Journal of KIIT. Vol. 18, No. 10, pp. 55-67, Oct. 31, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.10.55

네트워크 관점에서의 공격자 행위 매트릭스에 기반한 공격자 전술 및 기술 탐지 방안

전덕조*, 박동규**

Attacker Tactics and Technology Detection Method based on Attackers' Behavior Matrix from a Network Perspective

Deok-Jo Jeon*, Dong-Gue Park**

이 논문은 순천향대학교 연구비에 의하여 연구하였음.

요 약

최근 사이버공간의 복잡성과 초연결성 등으로 인해 해커들의 공격 기법은 매우 정교화·다양화하고 있으나, 기업의 보안 관리 수준과 대응 체계는 이를 따라가지 못하고 있다. 따라서 기업들은 최초 침투 행위 방어 이외에도 해커의 공격이 계속되는 과정에서 위협을 적기에 식별하고 대응할 수 있는 능동적 위협 관리체계로 개선하는 것이 필요하다. 위협 헌팅은 공격자가 데이터 파괴나 유출과 같은 목표를 완수하기 전에 실시간으로 공격을 식별하고 완화할 수 있는 사전 예방적 접근법을 제공한다. 본 논문에서는 위협 헌팅에 지표가 되고 있는 MITRE의 ATT&CK 매트릭스를 기반으로 새롭게 네트워크 관점에서의 공격자 행위에 대한 기술 매트릭스를 제안하고 실제 발생한 지능형 위협 헌팅에 적용함으로써 그 효과를 검증하고자 한다. 즉, 대한민국에 대한 실제 공격 사례인 이란 스파이 그룹과 라자루스 그룹이 사용한 네트워크 기반 공격 기술을 본 논문이 제시한 매트릭스로 검출되는 지를 제시한다.

Abstract

The hackers' attack techniques have recently become very sophisticated and diverse due to the complexity and hyper-connectivity of cyberspace, but current corporate security management levels and response systems have not been able to keep up with them, Therefore, companies are advised not only to defend their initial infiltration behavior, but also to improve the threat management system to be able to identify and respond to threats in a timely manner in the course of continued hacker attacks. The practice of threat hunting provides a proactive and iterative approach to identify and mitigate attacks in real-time before the attackers complete their objective such as data destruction or exfiltration. In this paper, we present a network-based threat hunting technique matrix inspired by the MITRE ATT&CK and verify its effectiveness by applying it to real-life advanced persistent threats (APTs). In other words, we present how the network-based attack techniques used by the Iranian spy group and the Lazarus group, examples of Korea attacks, are detected in the matrix proposed in this paper.

Keywords

malware detection, data mining, machine learning, decision tree, ransomware detection

* ㈜ 시큐비스타 대표이사
- ORCID: http://orcid.org/0000-0002-0343-3384
** 순천향대학교 정보통신공학과 교수(교신저자)
- ORCID: http://orcid.org/0000-0002-5864-8825

· Received: Aug. 11, 2020, Revised: Oct. 13, 2020, Accepted: Oct. 16, 2020
· Corresponding Author: Dong-Gue Park
Dept. of Information and Communication Engineering Soonchunhyang Univ.
Tel.: +82-41-530-1347, Email: dgpark@sch.ac.kr.

Ⅰ. 서 론

지능형 지속 가능 위협(APT, Advanced Persistent Threats)는 IT환경에서 지속적으로 증가하고 있다. APT는 지적 재산 탈취[1][2], 개인 정보 탈취[2] 그리고 금전적인 동기[3]를 가진 공격자에 의해 이루어지고 있다. 현재의 보안 관리 방법은 보안 통제 수단을 설정하고 경보가 트리거 될 때까지 기다리는 방식을 채택하고 있으므로, APT 공격의 탐지 및 대응관점에서는 유효하지 않은 방법이다. 따라서 보안 방어자 관점에서 지능형 공격자를 찾아내기 위해서는 보다 능동적인 접근방법이 필요하며 이러한 방법이 바로 위협 헌팅(Threat hunting) [4]이다. 위키피디아(Wikipedia)의 정의에 따르면, 위협 헌팅은 적극적인 사이버 방어 활동으로서, "기존 보안 솔루션을 회피하는 지능형 위협을 탐지하고 격리하기 위해 네트워크를 능동적이고 반복적으로 검색하는 프로세스"로 정의하고 있다. 이는 기존의 방화벽, 침입 탐지 시스템(IDS), 맬웨어 샌드 박스 및 SIEM 시스템과 같이 잠재적인 위협에 대한 경고가 발생한 이후에 증거 데이터를 조사하는 수동적인 형태의 위협 관리 조치와는 대조적이다. 위협 헌팅은 보안 분석가가 네트워크상에서 기존 보안 통제 수단이 탐지하지 못한 APT의 존재 유무를 탐색하는 것을 의미한다. 위협 헌팅의 궁극적인 목표는 공격자가 탐지되지 않은 채로 네트워크에 머무르는 체류 시간(Dwell time)을 최소화하는 것이다[5].

이러한 위협 헌팅의 첫 번째 단계는 분석가가 자신의 환경에서 악의적인 활동의 존재 유무를 확인할 수 있는 가설을 생성하는 것이다. MITER ATT & CK 매트릭스[6]는 알려진 APT 전술 및 기술(Tactics & techniques) 목록을 제공하므로 폭넓은 가설 생성을 용이하게 할 수 있다. 하지만 MITER ATT & CK 매트릭스는 엔드포인트 위협 탐지를 목표로 하고 있다. 즉, 윈도우, 리눅스 및 맥 OS 관점에서의 위협 탐지를 목표로 하고 있다. 따라서 현재 MITER ATT & CK 매트릭스는 호스트 기반 기술만 포함하고 있으며 네트워크 기반 기술을 포함하지 않고 있다.

본 논문에서는 네트워크 관점에서 위협 헌팅에 사용할 수 있는 APT 기술을 설명하기 위해 MITER ATT & CK 스타일과 유사한 매트릭스를 생성하여 제시하고자 한다. 효과적인 위협 헌팅을 위해서 보안 분석가는 네트워크 및 호스트 기반 기술을 모두 찾아내야 하는데, 현재 MITER ATT & CK 매트릭스만으로는 이러한 목표를 달성할 수 없기 때문이다. 보안 분석가는 본 논문에서 제시하는 네트워크 관점의 공격자 행위 매트릭스를 이용하여 네트워크 관점에서도 공격자 체류 시간을 줄이는 데 활용할 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 설명하고, 3장에서는 네트워크 관점의 공격자 행위 매트릭스 구축 방법을 제시한다. 4장에서는 두 가지 실제 APT 공격 사례를 이용하여 네트워크 관점의 공격자 행위 매트릭스의 효용성을 검증하고, 5장에서 결론을 짓는다.

Ⅱ. 관련 연구

2.1 위협 헌팅(Threat Hunting)

위협 헌팅에 대해 이해하기 위해서는 먼저 APT 절차를 이해하여야 한다. APT절차를 설명하기 위해 자주 이용되는 두 가지 모델이 존재한다. 이 두 가지 모델은 록히드 마틴 사이버 킬 체인(Lockheed Martin cyber kill chain)[7][8]과 맨디언트 공격 수명 주기(Mandiant attack lifecycle)[9]이다.

공개적으로 알려진 최초의 공격 모델은 록히드 마틴이 개발한 사이버 킬 체인 모델로 공격자가 목표 달성을 위해 완료해야 하는 활동에 대해 설명하고 있다[7][9]. 이 모델에서 공격 단계는 정찰, 무기화, 전송, 취약점 공격, 설치, 명령 및 제어(C2) 및 목표 행위의 7단계로 구성된다. 이 모델은 공격자 관점에서 만들어졌지만 방어자를 위한 것이다. 즉, 방어자가 어떤 단계에서든 공격을 방어하면 공격 사슬이 끊어지는 반면, 공격자는 성공적인 공격을 위해서 모든 단계를 완전히 거쳐야 한다. 이 모델에는 두 가지 문제점이 존재한다. 첫째, 방어자가 탐지 할 수 없는 공격 프로세스 단계가 포함되어 있으므로 방어자에게 적합하지 않다. 둘째, 록히드 마틴 사이버 킬 체인 모델은 선형적으로 공격 과정을

표현하고 있으므로 실제 공격자의 행동을 정확하게 표현하지 못하고 있다[7].

이러한 결함 때문에 맨디언트는 새로운 공격 수명주기를 만들었다[9]. 맨디언트의 공격 수명주기 모델은 공격자와 방어자에게 APT의 동작을 설명할 때 이용할 수 있는 공격 모델을 제공한다. 이 모델은 록히드 마틴 사이버 킬 체인 모델에서 방어자가 탐지 할 수 없는 “무기화” 단계를 제거함으로써 공격 수명 주기의 모든 단계가 방어자에 의해 탐지 될 수 있다. 이 모델은 주기(사이클)를 추가함으로써 공격이 항상 선형적으로만 진행이 되지 않을 수도 있는 점을 반영하고 있다. 그러나 맨디언트의 공격 수명주기 모델에는 네트워크에서 관찰 할 수 없는 단계가 포함되어 있다. 따라서 맨디언트의 공격 수명주기 모델도 네트워크 관점에서의 공격자 행위 분석에 대한 요구사항을 모두 충족시킬 수 없는 공격 모델이다.

그림 1의 브라이언트 킬 체인 모델(Bryant kill chain model)은 이전 두 가지 공격 모델에 대한 개선안이다 [10]. 이 모델은 록히드 마틴의 사이버 킬 체인과 맨디언트 공격 수명주기 모델 보다 개선된 방안이며, 네트워크 포렌식에 중점을 두고 있다. 브라이언트 킬 체인 모델은 앞에서 설명한 두 가지 공격 모델들의 문제점을 해결하는 동시에 네트워크 관점에서의 공격자 행위에 대한 단계를 제공한다.

하지만 브라이언트 킬 체인 모델에서도 권한 상승 단계는 네트워크 관점에서는 확인할 수 없는 단계이므로, 본 논문에서는 권한 상승 단계를 제외한 모든 브라이언트 킬 체인의 공격 단계를 사용한다. 또 “데이터 유출”은 목표에 대한 행위의 일부로서 발생할 수 있으므로 두 가지를 동일한 것으로 간주하여 사용한다.

APT와 같은 지능형 위협 헌팅은 "위협에 대한 사전 지식 없이 기업 네트워크 내에서 악의적인 활동의 징후를 적극적으로 찾는 프로세스”로 정의할 수 있다.

위협 헌팅의 일반적인 절차는 아래와 같은 6단계를 수행하는 것이다[1]:

1. 가설 설정
2. 가설을 증명할 증거 식별 - 식별이 안 되는 경우, 1로 복귀
3. 분석 개발
4. 자동화
5. 문서화
6. 의사소통 및 보고

위협 헌팅 절차의 첫 번째 단계는 보안 분석가가 입증하거나 반증 할 수 있는 가설을 생성하는 것이다[1]. 결론 도출이 가능하며, 범위가 정해져 있는 명확한 가설을 생성할 때, 일반적으로 선호되는 방법은 MITER ATT & CK 매트릭스를 활용하는 것이다[1]. MITER ATT & CK 매트릭스에는 APT 그룹에 대한 연구에서 도출된 열(컬럼) 제목이 존재한다. 예를 들어 "내부망 이동(Lateral movement)" 열(컬럼)에는 공격자가 내부 망을 이동하는 데 사용되는 기술이 포함되어 있다. "내부망 이동" 찾고자 한다면, 해당 열(컬럼)에서 하나의 기술을 선택하여 가설을 생성 할 것이다. 예를 들어 “공격자들이 내부망 이동을 위해 SMB를 활용하고 있다”고 설정하면, 하위 가설의 예는 "공격자가 PsExec을 활용하여 네트워크 환경에서 SMB 기반 내부망 이동을 수행하고 있다."이다. 그 다음에는 해당 가설을 입증하거나 반증하기 위해 네트워크 환경에서 관련 정보를 수집한다. 적절한 데이터를 수집 한 후, 분석해야 할 데이터 볼륨을 줄이기 위해서 PsExec을 사용하여 시스템을 원격으로 관리하는 IT 서버 정보를 제외 할 수 있다.

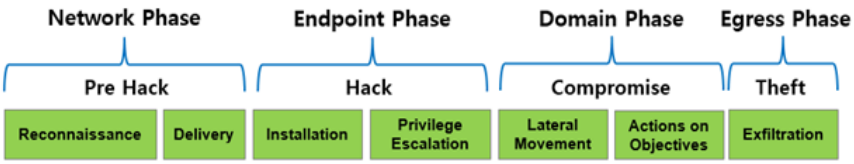

그림 1. 브라이언트 킬 체인 모델
Fig. 1. Bryant kill chain model

축소된 데이터 세트가 구성되면 데이터 수집 및 축소 프로세스를 자동화해야 한다. 자동화 후에는 해당 과정을 문서화하여 위협 헌팅을 재현 할 수 있도록 하고 데이터 축소에 대한 결정 기준과 결과를 해석하는 방법을 제공해야한다.

또 헌팅 결과는 소통 및 보고가 이루어져야 한다. 악의적인 활동을 발견하지 못했다고 해서 위협 헌팅이 실패한 것은 아니다. 그 이유는 악의적인 활동을 관찰할 수 없는 경우, 보안 통제가 의도한대로 동작하고 있다는 의미이기 때문이다.

2.2 MITER ATT & CK 매트릭스

MITER ATT & CK 매트릭스의 창시자인 Blake Storm은 많은 기업들이 보안 침해 지표(IOC, Indicator Of Compromise)에 의존하고 있다고 얘기하고 있다. IOC는 일반적으로 IP 주소, 파일 해시, 도메인 이름, 레지스트리 값 및 맬웨어 내의 고유 문자열이다. IOC는 임시적인 것으로서 단기간 동안에만 유효하다. 또 위협 행위자는 특정 조직을 공격하기 위해 한 세트의 IOC를 사용하지만 다른 조직을 공격하기 위해 완전히 다른 IOC세트를 사용한다. MITER는 이러한 문제점을 인식하고 알려진 APT에 대한 모든 공개 보고서를 수집 및 분석하여 각 APT에서 사용하는 기술을 추출하였다. 이후 MITER는 내부 레드 팀(모의 해킹 팀)의 지식을 바탕으로 알려진 기술 목록을 작성하였고 알려진 위협 행위자에 대한 공개 보고서, 맬웨어에 대한 공개 보고서 및 위협 인텔리전스를 작성된 기술 목록과 상호 참조하였다. 그 결과, 일련의 기술들이 그룹을 형성한다는 것이 드러났으며, 이러한 기술 그룹들이 바로 현재 MITER ATT & CK 매트릭스의 전술 또는 열(컬럼) 제목이다. 요약하면, FMX 프로젝트의 개선된 방안이 바로 현재의 MITER ATT & CK 매트릭스이다. 현재 MITRE ATT&CK 매트릭스는 정보보안 커뮤니티에서 호스트 기반 공격자 행위에 대해서 효과적인 소통의 수단으로 사용되고 있다[11].

그림 2는 MITRE ATT&CK 매트릭스와 TTP (Tactics, Techniques and Procedures)를 나타내고 있다[12][13]. 그림에서 각 열(컬럼) 헤더(파란색)는 공격자의 전술(Tactics)을, 각각의 셀은 기술(Techniques)를 표현하고 있으며, 절차(Procedures)는 특정 기술(Techniques)을 수행하기 위한 명령(Instruction)을 제시하고 있다.

앞서 언급한 바와 같이, 현재 MITER ATT & CK 매트릭스는 엔드포인트 탐지를 목표로 하고 있으므로 호스트 기반 기술만 포함하고 있으며 네트워크 기반 기술을 사용하여 공격자 행위를 추적할 수 있는 기술 기반을 제공하지 않고 있다.

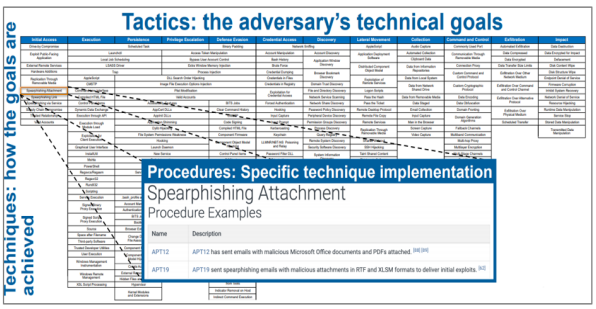

그림 2. MITRE ATT&CK 및 TTPs 설명
Fig. 2. MITRE ATT&CK and TTPs explanation

따라서 본 논문에서는 MITRE ATT&CK의 단점을 해결하기 위하여 네트워크 관점의 공격자 행위 매트릭스를 제안하며, 제안된 네트워크 관점에서의 공격자 행위 매트릭스는 네트워크 관점에서 APT 행위를 묘사하는 프레임워크를 제공한다.

III. 연구 방법

이 장에서는 네트워크 관점에서의 공격자 행위 매트릭스를 구축하는 데 사용되는 프로세스 및 방법 그리고 매트릭스를 활용하여 네트워크 관점에서 APT를 탐지하고 매트릭스의 효율성을 검증하는 실험에 관한 세부 정보를 제시한다.

그림 3은 네트워크 관점에서의 공격자 행위 매트릭스를 구축하는 데 사용되는 과정을 설명하고 있다.

그림 3에서 설명하고 있는 바와 같이, 먼저 다수의 실제 APT 보고서에서 브라이언트 킬 체인 모델[10]에 기반을 둔 키워드를 추출하여 키워드가 포함된 APT보고서를 수작업으로 분석하여 실제 APT 공격에서 사용한 기술들을 추출하여 네트워크 관점 공격자 행위 매트릭스를 완성한다.

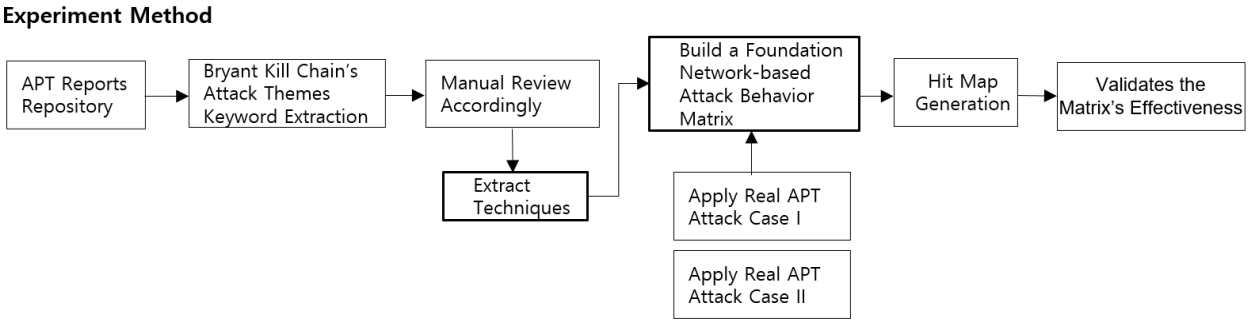

그림 3. 실험 방안
Fig. 3. Experimental method

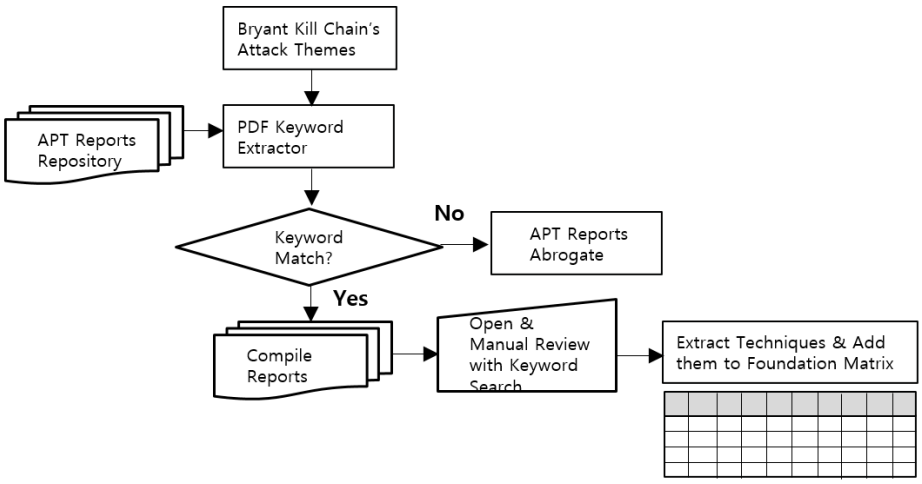

그림 4. 네트워크 관점의 공격자 행위 매트릭스 구축 방안
Fig. 4. Building the network-based attacker behavior foundational matrix

이후, 실제 APT 공격 보고서 (사례)를 매트릭스에 적용하여 히트 맵(Hit map)을 생성함으로써 네트워크 관점 공격자 행위 매트릭스가 실제 APT공격 사례를 효과적으로 검출할 수 있는지 여부를 검증한다. 이를 통하여 네트워크 관점 공격자 행위 매트릭스의 일반성 및 효용성을 확인한다.

3.1 네트워크 관점에서의 공격자 행위 매트릭스의 생성

네트워크 관점의 기술에 중점을 둔 MITER ATT & CK 스타일의 매트릭스를 만드는 데 사용하는 절차는 위에서 언급한 MITRE와 유사한 접근 방식을 사용한다. 먼저, 네트워크 관점에서의 공격자 행위를 설명하기 위해서는 공격자 모델이 필요한데, 앞서 논의한 바와 같이, 진보된 네트워크 관점의 공격자 모델인 브라이언트 킬 체인 모델[10]을 열(컬럼) 제목 (공격 테마)을 생성하는 데 사용하였다.

브라이언트 킬 체인 모델로부터 네트워크 관점 공격자 행위 매트릭스의 열(컬럼)을 채울 수 있는 키워드를 추출하였다. 이후 APT 보고서 리포지토리[14]를 위협 인텔리전스 자원으로 활용하여 APT가 사용하는 것으로 알려진 기술 목록을 추출하여 “네트워크 관점 공격자 행위 매트릭스”를 생성하였다.

그림 4는 네트워크 관점 공격자 행위 매트릭스의 생성 과정을 나타내고 있다.

3.2 브라이언트 킬 체인 모델 공격 테마

공격자 행위 매트릭스의 목표는 APT를 탐지할 때, 매트릭스의 효율성을 측정하고 매트릭스 상에 명시된 기술의 유효성을 검증하는 것이다. 따라서

본 논문에서 제시하는 네트워크 관점 공격자 행위 매트릭스도 본래의 MITER ATT & CK 매트릭스와 마찬가지로 열(컬럼) 제목을 가지며, 네트워크 관점에서의 공격 테마를 기반으로, 알려진 APT 공격 단계를 표현한다. 우선, 앞에서 언급한 브라이언트 킬 체인 모델을 초기 공격 테마(컬럼 제목)로 사용하였다.

네트워크 관점 공격자 행위 매트릭스 생성을 위해 사용한 브라이언트 킬 체인의 공격 테마는 다음과 같다:

- 정찰 및 무기화 (Recon and Weaponization)
- 내부망 이동 (Lateral movement)
- 초기 침입 (Initial compromise)
- 전송 (Delivery)
- 목표에 대한 행위 (Actions on objective)

3.3 APT 보고서 검토 방안

네트워크 관점의 공격자 행위 매트릭스는 APT 보고서에 대한 문서 검토 중에 발견된 기술로 구성되어 있으며, APT에서 공격자가 사용하는 기술을 네트워크 관점에서 기술한다. APT 보고서의 경우, 학술적인 출처가 있는 경우가 거의 없기 때문에 실제적이고 다양한 APT 보고서를 참고하여 공격자의 행위에 대한 위협 인텔리전스로 사용하였다. 다양한 APT 보고서를 검토하면서 브라이언트 킬 체인 모델에 포함되어 있지 않은 공격 테마가 발견되는 경우, 해당 기술을 네트워크 관점의 공격자 행위 매트릭스에 추가하였다.

위에서 언급한 브라이언트 킬 체인의 각 단계는 PDF 보고서에서 네트워크 관점의 공격자 행위에 대해 검색 할 수 있는 키워드 목록을 제공하지만 합리적인 시간에 표 1의 1,075개의 보고서 (논문시점: 5.2 GB)를 모두 읽고 분석한다는 것은 현실적으로 불가능하다. 따라서 본 논문에서는 APT 보고서의 효과적인 검토를 위해서 PDF문서에서 키워드를 추출하는 도구를 이용하였다[15][16]. PDF에서 키워드를 추출하는 도구는 키워드 목록과 PDF 디렉토리를 입력 값으로 키워드가 들어 있는 디렉토리 내의 모든 PDF를 스캔하여, 해당 키워드를 포함하고 있는 파일들을 식별한다. 식별된 PDF 파일에서 수작업으로 키워드를 검색한 다음 키워드와 관련된 문장을 읽은 후, 매트릭스 상에 새로운 기술을 추가하거나 이미 반영된 기술을 확인하였다. 네트워크 관점의 공격자 행위 매트릭스의 완전한 구성을 위해 이러한 과정을 반복하였다.

표 1. 검토한 APT 보고서
Table 1. Reviewed APT reports

Year	# of APT reports	Size (MB)
2006	1	0.792
2008	4	2.07
2009	3	6.32
2010	11	13.4
2011	15	18.4
2012	27	41.5
2013	59	130
2014	113	193
2015	129	232
2016	125	363
2017	115	256
2018	165	429
2019	176	412
2020.07	101	2790
Others	31	264
Total	**1,075**	**5.21 GB**

이러한 과정을 거쳐 추가로 추출한 공격 테마는 다음과 같다:

- 내부 정찰 (Internal recon)
- 가장 (Impersonation)
- 서비스 거부 (DoS)
- 회피 (Evasion)
- 명령 및 제어 (Command and control)

3.4 네트워크 관점의 공격자 행위 매트릭스 생성

3.1절 ~ 3.3절의 과정에서 매트릭스를 생성할 때, 초기에는 공격 테마에 따라 새로운 열(컬럼)을 생성하였는데, 새로운 공격 열(컬럼)이 유효한 지를 검증하기 위해서는 각 열(컬럼)에 해당되는 최소 두 가지 이상의 기술이 발견되는 경우에만 열(컬럼)으로 확정하였다. 즉, 해당 기술을 참조한 APT 보고서를 이용하여 APT에서 사용하고 있는 기술의 유효성을 확인하고, 각 열(컬럼)에 해당되는 두 가지 이상의 기술이 존재하는 경우에 해당 공격 테마가 유효한 것으로 판단하였다.

이러한 과정을 거쳐 생성된 매트릭스는 표 2와 같다.

본 논문에서 제안한 네트워크 관점 공격자 행위 매트릭스는 위에서 언급한 위협 헌팅 절차를 활용하여 보안 분석가가 네트워크 관점에서도 APT가 발생하고 있는지 여부를 판단할 수 있도록 한다. 추가적으로 본 논문에서 제안된 네트워크 관점에서의 공격자 행위 매트릭스를 APT 보고서에 적용함으로써 IP 주소와 같은 임시적이고 제한적인 IOC 대신 APT 맬웨어 또는 공격 행위를 묘사하는데 이용될 수 있을 것이다.

Ⅳ. 결과 및 분석

4.1 실험 방안

실험을 위해서 특정 위협 행위자 (APT 그룹)에 중점을 둔 두 가지 APT 공격 사례를 분석하였다. 각 테스트 사례에 대해 먼저 각 위협 행위자를 분석하기 위해 필요한 공개 보고서를 수집하였다. 이후 각 APT 보고서를 분석하여 네트워크 관점에서 관찰 가능한 공격자 기술에 주목하였다. 또 특정 위협 행위자에 대한 네트워크 관점 기술 목록을 작성하고 표 2의 공격자 행위 매트릭스에 적용하여 히트 맵(Hit map)을 생성하였다. 이러한 과정을 통해 생성된 히트 맵은 특정 위협 행위자 탐지관점에서 본 논문에서 제시한 매트릭스의 효율성을 나타낸다.

첫 번째 테스트 사례로 라자루스 그룹(Lazarus group)[17]을 분석하였는데, 2011년 농협 전산망 마비 사태와 국가정부기관 DDoS 사태와 관련이 있을 것으로 의심되는 공격 그룹이기 때문이다. 국가정부기관 DDoS 사태는 2011년 3월 3일부터 5일까지 청와대, 국방부, 국가정보원 등 국내 주요 정부기관과 국민은행, 네이버 등 국내 주요 40개 사이트를 대상으로 분산 서비스 거부 공격, 즉 디도스(DDoS) 공격이 발생한 사건이다. 농협 전산망 마비 사태는 2011년 4월 12일 농협 전산망에 있는 자료가 대규모로 손상되어 수일에 걸쳐 전체 또는 일부 서비스 이용이 마비된 사건이다. APT는 여러 산업과 조직을 대상으로 발생하고 있으며, 공격 대상이 되는 이유는 금전적인 동기, 공격 대상이 신뢰할 수 있는 제 3자 또는 C2의 중심축으로 사용할 수 있기 때문이다. 따라서 모든 조직은 공격자의 동기에 관계없이 모든 APT를 탐지하기 위한 보안 통제를 구현할 필요가 있다.

두 번째 테스트 사례로는 이란 스파이 그룹을 분석하였는데, 이 APT 그룹은 APT 33, APT 34, APT 35, APT 39 및 APT 41 등의 여러 APT 그룹과 연관되어 있기도 하고 학계에서 분석한 APT 보고서가 존재하며, 특히, 대한민국의 석유화학에 대한 사이버 스파이 활동이 포함된 공격자 그룹이기 때문이다[18].

일부 보고서의 경우, 공격자 그룹이 혼재되어 있어서 분석이 다소 어려운 부분도 있었으나, 모든 보고서의 공통적인 사실은 위협 행위자가 이란의 위협 행위자였다는 사실이다.

표 2. 네트워크 관점 공격자 행위 매트릭스
Table 2. Network-based attacker behavior matrix

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	Dos	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	UDP Flood	Poisoned torrents	IRC	Defacement
	SSH Hijacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	
								HTTP	

이란 스파이 그룹 사례는 시간이 지남에 따라 APT 그룹이 어떻게 진화했는지 그리고 해당 APT 그룹 탐지 방안이 어떻게 진화 했는지를 잘 보여주고 있다. 여기에서 주목할 점은 해당 위협 행위자가 사용하는 일부 기술은 모든 공격 캠페인에서 공통적으로 사용되었으며 따라서 그들이 사용하는 공통적인 기술을 탐지할 경우, 시간이 지나도 여전히 해당 위협 행위자를 특정할 수 있는 매우 중요한 요소라는 사실이다.

표 3. 라자루스 그룹이 사용한 네트워크 기술
Table 3. Network-based techniques used by Lazarus group.

Recon and Weaponization	No techniques for this category
Lateral movement	❖SMB : SorryBruteattempts to bruteforce SMB [18] ,SMB brute-forcing credentials [23] ❖Remote Desktop : APT 38 used RDP [23] ❖Exploit : Malware sends commands to configuration management agent on hosts via a vulnerability to run arbitrary code by pretending to be the configuration management server [21]
Internal recon	❖Service enumeration : Network tools to perform recon [18] ❖Network sniffing : IndiaBravoinstalls network monitoring library to monitor network [19]
Initial compromise	❖Malicious stager : Malicious documents downloaded malicious stager[20] [21] [22] [25], Malware downloads malicious tools and files [18] [21] [22]…. ❖Exploits : Exploited configuration management systems to delivery malware or run arbitrary commands [21]… Remote exploit by exploiting an Apache Struts2 server [23] Waterhole attacks to exploit browser vulnerabilities [21]
Impersonation	❖Trusted third party : Sent e-mails impersonating the national assembly member's office [33], Malware infection through financial union website waterhole [21] Compromised e-mail and gaming servers to use as C2 proxies [18] [21]…
Evasion	❖Encryption : Encryption for C2 communication [18] [21], QuickRide uses TLS over HTTP for C2 communication [23]… ❖Encoding : PowerRatankbacommands from C2 are encrypted with Base64 [22] ❖Covert comm : Covert communication channel using a port scanner [21] ❖Custom protocol : CheeseTrayuses a custom binary protocol for C2 [23] ❖Compression : Javascriptdownloader was stored in ZIP [22] ❖Public services : PowerSpritzwas stored on Google Drive [22], C2 addresses that were identified were public proxies [18]… ❖Custom obfuscation : Custom implementation of TLS [18]
DOS	❖HTTP flood : July 4, 2009 a large scale DDOS attack on US and South Korean websites [18] [24] ❖Unknown - Lazarus group used malware that contained DDOS functionality April 2011 DDOS attack targets Nonghyup Bank [18]
Delivery	❖Phishing : Spear phishing with malicious attachments [18] [20] [21] [22] [23] [25] ❖Waterhole : Malware infection through financial union website waterhole [21] [22] [23] , Waterhole attacks to exploit browser vulnerabilities [21] [23] ❖Internal IT assets : Instructed configuration management system to download malware via HTTP onto machines [21] ❖Poisoned torrents : Attackers compromised file-sharing sites such as torrent websites [18]
Command and control	❖HTTP : PowerRatankbautilizes HTTP for its C&C communication &QuickRide uses HTTPS to communicate with C2 [21] [22] [23] ❖TCP : IndiaIndiaTCP C2 + covert comm [19] ❖Listening service : APT38 planted backdoors and opened firewall ports [23] RemeoFoxtrott-Two is a server-mode RAT therefore it listens on a port [19] ❖Webshell : JspSpyused by APT38 is a webshell [18] ❖Peer-to-peer : Lazarus group used P2P malware against Sony [18]
Action on objectives	❖Exfiltration : Leakage of classified data such as aircraft drawing from defense contractors [21], Leakage of customer PII from a travel agency [21] Exfiltratedvarious info from the Sony network [20], Malware can upload files [18] [19] [21]… ❖Defacement : Lazarus group publicly released the data they stole from the Sony network [18]

4.2 실험 결과 분석

Novetta사의 보고[19]에 따르면 "소니 픽처스 엔터테인먼트에 대한 공격은 언론 보도 측면이나 기업에 대한 악의적인 파괴 능력의 명백한 사용" 측면에서 미증유의 사건으로 규정하고 있다. 소니 픽처스 엔터테인먼트에 대한 공격은 미국 영리 단체에 대한 파괴적인 맬웨어 공격뿐만 아니라 미국 정부가 북한 소행으로 규정함으로써 보복조치를 강구하는 지평을 열었다. 북한 소행, 핵티비스트의 소행, 또는 소니 픽쳐스 엔터테인먼트 직원 소행 등에 대한 논쟁이 언론에서는 가장 중요한 주제였지만, 보다 중요한 사실은 상업 기업이 파괴적인 의도를 가진 유능하고 결정적인 공격자들에게 얼마나 무력한지를 보여주는 사건이었다. 라자루스 그룹이 사용한 네트워크 기술은 표 3과 같다:

표 4는 라자루스 그룹이 사용한 네트워크 기반 기술이 본 논문에서 제시한 공격자 행위 매트릭스상에 존재하는 지 여부를 나타내는 히트 맵이다. 표 4에서 회색 계열로 표시된 부분은 라자루스 그룹이 사용한 네트워크 기반 공격 행위와 본 논문에서 제시한 매트릭스상의 기술과의 일치 여부를 나타내고 있으며, 검은 색 계열의 컬럼은 라자루스 그룹이 사용했으나 매트릭스에서 제시하지 못하는 부분을 나타내고 있다.

전체 매트릭스의 43개의 기술 중에서 라자루스 그룹은 27개의 기술을 사용했으며, 매트릭스가 커버한 기술은 24개이며, 커버하지 못한 기술은 3개이다. 따라서 전체적으로는 본 논문에서 제시한 매트릭스는 라자루스 그룹이 사용한 기술의 88.89%를 제시하고 있음을 알 수 있다.

이란 사이버 스파이 그룹에 대한 보고서는 “해당 그룹이 사우디아라비아와 대한민국의 석유화학 부문, 미국과 사우디아라비아의 군사 및 항공 산업을 대상으로 하는 사이버 스파이 위협 행위자”로 기술하고 있다. 이란 위협 행위자는 2013년 이후부터 운영되어 왔으며 사이버 스파이 전문가가 사이버 스파이 캠페인에서 관찰한 전술, 기술 및 절차(TTP)를 활용하여 파괴적인 사이버 공격에 관여할 수 있는 능력으로 잘 알려져 있다.

이란 사이버 스파이(Iranian cyber espionage)가 사용한 네트워크 기술은 표 5와 같다:

표 6은 이란 사이버 스파이가 사용한 네트워크 기반 기술이 본 논문에서 제시한 매트릭스에 존재하는 지 여부를 나타내는 히트 맵이다.

표 6에서 회색 계열로 표시된 부분은 이란 사이버 스파이가 사용한 네트워크 기반 기술과 본 논문에서 제시한 매트릭스상의 기술과의 일치 여부를 나타내고 있으며, 검은 색 계열의 열(컬럼)은 이란 사이버 스파이가 사용했으나 본 논문의 매트릭스에서는 제시하지 못하는 부분을 나타내고 있다.

표 4. 라자루스 그룹 vs. 네트워크 행위 기반 매트릭스 대응 맵
Table 4. Lazarus group vs. network behavior-based matrix hit map

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	Dos	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	UDP Flood	Poisoned torrents	IRC	Defacement
	SSH Hijacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB			Certificate impersonation	Encoding		Internal Assets	DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
					Compression			Listening Service	
					Covert Communication			HTTP	
								TCP	

표 5. 이란 사이버 스파이가 사용한 네트워크 기술
Table 5. Network-based techniques used by Iranian cyber espionage

Recon and weaponization	❖Vulnerability scanner : Metasploit, SQLMap, Acunetic, Netsparker, and WSO web shell were used to scan and attack targets [24]…
Lateral movement	❖Mimikatz [24] : Operation Cleaver used Mimikatz to pivot the network [24] ❖SSH : POWBAT uses SSH for lateral movement [24] ❖RDP : Operation Cleaver used RDP to run commands [24] ❖SMB : POWBAT uses SMB for lateral movement, Operation Cleaver used PsExec to move laterally [24] ❖Windows Management Instrumentation (WMI) [24]
Internal recon	❖Service enumeration : Powersploitfor internal reconnaissance [18] ❖Network sniffing : The malware MPK has the ability to perform traffic monitoring [18]
Initial compromise	❖Externally exposed services : APT39 brute-forced externally exposed services such as Outlook [24] ❖Exploits : Leafminerestablished an initial compromise with known network vulnerabilities [24]… ❖SQL injection : Operation Cleaver used SQL injection to achieve initial compromise [24]… ❖Malicious stager : DownPaperis a dropper that downloads more malware[25] Operation Woolean-Goldfish used a malicious document to instruct the machine to pull down CWOOLGER [24]….
Impersonation	❖ARP spoofing : Operation clever created malware code name JASUS to perform ARP spoofing [24] ❖Trusted third party : Charming Kitten sends thousands of phishing emails which contain TinyURL links[25]… ❖Illegitimate services and sites : Setup illegitimate websites to offer free classes for Aerospace. This website requested users to install a malicious Adobe Flash [24]…
Evasion	❖Public services : Operation Woolean-Goldfish used public services such as Microsoft OneDrive to host malicious executables [24] DropBoxwas used to host RAR files that contained malicious documents [24] ❖Encoded : DownPaperbase64 encodes the URL to download stager [25] Operation Cleaver double-encoded it's SQL injection payloads to bypass WAF [24] ❖Encryption : GHOLEE used encryption for data exfiltration [24], TEMP.Zagros supports encryption for C2[24]… ❖Compression : Moleratsused RAR files to hide malicious document, Exfiltrate data using WinRAR [24] ❖Custom obfuscation : EXPLOSIVE used custom obfuscation for C2 [24], After an initial compromise from a malicious document the C2 communication used obscured communication [24]
DOS	No techniques for this category
Delivery	❖Waterhole : Charming Kitty uses BEEF exploitation to exploit browsers [25] Phishing e-mails containing links to illegitimate websites with instructions to install malware [24]…. ❖Phishing : Charming Kitten sends thousands of phishing emails using Gmail [25]…. Spear phishing campaign used to deliver "Operation Protective Edge.xlsb", this malware is called GHOLEE [24]
Command and control	❖HTTP : DUSTYSKY used HTTPS for C2 [24], DownPaper uses HTTP for C2 [25], … ❖SMTP : Operation Cleaver used SMTP to exfil data and C2 [24] ❖SSH : Operation Cleaver used SSH to exfil data [24] ❖IRC : IRC was used for bot-based malware [24]… ❖FTP : CWOOLGER used FTP for C2 and data exfil [24]… ❖DNS : Data exfiltration would be performed through the use of DNS queries [24]
Action on objectives	❖Exfiltration : Collect intelligence on the military aviation capabilities of the Kingdom of Saudi Arabia and South Korea petrochemical companies [24]….

본 논문에서 제시한 매트릭스의 43개의 기술 중에서 이란 사이버 스파이는 30개의 기술을 사용했으며, 매트릭스가 커버한 기술은 24개이며, 커버하지 못한 기술은 6개이다. 따라서 전체적으로는 본 논문의 매트릭스는 이란 사이버 스파이가 사용한 기술의 80%를 제시하고 있음을 알 수 있다.

표 6. 이란 사이버 스파이 vs. 네트워크 행위 기반 매트릭스 대응 맵
Table 6. Iranian cyber Espionage vs. network behavior-based matrix hit map

Recon and Weaponization	Lateral movement	Internal recon	Initial compromise	Impersonation	Evasion	Dos	Delivery	Command and control	Action on objectives
Public scanning services	WMI	Service enumeration	Malicious stager	VPN tunneling	Anonymous services	UDP Flood	Watering hole	Peer-to-peer	Exfiltration
Vulnerability scanning	WinRM	Port scanning	SQL injection	Trusted third party	Public services	UDP Flood	Poisoned torrents	IRC	Defacement
	SSH Hijacking	Network sniffing	Exploit	Reverse RDP tunnel	Encryption	HTTP Flood	Phishing	ICMP	
	SMB		Externally exposed service	Certificate impersonation	Encoding			DNS	
	Remote Desktop			Domain spoofing	Custom protocol			Webshell	
	Exploit			ARP spoofing	Custom obfuscation			Remote Admin Tools	
	Mimikatz			illegitimate service or site	Compression			Listening Service	
								HTTP	
								SMTP	
								SSH	
								FTP	

V. 결 론

MITRE ATT&CK는 공격자 수명 주기의 전술 및 기술을 반영한 행위(Behavior) 식별을 위한 지식 기반 모델로서, 알려진 지능형 위협에 대한 위험성을 이해하고 보안 테스트 계획 및 방어 계획을 수립하는데 유용한 지식 기반이다. 복잡하고 다양한 오늘날의 공격에 대응하기 위해서는 공격자의 전술 및 기술에 대한 공통 지식을 기반으로 보안 전략을 수립하는 것이야말로 성공적인 사이버 보안의 핵심으로 부각되고 있다.

효과적인 위협 헌팅을 위해서 보안 분석가는 네트워크 및 호스트 기반 기술을 모두 찾아내야 하는데, 현재 MITER ATT & CK 매트릭스만으로는 이러한 목표를 달성할 수 없기 때문에, 본 논문에서는 MITRE ATT&CK을 기반으로 네트워크 관점에서 위협 헌팅에 활용할 수 있으며, 반복 가능하고 측정 가능한 결과를 도출할 수 있는 43개 네트워크 기반 행위와 관련된 기술에 대한 열(컬럼)을 가지는 네트워크 관점의 공격자 행위 매트릭스를 구현하였다.

본 논문에서 제시한 네트워크 관점 공격자 행위 매트릭스의 효용성을 검증하기 위해 대한민국 공격에 직접적으로 관여된 것으로 추정되는 두 가지 실제 APT 공격 사례를 매트릭스에 적용한 결과, 80% 이상의 효용성을 확인하여 제시하였다. 결론적으로 보안 분석가가 본 논문에서 제시한 네트워크 관점 공격자 행위 매트릭스를 활용한다면 네트워크 관점에서도 공격자 체류 시간을 줄이는 데 활용할 수 있을 것이다.

본 논문에서 제시한 네트워크 관점 공격자 행위 매트릭스를 발전시키기 위해서는 MITRE ATT&CK 매트릭스와 마찬가지로 지속적으로 공격 기법을 수집하고 분석하여 매트릭스의 셀을 추가해야 할 것으로 판단된다. 본 논문에서 제시한 매트릭스에서 제시한 기술을 효과적으로 탐지할 수 있는 네트워크 기반 보안 분석 기술을 구현하여 실제 기업 네트워크에 적용한다면 보다 상세한 실증이 가능할 것으로 판단되며, 향후 연구 주제로 남기고자 한다.

References

[1] Christopher A. Korban, Douglas P. Miller, Adam Pennington, and Cody B. Thomas, "APT3 Adversary Emulation Plan", MITRE, Sep. 2017.

[2] NOVETTA, "Operation Blockbuster: Unraveling the Long Thread of the Sony Attack", 24 Feb. 2016.

[3] Yonathan Klijnsma, RiskIQ, Vitali Kremez, Flashpoint, and Jordan Herman, RiskIQ, "Inside

Magecart: Profiling the Groups Behind the Front Page Credit Card Breaches and the Criminal Underworld that Harbors Them", RISKIQ, 13 Nov. 2018.

[4] Wikipedia, "Cyber threat hunting", https://en.wikipedia.org/wiki/Cyber_threat_hunting. [accessed: 13 Jun. 2020]

[5] Paul Ewing, Devon Kerr, "The Endgame Guide to Threat Hunting: Practitioner's Edition", ENDGAME, 3 Jun. 2018.

[6] MITRE, ATT&CK Matrix for Enterprise, MITRE, https://attack.mitre.org/. [accessed: 12 June 2020]

[7] Lockheed Martin, "GAINING THE ADVANTAGE Applying Cyber Kill Chain® Methodology to Network Defense", Lockheed Martin Corporation, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf. [accessed: 15 May 2020]

[8] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains",Leading Issues in Information Warfare and Security Research, Vol. 1, No. 1, pp. 80-106, 2011.

[9] FireEye, "APT1: Exposing One of China's Cyber Espionage Units", MANDIANT, 25 Oct. 2004.

[10] Blake D. Bryant, Hossein Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software", ResearchGate, https://www.researchgate.net/publication/314782193_A_novel_kill-chain_framework_for_remote_security_log_analysis_with_SIEM_software. [accessed: 3 May 2020]

[11] Blake Strom, "A CYBER SECURITY ENGINEER SCORES A BIG WIN WITH ATT&CK", MITRE, https://www.mitre.org/careers/working-at-mitre/employee-voices/a-cyber-security-engineer-scores-a-big-win-with-attck. [accessed: 25 June 2020]

[12] MITRE, "Using ATT&CK for Cyber Threat Intelligence Training", MITRE, https://attack.mitre.org/resources/training/cti/. [accessed: 10 May 2020]

[13] MITRE, "Enterprise Matrix", MITRE, https://attack.mitre.org/matrices/enterprise/. [accessed: 25 May 2020]

[14] Rizwan Qaiser, "How to Extract Words From PDFs With Python", BetterProgramming, https://medium.com/better-programming/how-to-convert-pdfs-into-searchable-key-words-with-python-85aab86c544f. [accessed: 25 May 2020]

[15] Marie Baezner, "Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions", © 2019 Center for Security Studies (CSS) ETH Zürich, May 2019.

[16] Andrea Zivalich, "NORTH KOREA, CYBERATTACKS AND 'LAZARUS': WHAT WE REALLY KNOW", NOVETTA, 12 Jun. 2017.

[17] MITRE, "Lazarus Group", The MITRE Corporation, https://attack.mitre.org/groups/G0032/. [accessed: 25 May 2020]

[18] NOVETTA, OPERATION BLOCKBUSTER Unraveling the Long Thread of the Sony Attack, Dec. 2014.

[19] ThaiCERT, THREAT GROUP CARDS: A THREAT ACTOR ENCYCLOPEDIA, 19 June 2019.

[20] NOVETTA, OPERATION BLOCKBUSTER Unraveling the Long Thread of the Sony Attack, Dec. 2014.

[21] AhnLab, "Full Discloser of Andariel, A Subgroup of Lazarus Threat Group", 23 June 2018.

[22] Darien Huss, North Korea Bitten by Bitcoin Bug, proofpoint, 19 Dec. 2017.

[23] FireEye, APT38: UN-USUAL SUSPECTS, 15 Nov. 2018.

[24] Jason G. Spataro, Iranian Cyber Espionage, ProQuest Research Library, May 2019.

[25] ClearSky Cyber Security, Charming Kitten: Iranian Cyber Espionage Against Human Rights Activists, Academic Researchers and Media Outlets, 2 Dec. 2017.

[26] Akashdeep Bhardwaj and Sam Goundar, "A framework for effective threat hunting", Network Security, Vol. 2019, No. 6, pp. 15-19, Jun. 2019.

[27] Sahad Homeayoun, Ali Dehghantanha, Marzieh Ahmadzadeh, Sattar Hashemi, Raouf Khayami, Kim-Kwang R. Choo, and David E. Newton, "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer", Future Generation Computer Systems, Vol. 90, pp. 94-104, Jan 2019.

[28] DeokJo Jeon and Dong-Gue Park, "Analysis Model for Prediction of Cyber Threats by Utilizing Big Data Technology", Journal of KIIT, Vol. 12, No. 5, pp. 81-100, 31 May 2014.

저자소개

전 덕 조 (Deok-Jo Jeon)

1989년 2월 : 아주대학교 전자계산학과(공학사)
1995년 5월 : 뉴멕시코대학교 컴퓨터과학과(이학석사)
2005년 10월 ~ 현재 : (주)씨큐비스타 대표이사
관심분야 : 지능형 위협 대응, 지능형 보안관제, 네트워크 보안

박 동 규 (Dong-Gue Park)

1992년 2월 : 한양대학교 전자공학과(공학박사)
1992년 3월 ~ 현재 : 순천향대학교 정보통신공학과 교수
관심분야 : 제어 시스템 보안, 네트워크보안, 시스템 보안, 모바일 보안