TTP 단어 치환을 활용한 사이버 캠페인 변형 기법
Mutating Cyber Campaign With TTP Word Replacement

이인섭* · 신찬호* · 최창희*
Insup Lee* · Chanho Shin* · Changhee Choi*

* 국방과학연구소
(dlstjq0711@add.re.kr)

ABSTRACT

Cyber Threat Intelligence (CTI) has received significant attention to cope with cyber attacks, especially large-scale cyber campaigns. Although there have been studies to adopt deep learning to CTI, the lack of campaign data has become a critical bottleneck. To address the data shortage issue, we propose a campaign variants generation method using synonym replacement in the natural language processing domain. Visualized results show that the proposed campaign augmentation produces reasonable data.

Key Words : Cyber campaign, cyber threat intelligence, data augmentation, NLP, ATT&CK

1. 서론

정보통신의 발달은 생활에 많은 편의를 가져왔으나 공격 표면이 증대되고 사이버 공격 위협 역시 증대되었다. 최근 들어 공격이 고도화되고 공격 방식이 대규모로 확대됨에 따라 이를 사이버 킬체인 (cyber kill chain)으로 모델링 하여 대응하는 시도들이 나타나고 있다. 대표적인 예시인 MITRE에서 제공하는 ATT&CK ®[1]은 차세대 사이버 위협 인텔리전스 (CTI)의 핵심 요소로써 주목받고 있다.

인공지능 기술이 발전함에 따라 ATT&CK 기반의 CTI 연구에 머신러닝과 딥러닝을 활용한 연구들이 많이 수행되고 있다[2]. 효과적으로 딥러닝 모델을 학습하기 위해선 양질의 학습데이터를 충분히 마련하는 것이 가장 중요한 문제인데, 발생 빈도가 높지 않은 사이버 캠페인 데이터 특성상 캠페인 데이터를 확보하는 것이 제한되는 상황이다. 본 논문에서는 자연어처리 분야의 텍스트 증강 기법인 유어의 치환 기반의 변종 사이버 캠페인 데이터 증진 기법을 제안한다.

2. 사이버 캠페인 데이터

본 장에서는 MITRE ATT&CK 프레임워크와 데이터 전처리과정을 서술한다.

2.1 MITRE ATT&CK 프레임워크

MITRE에서 제공하는 ATT&CK 프레임워크는 정의된 Tactics 및 Techniques를 활용하여 사이버 킬체인의 각 단계를 정의한 매트릭스이다. 사이버 캠페인을 분석하는 과정에서 Tactics, Techniques, Procedures (TTP)를 구조화 및 패턴화한다.

2.2 캠페인 데이터 전처리

본 논문에서는 캠페인 데이터를 '해당 캠페인을 분석한 리포트에 태깅된 TTP 시퀀스'로 정의한다. APT & Criminals Campaign Collection [3]에서 제공한 858개의 리포트에 대해 보안 전문가들이 TTP 라벨 태깅 작업을 수행하며, TTP 중 Technique 정보만을 실험에서 사용한다. 전처리 완료된 TTP 시퀀스는 표 1과 같다. 시퀀스 길이가 너무 짧은 경우 캠페인의 패턴이 누락 될 수 있으므로 TTP 시퀀스 길이가 최소 5 이상인 634개의 캠페인 데이터를 활용한다.

Table 1. 전처리 된 TTP 시퀀스

Cyber Campaign	TTP Sequence
11	T1066 → T1064 → T1027
35	T1066 → T1108 → T1045 → T1110
335	T0002 → T0003 → T0004 → T0005 → T1053 → T1106 → T1117 → T1059 → T1015 → T1034

3. TTP 유의어 치환 기반 캠페인 증진 기법

캠페인 데이터 부족 문제를 해결하기 위해, 본 논문에서는 자연어처리 분야의 대표적인 텍스트 데이터 증강 연구인 Easy Data Augmentation (EDA) [4] 기반의 캠페인 증진 기법을 제안한다. EDA의 세부 기술 4가지인 유의어 치환 (synonym replacement), 임의 삽입 (random insertion), 임의 제거 (random deletion), 임의 치환 (random swap) 중 유의어 치환 기법을 통해 데이터를 증강하며 캠페인 증진을 위한 4단계 절차는 다음과 같다.

(1) 공격 그룹 선정: 어떤 공격 그룹이 수행한 캠페인 데이터를 증진할 것인지 결정하는 과정에서, 본 논문은 대표적인 공격 그룹인 Lazarus와 menuPass 그룹을 선정한다. 두 그룹은 널리 알려진 그룹이며 여러 APT 공격과 캠페인을 수행한 바 있다.

(2) 그룹 대표 캠페인 선정: 선정된 그룹의 어떤 캠페인을 중심으로 변형 및 증진할 것인지 결정하는 과정에

서, 본 논문은 TTP 시퀀스 길이를 측정하여 길이가 긴 캠페인을 해당 그룹의 대표 캠페인으로 선정한다.

(3) 변형 대상 TTP 결정: 본 논문에서는 TF-IDF 정보량이 가장 낮은 TTP를 변형 대상 TTP로 결정한다. TTP 변형 수준도 중요한 문제인데, 그룹 대표 캠페인인 TTP 시퀀스의 너무 많은 부분을 변형할 시 공격 그룹의 패턴이 누락 될 수 있고 너무 적게 변형할 시 생성 캠페인이 원본 캠페인과 거의 동일해지므로 적절한 변형 수준을 고려한다.

(4) TTP 유의어 치환: 본 논문에서는 유사한 TTP를 '같은 Tactic 내의 다른 Technique'으로 정의한다. 변형 대상으로 선정된 TTP는 유사한 TTP 중 임의의 TTP로 치환되어 캠페인 증진을 수행한다. 캠페인 증진 전후의 TTP 시퀀스 예시는 표2와 같다. 'T1566 T1136 T1037 T1110 T1485'로 구성된 길이 5의 원본 TTP 시퀀스에 대해, T1136 (Persistence의 Create Account)을 T1556 (Persistence의 Modify Authentication Process)로 변형하여 증진한다.

Table 2. TTP 유의어 치환 기반 캠페인 데이터 증진

Cyber Campaign	TTP Sequence
Original Campaign	T1566→ T1136→ T1037→ T1110→ T1485
Generated Campaign	T1566→ **T1556**→ T1037→ T1110→ T1485

4. 캠페인 임베딩 및 시각화

증진된 캠페인의 타당성을 확인하기 위해 캠페인 데이터 임베딩 및 시각화 과정을 수행한다. 본 논문에서는 TF-IDF 알고리즘을 사용하여 캠페인 임베딩을 수행한 후 임베딩 된 캠페인 벡터에 대해 2차원 평면으로 t-SNE 시각화한다. TF-IDF를 통해 캠페인과 테크닉의 관계를 문서와 단어의 관계로 해석 가능하며, t-SNE를 통해 2차원 벡터공간으로 차원 축소한다.

본 논문에서는 그룹 대표 캠페인의 비율은 0.2로 설정하여 Lazarus의 38개 캠페인 중 7개 캠페인을, menuPass의 13개 캠페인 중 3개 캠페인을 그룹 대표 캠페인으로 선정하고 대표 캠페인 별 7개 캠페인을 증진한다. 변형 대상 TTP 비율은 0.3으로 설정한다.

캠페인 증진 전 t-SNE 시각화 결과는 그림 1과 같다. 캠페인 수가 부족할 뿐 아니라, 공격 기법과 전략이 고도화됨에 따라 공격 그룹의 패턴이 잘 드러나지 않아 캠페인 벡터들의 분포가 산재 된 것을 확인할 수 있다. 다음으로 캠페인 증진 후 t-SNE 시각화 결과는 그림 2와 같다. Lazarus와 menuPass에 대해 캠페인 증진을 수행한 결과, 증진 전에 비해 공격 그룹 간 구분되는 정도가 개선되는 것을 확인할 수 있다.

5. 결론

본 연구에서는 자연어처리 분야의 텍스트 증진 방법인 유의어 치환 기법을 활용해 사이버 캠페인 증진 기법을 제안했다. 시각화 결과는 제안된 증진 기법을 통해 캠페인 데이터 부족 문제를 해결하여 공격 그룹 분류 성능을 개선 가능성을 보여준다.

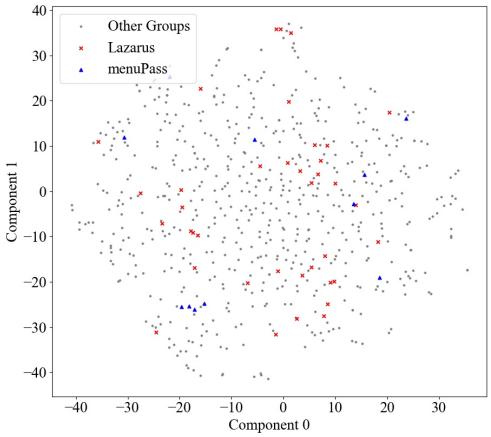

Fig. 1. 캠페인 증진 전 t-SNE 기반의 캠페인 벡터 시각화.

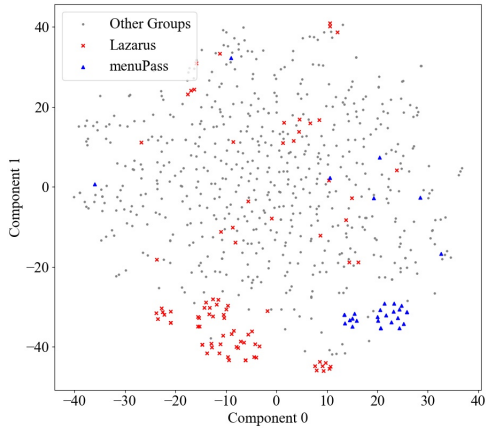

Fig. 2. 캠페인 증진 후 t-SNE 기반의 캠페인 벡터 시각화.

References

[1] MITRE ATT&CK, https://attack.mitre.org

[2] C. Xiong, T. Zhu, W. Dong, L. Ruan, R. Yang, Y. Cheng, Y. Chen, S. Cheng, and X. Chen, "CONAN: A Practical Real-Time APT Detection System With High Accuracy and Efficiency," *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 1, pp. 551-565, 2022.

[3] APT&CyberCriminal Campaign Collections, https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections.

[4] J. Wei and K. Zou, "EDA: Easy Data Augmentation Techniques for Boosting Performance on Text Classification Tasks," in *Proc. of ACM EMNLP*, 2019.