TF-IDF 기법을 활용한 TTP 임베딩 및 사이버 캠페인 분석
cyber campaign analysis with TTP embedding using TF-IDF

신성욱* · 이인섭* · 신찬호* · 서성연* · 최창희*
Sunguk Shin* · Insup Lee* · Chanho Shin* · Seongyun Seo* · Changhee Choi*

* 국방과학연구소
(ssw1419@add.re.kr)

ABSTRACT

As cyber attack develop in recent years, it is expanding to APT attack by group rather than individual. Research is being conducted to analyze cyber attacks, and MITRE ATT&CK has proposed the concept of TTP to analyze cyber attacks. The attack technique amng TTP has a description and the description can be embedded using the TF-IDF. To analyze the cyber campaign, we use a tool that automatically labels techniques to label the published reports and add group labels. In this paper, we analyze cyber campaigns and visualize using embedded techniques through TF-IDF using labeled data.

Key Words : Key Words : TF-IDF, TTP, cyber security, MITRE ATT&CK

1. 서론

사이버 공격이 고도화됨에 따라 하나의 목적을 가진 공격이 아닌 최종 목적을 달성하기 위해 여러 개의 중간 목표를 가지며 각 목표를 달성하기 위해 다양한 기술을 사용하는 킬체인 형태의 공격으로 발전하였다.

사이버 공격을 탐지하기 위해선 사이버 공격을 할 때 수행되는 기술에 대해 분석하고 그 기술들이 모여서 수행할 수 있는 목적을 알아내야할 필요가 있다. 사이버 캠페인을 수행하는 다양한 그룹이 존재하며 각 그룹은 특정한 목적을 가지고 캠페인을 수행하게 된다.

최근 이러한 사이버 공격에 대해 MITRE ATT&CK를 활용하여 공격 그룹[1], 국가[2], 최종 목표[3]를 예측하는 연구가 진행되고 있다.

본 논문에서는 사이버 공격의 형태인 캠페인을 분석하기 위해서 공격 캠페인에 사용된 technique을 분석하여 임베딩을 수행한 뒤, 임베딩 technique을 하나로 합쳐 캠페인을 임베딩하는 과정을 수행하였다. 캠페인을 임베딩 결과를 확인하기 위해서 널리 알려진 공격 캠페인 그룹을 라벨링하여 그룹간 연관성에 대해 확인하였다.

2. background

2.1 MITRE ATT&CK[4]

MITRE ATT&CK는 실제로 발생한 사이버 공격을 관찰하고 tactic 및 technique에 대해 정리한 프레임워크이다. 각 tactic은 해당 tactic을 달성하기 위한 technique이 존재하며 하나의 technique은 여러 개의 tactic을 가지고 있을 수 있다.

MITRE ATT&CK는 enterprise와 mobile이 존재하며 버전 11까지 등장하였으나 본 논문에서는 버전 10의 enterprise에 대해서만 실험을 수행하였다. 버전 10의 enterprise에는 14개의 tactic과 188개의 technique과 379개의 sub-technique이 존재한다.

2.2 TF-IDF

TF-IDF(Term Frequency-Inverse Document Frequency)는 문서의 단어 빈도와 문서 빈도의 역을 사용하여 단어 및 문서의 벡터를 만드는 방법이다. MITRE ATT&CK는 모든 technique마다 해당 기술이 어떤 기술인지 설명하는 설명문이 존재하며 같은 tactic에 속하는 경우 비슷한 목적을 갖기 때문에 특정 동일한 단어를 사용하게 된다. 이러한 특성으로 인해 본 논문에서는 TF-IDF를 사용하여 technique 임베딩을 수행하였다.

2.3 T-SNE

T-SNE는 t 분포를 사용한 Stochastic Neighbor Embedding으로 feature extract 방법이다. 두 개의 노드 사이 거리 가중치를 계산하여 거리합이 최소가 되는 함수를 찾는다. T-SNE를 적용하기 위해서 python의 sklearn에 있는 TSNE 함수를 사용하여 임베딩된 캠페인에 대해 시각화를 진행하였다.

2.4 GCN을 적용한 TTP 사이버 데이터 기반 국가 예측 방안

[2]는 사이버 국가 예측을 위한 연구로 2개의 국가를 GCN 모델을 활용하여 분류하였다. 분류국가가 2개였으며 학습 데이터 및 테스트 데이터 개수가 46개, 19개라는 제한이 존재하였다. 이러한 제한점을 보완하여 본 논문에서는 4개의 국가에 대해선 130개의 데이터를

활용하였으며 9개의 그룹에 대해 81개의 데이터를 활용하여 시각화를 수행하였다.

3. 제안하는 방법

3.1 데이터셋

공격 그룹 및 공격 technique 라벨링을 위해서 github에 공개된 cyberMonitor의 APT 공격 분석 보고서[5]를 사용하였다. 공개된 보고서에서 technique 라벨링을 하기 위해서 rcATT[6]라는 도구를 활용하였으며 보고서에 등장한 group을 통해 group 라벨링을 수행하였다. 그룹 라벨링을 진행한 후, 국가 라벨링을 위해서 ThaiCERT와 Malpedia에서 제공하는 그룹과 국가 정보를 활용하여 라벨링을 수행하였다.

3.2 technique 및 캠페인 임베딩 방법

MITRE에서 제공하는 technique에 대한 설명문을 모두 수집한 뒤 TF-IDF를 활용하여 임베딩을 수행한 것을 technique에 대한 벡터로 정의하였다. 이후 3.1에서 수행한 캠페인에 대한 technique 라벨링 정보를 가지고 technique 임베딩 벡터에 technique이 존재할 경우 1, 존재하지 않을 경우 0을 곱하여 모두 더하여 계산하였다. 해당 실험에서 sub-technique 정보는 활용하지 않았다.

4. 실험 결과

실험을 통해 캠페인 임베딩을 수행하였으며 국가와 그룹에 대해 라벨링을 수행한 결과를 가지고 T_SNE 시각화를 수행하였다. 그림 1은 그룹에 대한 시각화 결과이며 그림 2는 국가에 대한 시각화 결과이다.

그림 1의 결과를 보면 왼쪽 아래의 Turla, 중앙 아래의 Threat-group-3390, 왼쪽 위의 MuddyWater 등 일부 그룹이 뭉쳐있는 것을 확인할 수 있다. 그림 2의 결과는 모든 점들이 큰 경향성 없이 골고루 분포되어있는 것을 확인할 수 있다.

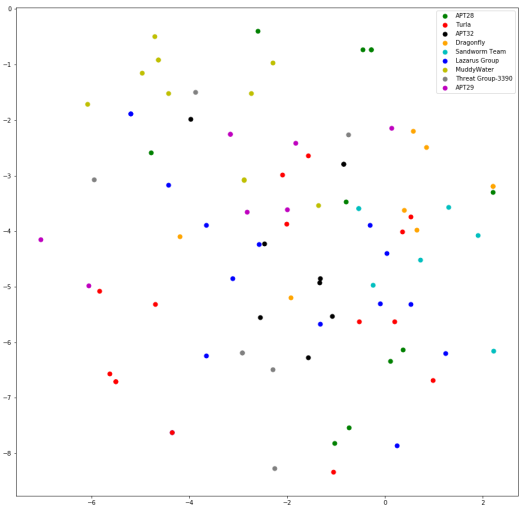

Fig. 1. group에 대한 캠페인 임베딩 결과

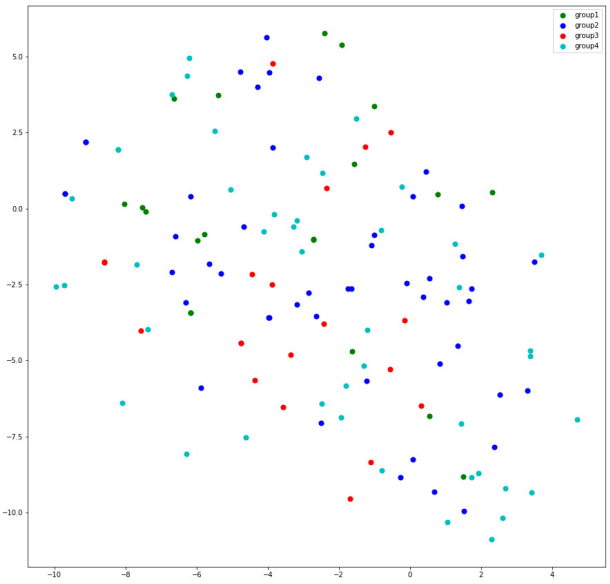

Fig. 2. 국가에 대한 캠페인 임베딩 결과

5. 결론

사이버 캠페인 분석을 위해 MITRE ATT&CK에서 제공하는 technique에 대한 임베딩을 수행하였으며 이를 활용하여 캠페인에 대한 임베딩을 수행하였다. 수행한 결과 비슷한 목적을 갖는 그룹에 대해서는 TF-IDF 방법을 통한 임베딩이 효과적이었으나 여러 목적을 갖는 국가에 대해서는 임베딩이 효과적이지 못했음을 확인할 수 있었다.

추후 임베딩을 수행한 뒤, 비지도 학습을 통해 분류를 수행하고 같은 라벨로 묶이는 데이터들에 대한 연관관계를 분석하는 등의 연구를 진행할 수 있을 것이다.

References

[1] 최창희, 신찬호, 신성욱, 서성연, 이인섭, “사이버 공격 행위 예측을 위한 딥러닝 학습 방법”, 한국군사과학기술학회 종합학술대회, 2021.

[2] 신성욱, “GCN을 적용한 TTP 사이버 데이터 기반 국가 예측 방안”, 한국군사과학기술학회 종합학술대회, 2021.

[3] 신찬호

[4] MITRE ATT&CK, https://attack.mitre.org/, (accessed May, 2, 2022)

[5] APT & Cybercriminals Campaign Collection, https://github.com/CyberMonitor/APT_CyberCriminal_Campaign_Collections

[6] rcATT, https://github.com/vlegoy/rcATT

[7] ThaiCERT, https://www.thaicert.or.th

[8] Malpedia, https://malpedia.caad.fkie.fraunhofer.de