정 보 보 호 학 회 지
제 29 권 제3호, 2019. 6

머신러닝 기반 보안데이터 분석 연구

이 식*, 김 동 훈*, 조 영 훈*, 명 준 우*, 문 다 민*, 이 재 구*, 윤 명 근*

요 약

최근 머신러닝 기술이 비약적으로 발전하고 있다. 하드웨어 성능이 향상되고 머신러닝 활용 도구가 오픈소스로 사용 편리하게 개발되어 대중화됨으로써 보안데이터 분석 분야에서도 머신러닝을 이용한 기술 개발이 활발히 진행되고 있다. 본 논문에서는 보안 분야의 악성코드 데이터와 보안관제 로그 데이터를 주요 대상으로 머신러닝 기술을 적용할 때 고려되어야 할 기술적 사항들과 최신 연구 동향, 데이터 셋 특징, 그리고 머신러닝 기반의 보안데이터 분석 기술의 기대 효과 및 현재 기술의 한계점 등을 다루도록 한다.

Ⅰ. 서 론

머신러닝과 인공지능 기술이 급속히 발전하고 있으며, 자율 주행, 스마트팩토리, 의료 및 헬스케어 등 많은 분야에서 실용적인 기술로서 이미 활용되고 있다. 우리 주변의 사물인터넷 기기부터 데이터센터 클라우드에 이르기까지 다양한 컴퓨팅 환경에서 빅데이터가 생산되고 있으며 머신러닝을 위한 양질의 학습 데이터로 사용될 수 있을 것으로 기대된다. 데이터가 연료가 되고 인공지능 기술이 엔진 역할을 하는 소위 4차 산업혁명 시대가 개막된 것이다.

보안 분야에서도 최근 인공지능이 화두가 되면서, 다양한 보안데이터를 분석하는데 머신러닝 기술이 활발히 도입되고 있다. 보안 산업은 전통적으로 데이터가 많이 생산되는 분야이며, 누적된 데이터로부터 사이버 공격이나 이상징후를 탐지하는 것이 중요한 문제였다. 하지만 보안 분야에서 생산되는 데이터의 양은 항상 동시대 분석 기술로는 감당하지 못할 정도로 많았으며, 한정된 보안전문가의 인력으로는 도저히 전체 데이터를 분석하는 것이 불가능했고, 또한 다양하게 변화되는 새로운 공격 기법을 유연하게 인식하여 분석 업무에 반영시키는 것은 요원한 기술처럼 보였다.

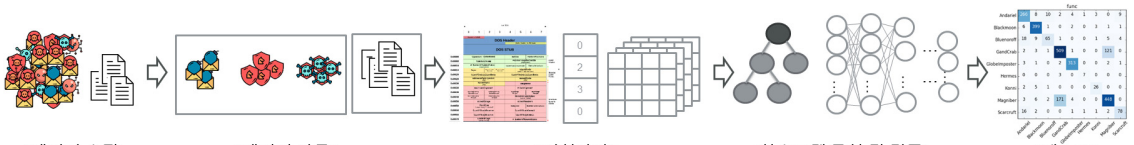
최근 머신러닝 기술이 비약적으로 발전하고 대중화되면서 보안데이터 분석이라는 전통적 난제에 보안전문가들이 다시 한번 도전할 수 있다는 희망이 생겨났다. 멀티프로세서, GPU(Graphical Processing Units), 고속 저장장치 등 하드웨어 기술의 비약적 발전으로 머신러닝은 이전보다 많은 데이터를 신속하게 처리할 수 있게 되었다. 동시에 심층학습(deep learning) 알고리즘과 소프트웨어 기술의 발전으로 머신러닝은 이전보다 유연하게 공격이나 이상징후를 탐지할 수 있게 되었다. 보안데이터 분석을 위한 강력한 도구가 준비된 것이다.

학계와 산업계에서도 머신러닝 기반의 보안데이터 분석 연구가 국내외에서 활발히 진행되고 있다. 최근 국제 학회와 저널에서는 딥러닝을 이용한 보안데이터 분석 연구가 논문으로 발표되고 있으며[1][2][3][4], 구글이 인수한 캐글(kaggle)이나 국내 기관에서도 등 보안데이터 분석 대회를 개최하고 있다[5][6][7][8]. 사실 이러한 데이터 분석 연구에 대한 니즈와 기대는 이번이 처음이 아니다. 인터넷 비즈니스가 시작되었던 2000년 전후에도 보안데이터를 데이터마이닝과 인공지능으로 분석해보려는 적극적인 시도가 있었으며, 20년이 지난 최근에 와서 딥러닝과 인공지능 열풍으로 한 번 더 많은 관심이 집중되고 있다.

본 논문에서는 최근 머신러닝 기술을 이용한 보안데이터 분석 분야의 연구 동향을 소개한다. 주요 연구 논

이 논문은 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016R1A2B4009083, No. NRF-2018R1C1B5086441). 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2018-0-00429, 보안 빅데이터 자동 분석을 위한 실시간 유사도 측정 원천 기술 연구)

* 국민대학교 컴퓨터공학과 (seek2058@kookmin.ac.kr, donghon92@naver.com, cyh905@gmail.com, mjw9505@naver.com, vmfn0401@gmail.com, jaekoo@kookmin.ac.kr, mkyoon@kookmin.ac.kr)



〔그림 1〕 머신러닝 기반 보안데이터 분석 과정

문과 보안데이터 분석 대회를 소개한다. 그리고 주요 머신러닝 알고리즘과 보안데이터 분석에서 이용할 때의 주요 고려사항들을 다룬다. 특히 보안데이터 분석 분야에 머신러닝 기술을 도입할 때의 장점과 현재 기술의 한계에 대해서도 다루도록 한다.

Ⅱ. 머신러닝 기반 보안데이터 분석

보안데이터 분석에 이용될 수 있는 머신러닝 기술들에 대해서 데이터의 종류를 악성코드와 보안관제 로그로 한정하여 구체적으로 살펴본다.

머신러닝을 이용한 보안데이터 분석 과정은 데이터 수집, 가공, 피처추출, 학습모델 구현 및 검증, 테스트 과정으로 이루어진다([그림 1] 참고). 딥러닝은 이 중에서 피처추출 부분을 자동으로 해준다는 장점이 있으며, 특히 원본 데이터(raw data)만을 입력으로 주면 알아서 피처추출과 학습까지 자동으로 완료해주는 경우를 E2E 딥러닝(end-to-end deep learning)이라고 한다. 악성코드 연구 논문 중에서는 Raff 등이 CNN(Convolutional Neural Network) 기반의 E2E 딥러닝 모델과 2,000,000개의 파일을 사용해서 악성코드 파일을 탐지하는 모델을 개발했다고 발표했으나[5], 탐지 정확도는 동질적 데이터 셋에 대해서 94% 정도로 크게 높지는 않은 수준이다.

아직까지는 대다수의 연구에서 보안데이터 피처추출에 사람이 개입하는 경우가 많다. 예를 들면 요즘 많이 유행하는 악성코드의 실행 영역에서 추출한 실행 명령어를 2차원 이미지로 바꾼 후 CNN으로 학습시키는 방식이 대표적인데[2][13], 이는 E2E 딥러닝으로 보기 어렵다. 바둑에서 알파고가 인간이 생각하지 못했던 방식으로 프로 기사들을 이겼던 것처럼, 보안데이터 분석에서도 기존 전문가들이 상상할 수 없었던 새로운 피처를 딥러닝이 발견할 수 있도록 하려면, 다시 말해서 딥러닝을 가장 딥러닝답게 잘 활용하기 위해서는 더 많은 연구가 필요하다.

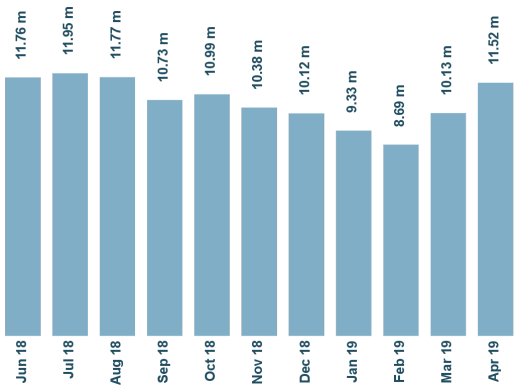
2.1. 머신러닝 기반 악성코드 데이터 분석

악성코드 발생량은 꾸준히 증가하고 있으며, 공격자들은 기존 코드를 조금씩만 변형하여 단순 규칙 기반의 안티바이러스와 탐지 시스템을 우회하고 있다. [그림 2]는 AVTest에서 발표한 매달 발견되는 새로운 악성코드의 개수에 대한 통계인데, 매달 평균 천만 개 이상이 수집되고 있으며 이는 분석 전문가의 수동 분석이 가능한 수준을 넘어선 것이다. 따라서 인공지능에 의한 자동 분석 기술 개발이 이제는 선택이 아닌 필수가 되었다. 본 논문에서 악성코드 중 가장 많은 영역을 차지하고 있으며 최종적으로 타격을 가하는 실행파일에 대해서 주로 다루기로 한다[14].

머신러닝을 데이터 분석 기술로서 사용할 때는 머신러닝 알고리즘 및 모델 최적화 기술만큼이나 데이터의 특성을 분석하는 것이 중요하다. 본 논문에서는 최근 악성코드 데이터의 특징을 소개하고 이러한 특징이 데이터 분석에 어떤 영향을 미치는지 살펴본다.

최근의 악성코드 데이터가 갖는 큰 특징 중 하나는 상당히 유사한 악성코드들이 지속적으로 반복적으로 등장한다는 사실이다. 이는 데이터 분석 대회에서 배포하는 데이터 셋에서도 발견되는 현상이다. 유사하다는 것을 공학적으로 명확히 정의하는 것은 데이터를 보는 관점에 따라서 크게 달라진다. 가장 많이 사용하는 유사도 측정 지표 중 하나인 자카르드 인덱스(Jaccard index)를 예로 들면, 우선 주어진 데이터를 집합 형태로 변형시킨다. 이제 주어진 두 개의 데이터 사이의 유사도는, 각 데이터로부터 생성된 집합들의 교집합과 합집합을 구하고, 교집합의 크기를 합집합의 크기로 나눔으로써 측정될 수 있다.

본 논문의 저자들은 최근에 수집한 백만 개의 악성코드 데이터 셋을 분석한 결과, 절반 이상의 악성코드는 이전에 수집된 악성코드 중 적어도 하나 이상과 0.95 이상의 자카르드 인덱스를 가지는 것을 확인했다. 즉, 악성코드 사이의 유사한 관계를 분석하는 것만으로도



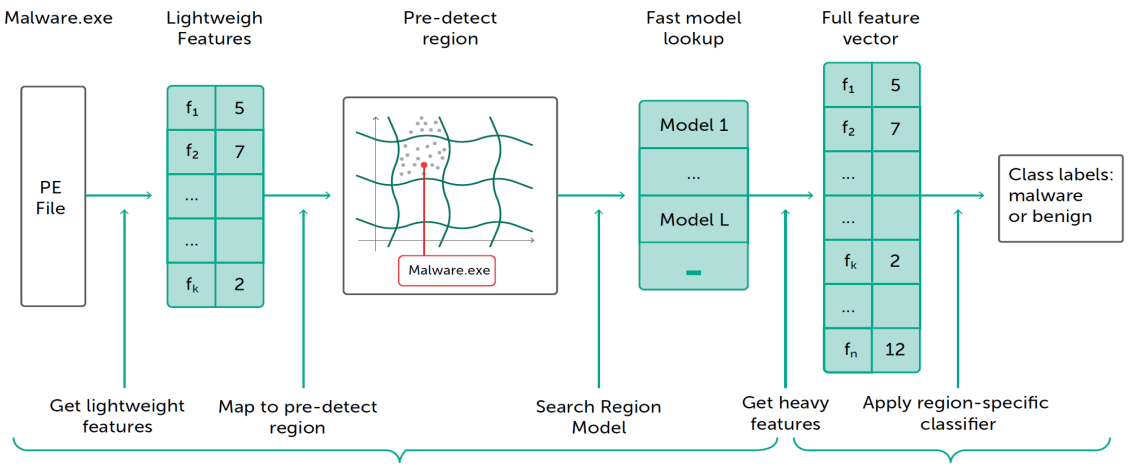
〔그림 2〕 최근 매달 발견된 새로운 악성코드의 개수. 2018.6~2019.4 (출처: AVTEST)

절반 이상의 데이터는 이전에 분석한 자료만으로 분석이 완료될 수 있으며, 이는 머신러닝 기반 악성코드 분석에서 주목해야 할 점이다. 이 실험 결과는 최근에 발표된 악성코드 빅데이터에 대해서 유사성을 분석한 논문의 결과와도 일치한다[14].

실제로 악성코드 분석에 대한 대다수의 기존 논문과 데이터 분석대회 결과를 보면 정확도가 95%를 넘으며 99% 이상을 달성하였다는 보고도 자주 목격할 수 있다. 이런 경우는 학습 데이터를 구성하는 악성코드의 피처가 유사한 형태로 반복적으로 나오기 때문에 분류(classification) 정확도가 높아진 것으로 볼 수 있는데, 학습된 모델을 다른 악성코드 데이터 셋에 대해서 테스트를 해보면 정확도가 형편없이 낮아지는 경우가 많다. 즉, 학습데이터에 등장했던 악성코드와 매우 유사한 형태가 테스트 데이터에서도 자주 등장했기 때문에 실험 과정에서만 정확도가 높게 얻어지는 전형적인 오버피팅(overfitting) 현상으로 볼 수 있다. 한정된 데이터 셋으로 실험한 정확도 결과에 지나치게 낙관적으로 기대하는 것은 바람직하지 못하다.

머신러닝 기반 악성코드 분석 연구에서 어려운 부분 중 하나는 데이터 셋의 분포가 한 쪽으로 치중되는 경우가 많다는 점이다. 악성과 정상을 분류하는 문제에서는 일반적으로 정상 파일이 악성 파일보다 구하기 어려운 경우가 많다. 이 문제를 해결하기 위해서 부족한 파일을 확보된 데이터로부터 생성해내는 머신러닝 분야의 데이터 증강(data augmentation) 기술을 도입하여 사용할 수 있다[2].

다른 대안으로는 카스퍼스키 보고서에서 소개된 방식처럼 일차적으로 악성코드들을 대분류해놓고 분류된 그룹별로 악성과 정상을 판별해주는 이진 분류기를 학습시키는 방식을 고려할 수 있다[15]. [그림 3]는 카스퍼스키의 머신러닝 기반 악성코드 탐지 전략을 보여준다. 그림 밑 부분에서 표시된 것처럼 크게 두 부분으로 나뉘어져 있는데, 첫 번째 부분에서 악성코드에 대한 대분류를 일차적으로 진행하고, 여기에서 명확히 판별되지 않는 파일들에 한하여 이차 분류를 진행한다. 흥미로운 부분은 명확한 판별이 어려운 파일들로 형성된 여러 그룹이 만들어질 수 있다는 점이며, 각 그룹에 대해서 머신러닝 모델을 학습시킬 때에는 해당 그룹의 악성코드와 정상 파일 전체에 대해서 학습을 진행한다는 점이다. 세부적인 내용은 카스퍼스키 자료를 참고하기 바란



〔그림 3〕 카스퍼스키 악성코드 2단계 분류 기술 개념도. 1단계 분류 실패한 대상에 한하여 2단계 분류 기술 적용〔15〕

다[15].

2.2. 머신러닝 기반 보안관제 로그 분석

보안관제 로그는 이미 오래전부터 엄청난 분량이 축적되고 있는데, 아직 데이터의 극히 일부만이 분석 대상으로 활용되고 있다. 국내외 보안관제 서비스를 제공하는 회사나 기관에서도 침입탐지시스템이나 침입방지시스템의 로그처럼 장비의 탐지 규칙을 한 번 통과한 데이터만을 주로 저장 및 활용하고 있다.

보안관제 로그의 특징은 발생한 이벤트 중 정탐(true positive)의 비율이 전체 로그 대비 매우 적으며, 오탐(false positive) 발생이 매우 많다는 점이다. 과거 보안관제 로그 분석 연구는 정탐 비율을 높이고 오탐 비율을 낮추는 것을 주요 목표로 하였으며, 대다수의 보안관제 로그 분석을 수행하는 실무 기관에서는 발생한 공격 탐지 이벤트들을 내부적으로 한 번 더 거르는 규칙들을 보유하고 있다.

최근에는 딥러닝을 적용한 보안관제 로그 연구 결과가 주요 학회에서 발표되고 있다. 다양한 보안 장비로부터 수집되는 이벤트 로그를 중앙 SIEM(Security Information and Event Management)에서 RNN(Recurrent Neural Network) 모델로 학습시켜 분석하는 연구가 발표되었으며[3], 스토리지 장비로부터 생성되는 이벤트들을 머신러닝 모델 학습을 시켜서 심각한 정도와 해결하는데 걸리는 시간을 예측할 수 있는 연구 결과도 발표되었다[16]. 즉, 단순하게 정탐 오탐을 판별하는 것을 넘어서 미래에 발생할 일을 구체적으로 예측하는 연구로 범위가 확대되었다.

비슷한 맥락에서, 전 세계에 설치된 시만텍 침입방지시스템(Intrusion Prevention System)으로부터 수집된 단일 타입 이벤트를 딥러닝 모델로 학습시켜 향후 발생할 이벤트 정보를 예측시키는 연구 결과가 발표되었다[1]. 흥미로운 부분은 침입방지시스템이 서로 다른 장소에 설치된 상황에서 수집된 모든 이벤트를 RNN으로 학습시켜 다음번 이벤트의 발생을 예측하도록 했는데, 논문 저자들은 설치 장소에 무관하게 비교적 정확한 예측이 가능하다고 주장한다.

2.3. 머신러닝과 딥러닝 비교

일반적으로 머신러닝은 데이터의 양이 한정되어 있을 때 잘 동작하고, 딥러닝은 데이터의 양이 많은 경우에 잘 동작하는 것으로 알려져 있다. 딥러닝을 머신러닝과 차별화시키는 부분은 많은 양의 데이터로부터 자동으로 유용한 피처를 추출할 수 있다는 점이다.

보안데이터 분석 분야에서 최근 발표되는 논문 중에는 딥러닝과 대량 데이터를 이용해서 E2E 학습에 성공했다는 주장도 있으나[5], 아직 철저한 검증이 끝난 것으로 보이지는 않는다. 보안데이터 분석에 딥러닝을 적용하려고 할 때 가장 까다로운 점 중 하나는 고정된 크기의 학습 입력 벡터를 생성하는 부분인데, 가공 전 보안데이터는 가변적 크기로 대부분 구성되기 때문에 입력 벡터 생성 과정에서 필연적으로 정보 손실이 발생한다. 이 부분에서 보안전문가들의 도메인 지식을 이용한 피처 가공 과정은 매우 유용하게 활용될 수 있다. 또 다른 측면으로는 임베딩 기술을 도입하여 정보 손실을 최소화하면서 딥러닝의 입력값을 생성하는 연구가 병행될 수 있다.

다음에 소개될 공개 보안데이터 중 데이터 분석 경진대회 데이터 셋은 한정된 개수의 데이터가 주어지고 데이터 내에 반복성이 일반적으로 강하기 때문에 머신러닝 계열의 학습모델이 높은 정확도를 달성하는데 유리하다. 특히 트리 모델 중 부스팅 기법들이 대회에서 우수한 성적을 내고 있다.

딥러닝 기술이 이미지나 자연어 처리 분야에서 보여주고 있는 탁월한 기술적 우위를 아직 보안데이터 분석 분야에서 보여주지는 못하고 있다. 하지만 기존 머신러닝 기반 기술의 한계를 극복하기 위해서는 대량의 데이터로부터 사람의 직관으로 찾지 못했던 피처들을 추출하는 것이 중요한 연구과제로 진행되어야 할 것이다. 머신러닝 기술과 딥러닝 기술의 상호 보완적 활용에 대한 본격적인 연구가 필요한 시점이다[15].

Ⅲ. 공개 보안데이터 종류와 특징

3.1. 악성코드 데이터 셋

공개된 악성코드 데이터 셋 중 가장 많이 참조되는 것 중 하나는 2015년에 마이크로소프트사가 개최한 캐

글 경진대회 데이터 셋이다[6]. 악성코드 20,000개 샘플로부터 디스어셈블(disassemble)된 코드와 바이트코드가 제공되며 총 0.5 테라바이트의 분량이다. 악성코드 샘플은 9개의 라벨 중 하나의 값을 갖는다. 주어진 악성코드 샘플에 대해서 다중클래스 분류를 하는 대회이다. 악성코드가 실제로 동작하는 것을 막기 위해서 헤더 정보는 삭제되어 있다.

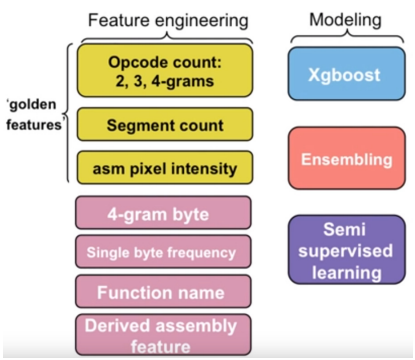
마이크로소프트 대회 우승은 보안 쪽 전문 지식이 없는 데이터분석가 팀이 99.83의 정확도를 달성하며 차지했다. [그림 4]와 같이 opcode n-그램과 세그먼트 개수, 그리고 어셈블리 코드를 이미지화한 후 화소 강도(pixel intensity)를 구하여 주요 피처로 사용했으며, 머신러닝 모델은 Xgboost를 세 개 사용한 후 앙상블을 적용했다. 흥미로운 사실은 이 대회의 상위 세 개 팀이 모두 Xgboost를 사용했다는 점이며, 한정된 데이터 셋과 시간 안에 높은 정확도를 높이는데 있어서는 Xgboost 모델이 가장 적합할 수 있다는 것이 입증된 사례이다.

실제로 다른 데이터 분석 대회에서도 부스팅 계열의 모델이 좋은 성적을 내고 있다. 랜덤 포레스트(random forest)가 약한 분류기를 많이 병렬적으로 사용하여 배깅(bagging) 방식으로 변수와 데이터를 샘플링하여 분산을 줄임으로써 정확도를 높인다면, 부스팅 계열(Xgboost, Lightgbm 등)은 약한 분류기를 많이 사용한다는 점은 동일하나 분류기들을 순서대로 적용하여 앞선 분류기가 틀리는 문제를 뒤쪽 분류기에서 더 집중하여 학습할 수 있도록 함으로써 보다 높은 정확도를 얻을 수 있다.

국내에서는 한국인터넷진흥원이 주최하는 정보보호 R&D 데이터 챌린지 대회가 2017년부터 개최되고 있다[8][9]. 보안데이터를 몇 개의 주제로 나누어 각 트랙별로 대회를 개최하는데, 그중 하나가 악성코드 탐지 트랙이다. 이 대회에서는 악성코드와 정상코드를 나누어 주고 이진 분류기 역할을 하는 머신러닝 모델을 학습시키게 한 후 테스트 데이터로 정확도를 계산하여 우승자를 가리게 된다. 2018년도 대회에서 우승자는 Xgboost 모델을 사용하였으며 정확도 96.83을 달성했다. 마이크로소프트 경진대회에서 배포한 데이터 셋의 악성코드는 헤더 정보가 없었지만, 데이터 챌린지 대회에서 배포한 데이터 셋은 모든 정보를 포함한다.

보안데이터 분석가들은 헤더 정보가 포함된 사실을 적극적으로 활용할 수 있다. 첫째, 헤더 정보는 좋은 피처들을 많이 포함하고 있으므로 이 부분을 머신러닝 모델에 잘 보여주면 정확도를 높이는데 큰 도움이 된다. [표 1]는 대회에서 배포한 데이터 셋을 이용해서 헤더 정보로부터 단지 7개의 피처만 뽑아와서 부스팅 알고리즘으로 학습을 시켰을 때 얻어지는 평가 지표이다. 7개라는 적은 개수와 최종 우승자의 정확도가 96.83임을 감안하면 정확도 89.92는 나쁘지 않은 수치이다. 실제로 여기에 몇 가지 헤더 정보 피처를 잘 가공해서 추가하면 94 정도의 정확도까지는 얻어진다.

최근 마이크로소프트는 캐글 사이트를 통해서 악성코드와 관련된 데이터분석 대회를 2019년도에 한 번 더 개최했다[7]. 2015년 대회와는 다르게 이번에는 PC가 앞으로 악성코드에 감염될지를 예측하는 대회였다. PC로부터 추출된 82개의 피처 정보와 악성코드 감염 여부가 라벨로 주어졌다. 피처 정보에는 윈도우 디펜더 버전, 기본 브라우저, 프로세서, 방화벽 설치 여부, 펌웨어 정보, OS 버전 등이 포함되어있다.



〔그림 4〕 마이크로소프트 악성코드 경진대회 우승팀 사용 피처와 모델〔17〕

〔표 1〕 7개 헤더 정보만으로 부스팅 알고리즘을 학습시켰을 때 얻어지는 지표(정보보호R&D데이터챌린지 2018)

지표 종류	값
Accuracy	0.8992
Precision	0.9271
Recall	0.9354

3.2. 보안관제 로그 데이터 셋

공개된 보안관제 로그 데이터 셋은 악성코드 데이터 셋에 비해서 상대적으로 많지 않다. 관제 데이터의 성격

상 수집되는 대상 기관의 정보가 로그 안에 포함되는 경우가 많기 때문이며, 악성코드처럼 불특정 다수가 공유하는 사이트도 거의 존재하지 않는다. 일부 사이트들이 보안데이터 분석 차원에서 네트워크 트래픽이나 침입탐지시스템 계열의 로그를 공개하고 있다.

KDD Cup 1999 데이터 셋은 이 분야에서 오래된 잘 알려진 데이터이다[18]. 접속 레코드 5백만 건이 학습 데이터를 구성하며, 2백만 건이 테스트 데이터를 형성한다. MIT Lincoln 연구소에서 미국 공군의 LAN을 시뮬레이션하기 위해서 데이터를 생성하였으며, 크게 4가지 범주의 공격(DoS, R2L, U2R, probing) 레코드들이 포함되어있다. Tavallaee 등은 일부 내용을 보완하여 NSL-KDD 데이터 셋을 공개하고 있으며[10], 참고로 해당 사이트에서는 다른 IPS/IDS 데이터셋, 봇넷 데이터 셋 등 다양한 보안데이터 셋을 오픈하고 있다[11].

Du 등은 딥러닝을 이용해서 시스템 로그를 분석하여 이상징후를 탐지하는 연구를 발표했다[3]. 제안하는 아이디어를 검증하기 위해서 다양한 데이터 셋을 사용하였는데, 그중 하나가 VAST challenge 2011 대회 문제에서 출제된 데이터 셋이었다[12]. 컴퓨터 네트워크 운영센터로부터 생성되는 로그로부터 시각화 기술을 이용해서 의심 행위를 찾아내는 것이 대회의 취지였는데, Du 등은 제안하는 로그 분석 시스템의 우수성을 증빙하기 위하여 동 데이터를 사용했다.

보안관제 로그를 대상으로 하는 데이터분석 대회도 악성코드 분석대회와 마찬가지로 학습 데이터와 테스트 데이터 간에 중복되거나 많이 유사한 형태의 로그들이 포함되어있으며, 머신러닝 알고리즘들이 이러한 패턴을 찾아서 학습하여 테스트 데이터의 라벨을 추측할 수 있다.

Ⅳ. 결 론

본 논문에서는 보안데이터 중 악성코드와 보안관제 로그 분석을 위하여 머신러닝과 딥러닝을 이용하는 최근 연구 동향과 국내외 주요 데이터 분석대회 동향을 소개했다. 보안데이터 분석은 학문적으로나 실용적으로 사이버보안에 있어서 중요한 영역이었으며, 인공지능 기술이 결합 되었을 때 가장 크게 발전할 수 있는 영역이기도 하다. 특히 최근 이미지와 자연어 처리 분야에서 혁신적 발전을 주도하고 있는 딥러닝 기술을 보안데이터 분야에 활용하기 위한 본격적인 연구가 필요하며, 전통적 머신러닝 기술과 딥러닝 기술이 상호 보완적 역할을 해줄 것으로 기대된다.

인공지능 기술이 발전하면 보안전문가의 업무 영역이나 일자리가 축소될지 모른다는 일부 우려의 시각이 있다. 하지만 인공지능 기술이 발전하더라도 여전히 보안전문가의 도메인 지식과 경험은 인공지능 기술 개발 과정에서 필수적이며, 완벽한 정확도가 달성되기 이전에는 보안전문가의 개입은 필연적이다. 특히, 현재 보안전문가의 시간을 대부분 차지하는 단순 반복적 업무를 많은 부분 인공지능 기술로 대체시키고, 보안전문가들은 창의력과 경험이 필요한 고도화된 사이버 공격에 대한 분석 업무에 치중하도록 하는 선순환 구조가 인공지능 기술에 의해서 가능해질 수 있을 것으로 기대된다.

참 고 문 헌

[1] Y. Shen, E. Mariconti, P. Vervier, and G.Stringhini, “Tiresias: Predicting Security Events Through Deep Learning,” Proceedings of ACM CCS’18

[2] Z. Cui, F. Xue, Y. Cao, and G. Wanf, “Detection of Malicious Code Variants Based on Deep Learning”, IEEE Trans. on Industrial Informatics, Vol.14, No.7, 2018

[3] M. Du, F. Li, G. Zheng, V. Srikumar, “DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning,” Proceedings of ACM CCS’17

[4] Z. Li, D. Zou, S. Xu, X. Ou, H. Jin, S. Wang, Z. Deng, and Y. Zhong, “VulDeePecker: A Deep Learning-Based System for Vulnerability Detection,” NDSS’18

[5] E. Raff, J. Barker, J. Sylvester, R. Brandon, B. Catanzaro, and C. Nicholas, “Malwrae Detection by Eating a whole EXE,” AAAI Workshop on Artificial Intelligence for Cyber Security, 2018

[6] R. Ronen, M. Radu, C. Feuerstein, E. Yom-Tov, and M. Ahmadi, “Microsoft Malware Classification Challenge,” https://arxiv.org/abs/1802.10135

[7] Microsoft Malware Prediction, 2019,

https://www.kaggle.com/c/microsoft-malware-prediction
[8] http://datachallenge.kr/
[9] http://ocslab.hksecurity.net/Datasets
[10] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” Proceedings of the IEEE CSIDA’09
[11] Canadian Institute for Cybersecurity, https://www.unb.ca/cic/datasets/index.html
[12] 2011-2013 VAST Cyber Challenge: Computer Network Operations at All Freight Corporation, http://www.vacommunity.org/2011+-+2013+VAST+Cyber+Challenges
[13] E. Rezende, G. Ruppert, T. Carvalho, F. Ramos and P. Geus, “Malicious Software Classification Using Transfer Learning of ResNet-50 Deep Neural Network,” in Proceedings of the IEEE ICMLA’17
[14] X. Ugarte-pedrero, M. Graziano, and D. Balzarotti, “A Close Look at a Daily Dataset of Malware Samples,” ACM Transactions on Privacy and Security, Vol. 22, Jan., 2019
[15] Kaspersky, “Machine Learning for Malware Detection,” 2017
[16] S. Khatuya, N. Ganguly, J. Basak, M. Bharde, and B. Mitra, “ADELE: Anomaly Detection from Event Log Empiricism,” Proceedings of IEEE INFOCOM'18
[17] Microsoft Malware Winners’ Interview, http://blog.kaggle.com/2015/05/26/microsoft-malware-winners-interview-1st-place-no-to-overfitting/
[18] KDD Cup 1999: Computer network intrusion detection, https://www.kdd.org/kdd-cup/view/kdd-cup-1999/Data

〈저자소개〉

이 식 (Lee, Seek)
2018년 2월 : 국민대학교 컴퓨터공학부 학사
2018년 3월～현재 : 국민대학교 컴퓨터공학부 석사과정
<관심분야> 정보보호, 기계학습

김 동 훈 (Kim, DongHoon)
2018년 2월 : 국민대학교 컴퓨터공학부 학사
2018년 3월～현재 : 국민대학교 컴퓨터공학부 석사과정
<관심분야> 정보보호, 빅데이터, 인공지능

조 영 훈 (Cho, YoungHun)
2017년 8월 : 국민대학교 컴퓨터공학과 학사
2017년 8월～현재 : 국민대학교 컴퓨터공학과 석사과정
<관심분야> 정보보호, 기계학습, 랜섬웨어 탐지

명 준 우 (Myung, JoonWoo)
2019년 2월 : 국민대학교 컴퓨터공학부 학사
2019년 3월～현재 : 국민대학교 컴퓨터공학부 석사과정
<관심분야> 정보보호, 기계학습, 보안관제

문 다 민 (Moon, DaMin)

2016년 3월~현재 : 국민대학교 컴퓨터공학부 학사과정
<관심분야> 정보보호, 기계학습, 데이터마이닝

이 재 구 (Lee, JaeKoo)

2011년 5월 : UC SanDiego 전기컴퓨터공학부 석사
2018년 2월 : 서울대학교 전기컴퓨터공학부 박사
2018년 9월~현재 : 국민대학교 소프트웨어학부 조교수
<관심분야> 인공지능, 자율주행, 정보보호

윤 명 근 (Yoon, MyungKeun)

종신회원
1996년 2월 : 연세대학교 컴퓨터 과학과 학사
1998년 2월 : 연세대학교 컴퓨터 공학과 석사
2008년 12월 : University of Florida, 컴퓨터공학 박사
1998년 1월~2010년 2월 : 금융결제원 과장
2010년 3월~현재 : 국민대학교 컴퓨터공학과 부교수
<관심분야> 보안 빅데이터 분석, 지능형 보안, 컴퓨터&네트워크 보안, 금융 보안