결과를 확인할 수 있습니다. 유사도 검사는 모든 함수에 대해 수행되므로 모든 함수에 대한 결과를 확인할 수 있고, 이상탐지는 손실값이 특정 임계값 이하인 함수에 대해 수행되므로 악성이라 의심되는 함수에 대한 결과를 확인할 수 있습니다.

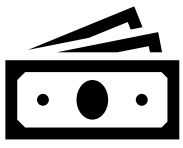
3. 분석 결과

각 함수별 Elasticsearch 화면 완성본을 넣어주세요. (그래프가 있는 그림)

각 함수와 유사한 함수를 Elasticsearch로 검색한 결과를 확인할 수 있습니다. asi는 이를 기반으로 각 함수의 악성 행위 수행 가능성을 점수화 및 시각화하여 보여줍니다. 분석자는 asi의 결과를 토대로 우선적으로 분석해야 하는 함수를 판정할 수 있습니다.

IV. 기대효과

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



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