JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 9, pp. 71-80, September 2020
https://doi.org/10.9708/jksci.2020.25.09.071

Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training

Donghwa Kim*, Yonghyun Kim**, Myung-Kil Ahn***, Heejo Lee****

*Student, Dept. of Computer and Radio Communications Engineering, Korea University, Seoul, Korea
**Principal Researcher, The 2nd R&D Institute, Agency for Defense Development, Seoul, Korea
***Student, School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, Korea
****Professor, Dept. of Computer Science and Engineering, Korea University, Seoul, Korea

[Abstract]

As societies become hyperconnected, we need more cyber security experts. To this end, in this paper, based on the analysis results of the real world cyber attacks and the MITRE ATT&CK framework, we developed CyTEA that can model cyber threats and generate simulated cyber threats in a cyber security training system. In order to confirm whether the simulated cyber threat has the effectiveness of the actual cyber threat level, the simulation level was examined based on procedural, environmental, and consequential similarities. in addition, it was confirmed that the actual defense training using cyber simulation threats is the same as the expected defense training when using real cyber threats in the cyber security training system.

▸ **Key words**: Red team emulation, cyber range, ATT&CK, Operation Dust Storm, threat emulation

[요 약]

사회가 초연결 사회가 되어 갈수록 우리는 더 많은 사이버 보안 전문가들이 필요하다. 이를 위해 본 논문에서는 실제 사이버 공격에 대한 분석결과와 MITRE ATT&CK 프레임워크를 바탕으로 사이버 모의 위협을 모델링하고 실제 사이버 보안 훈련 시스템에서 모의 된 사이버 위협을 생성할 수 있는 CyTEA를 개발하였다. 모의 된 사이버 위협이 실제 사이버 위협 수준의 유효성을 갖는지를 확인하기 위해 절차적, 환경적, 결과적 유사성을 기준으로 모의 수준을 알아보고 또 실제 사이버 보안 훈련 시스템에서 모의 위협을 실행하면서 방어훈련 시 예상되는 위협의 실제 위협실행 결과와 모의 위협의 실행 결과가 동일하여 실제 사이버 위협에 준하는 훈련을 가능함을 확인하였다.

▸ **주제어**: Red team 에뮬레이션, 사이버 레인지, ATT&CK, Operation Dust Storm, 위협 모의

• First Author: Donghwa Kim, Corresponding Author: Heejo Lee
*Donghwa Kim (donghwa78@korea.ac.kr), Dept. of Computer and Radio Communications Engineering, Korea University
**Yonghyun Kim (yonghyunkim@add.re.kr), The 2nd R&D Institute, Agency for Defense Development
***Myun-Kil Ahn (lovedew@cau.ac.kr), School of Electrical and Electronics Engineering, Chung-Ang University
****Heejo Lee (heejo@korea.ac.kr), Dept. of Computer Science and Engineering, Korea University
• Received: 2020. 07. 29, Revised: 2020. 09. 03, Accepted: 2020. 09. 05.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

국가 간 사이버전이 현실화되고, 금전적 목적으로 사이버 공격이 대상을 가리지 않고 발생하게 됨에 따라 대부분의 사회/경제 시스템이 정보화된 현실에서 거의 모든 분야에서 사이버 보안에 대한 경각심과 관련 인력에 대한 수요가 폭증하고 있고, 사회가 점점 더 초연결 사회로 나아감에 따라 그런 경향은 더 커질 것이 확실시되고 있다. 이런 요구에 발맞추어 대학 및 산업계뿐 아니라 국방 분야에서도 사이버 보안 기술 교육에 대한 필요성을 느끼고 사이버 보안 기술에 대한 훈련 시스템 연구개발이 수행되었다[13] [14].

사이버 보안 훈련은 일반적으로 공격을 수행하는 레드팀과 방어를 수행하는 블루팀 그리고 훈련을 계획/관리하기 위한 화이트팀으로 구성된다. 사이버 방어 기술, 즉 블루팀을 훈련시키기 위해서는 그에 맞는 레드팀도 준비가 되어야 하며, 레드팀의 수준은 블루팀 보다 더 높은 기술적 수준을 유지하여야 한다. 이런 고도로 훈련된 인적자원을 대체할 수 있는 자동화 기술을 통해 인력 활용의 효율성을 높일 수 있고, 동일한 훈련을 여러 클래스에서 동일한 수준을 유지하면서 수행할 수 있다.

이를 위해 본 논문에서는 MITRE의 ATT&CK 프레임워크에서 정의한 전략(Tactic)과 기술(Technique)을 단위위협으로 이용하여 단위위협의 조합을 통해 사이버 위협을 모델링 하고 이를 사이버 보안 훈련 시스템에 자동화 위협으로 생성할 수 있는 사이버 위협 모의 도구인 CyTEA (Cyber Threat Emulation and Automation)를 개발하였다. 또한, 실제 APT 형태의 사이버 위협인 Operation Dust Storm에 대한 사이버 공격 분석 커뮤니티의 분석 결과[7]를 기반으로 모의한 사이버 위협을 이용한 사이버 방어 훈련 결과가 실제 사이버 위협을 방어 시 예상되는 결과와 유사하여 사이버 방어훈련에서 유효함을 확인하였다.

본 논문의 구성은 다음과 같다. II장에서 사이버 보안 훈련 시스템, MITRE ATT&CK, 그리고 사이버 위협 모의 기술에 대해 알아보고, III장에서 CyTEA에 대해 구성과 각 모듈의 기능에 관해 설명하였다. IV장은 사이버 위협 모델링 방안에 대해 구체적으로 기술하였고, V장에서 사이버 모의 위협의 실행 결과와 사이버 보안 훈련에 적용한 결과를 기술하였다.

II. Related Works

1. Cyber security training system

사이버 보안 기술에 대한 훈련을 위해 사이버 공격이 가능하고, 방어훈련자가 공격에 대한 대응을 진행할 수 있는 환경을 제공하는 방식에는 크게 2가지가 있다. 하나는 구성 모의(constructive simulation) 방식이고, 다른 하나는 실가상 환경 모의(Live-Virtual simulation) 방식이다[1]. 2가지 방식은 훈련 시나리오의 저작 레벨, 실제 환경의 반영 충실도, 훈련의 제한, 실시간성 등 많은 부분에서 장단점이 있지만, 각각의 필요성에 따라 연구가 지속되고 있다. 실가상 환경 모의 방식은 2000년대 후반부터 DARPA에서 추진한 NCR(National Cyber Range)[13]과 2016년에 JAIST에서 개발한 CyRIS(Cyber Range Instantiation System)[14]가 있다.

NCR[13]은 2009년부터 2012년까지 DARPA에서 추진한 프로젝트로 사이버전 공간을 실체계 및 가상화 기반으로 모델링하여 보안기술에 대한 실험과 분석이 가능할 수 있도록 개발하는 것을 목표로 사이버전 환경 가상화 및 M&S, 시험장관리 자동화, 테스트베드 재구성 기술 등에 관한 연구를 진행하였다.

CyRIS[14]는 KVM 기반 가상화 기술을 사용하고 있으며, 사전에 설정된 OS 별 호스트, 웹서버, 메일서버의 VM을 구축하고, 사용자가 원하는 훈련환경 정보를 YAML로 작성하고 이를 기반으로 각 VM을 복제하여 사이버 훈련장을 생성하는 방식이다.

기존의 사이버 보안 훈련 시스템에서의 위협 발생은 사전에 정해진 시나리오에 따라 필요한 VM 및 공격코드 그리고 공격 진행을 위한 스크립트를 미리 준비하여 발생시킨다. 이러한 방식은 숙련된 보안 인적자원에 대한 지속적인 낭비와 훈련 시나리오에 따라, 훈련 네트워크 환경이 변경될 때마다 매번 공격코드나 스크립트를 재작성해야 하는 한계를 갖는다.

2. ATT&CK Framework

MITRE에서 공개한 ATT&CK(Adversarial Tactics, Techniques & Common Knowledge) 프레임워크[5]는 실제 발생한 사이버 공격에 관한 분석을 바탕으로 공격자의 전술과 기술에 대해 분류한 것이다. 전술과 기술은 대상 시스템과 단계에 따라 PRE-ATT&CK, Enterprise, Mobile 3가지로 나눠 구축하였으며, 본 논문에서는 Enterprise에서 사용되는 전술과 기술을 이용하였다. 2020년 7월 현재 ATT&CK for Enterprise는 12개의 전술 분야에 184개 기술을 식별하고 있고, 지속적으로 업데이트될 것으로 예상된다. 2019년부터 공격행위에 대항하여 수행될 수 있는 방어행위(Mitigations)가 추가되었다.

ATT&CK 프레임워크의 GROUP[6]은 사이버 공격 그룹에 대한 분석 커뮤니티의 분석 결과를 토대로 사이버 공격

그룹이 사용하는 공격방법에 대한 정보를 ATT&CK에서 식별된 전술과 기술 등을 이용하여 표현하였다.

ATT&CK의 전술과 기술의 매트릭스가 발표되고 많은 사이버 위협 에뮬레이터들이 이 매트릭스를 적용하고 있으며, 비교적 새롭게 시장이 형성되고 있는 BAS(Breach and Attack Simulation) 분야에서도 ATT&CK 프레임워크를 포괄적으로 적용하며 시장을 키워가고 있다[1].

3. Cyber threat emulators

사이버 위협 모의 기술은 최근 보안시장에서 주목을 받고 있는 상용 제품 중심의 침입 및 공격 시뮬레이션(BAS: Breach & Attack Simulation)[16][17]와 오픈소스 도구 중심의 위협 에뮬레이터가 있다. BAS 관련해서는 [10]에서, 오픈소스 도구 관련해서는 [8]에서 잘 정리하였다.

[8]에서는 위협 모의의 실행방식, 측면 이동(Lateral movement) 공격의 가능 여부에 따라 사이버 위협 모의 기술을 분류하고 있다. [8]은 11개의 오픈소스 도구에 대한 상세한 분석 및 비교를 통해 사용자가 필요성에 맞는 도구를 선택할 수 있도록 가이드도 같이 제시해주고 있다. 여기서 소개한 주요 모의 기술로는 Red Team Automation [9], Caldera[11], Atomic Red Team[12]이 있다.

Red Team Automation(RTA)[9]은 파이썬 스크립트로 구성된 프레임워크로, 중앙에서 컨트롤하는 C&C 서버가 없는 것이 특징이다. RTA는 여러 단계의 공격을 실행하기 위해 여러 스크립트를 조합하여 생성된 스크립트를 이용할 수 있으며, 측면 이동 공격 기술을 제공한다.

Caldera[11]는 MITRE에서 개발한 도구로 Windows에 대한 보안성 테스트를 위한 것이다. Caldera는 사용자가 설정한 타겟 호스트를 공격하기 위해 경로와 공격 기술 등을 자동으로 선택하여 공격을 진행한다. 자율적 공격을 위해 공격행위와 그에 대한 보상을 기반으로 공격계획을 수립한다. 그 과정에서 사용자가 자체 확보한 RAT(Remote Administrative Tool)을 사용할 수 있는 기능도 제공한다.

Atomic Red Team[12]은 보안성 시험을 위해 사용될 수 있는 라이브러리 형태이며, Atomic Red Team에서 제공하는 API를 이용하여 사이버 위협을 모의하고 자동화할 수 있다. 제공되는 스크립트와 실행파일 형태의 툴 외에 다른 도구를 사용할 수 있도록 기능을 제공하지만, 측면 이동 공격을 위한 공격 기술을 제공하지 않는다.

[10]에서는 사이버 공격 시뮬레이션 기술의 트렌드 변화 관점에서 BAS 기술을 평가하였다.

AttackIQ[16]의 Firedrill은 가장 잘 알려진 상용 BAS 도구로, MITRE ATT&CK 기반의 해킹 대응 능력 평가 플랫폼으로 1,500개 이상의 단위 공격 라이브러리를 구축하고 있다. 공격 템플릿과 시나리오를 통해 공격을 모의할 수 있다.

Cymulate[17]는 클라우드 기반의 사이버 보안 시뮬레이션으로 각 단계별 모의 된 공격을 에이전트가 실제와 같은 악성코드를 다운받아 실행시켜 공격을 진행하며, 그 과정에서 보안 시스템의 취약점과 대응의 문제점을 탐색한다.

오픈소스 기반 기술뿐 아니라 BAS 군의 상용 제품의 사이버 위협 모의 기술들은 시스템에 대한 모의 해킹 자동화를 통해 보안 인프라에 대한 취약점 분석 및 테스트에 초점이 맞춰져 있으며, 단위 공격들의 나열을 통해 사이버 위협을 모의하는 수준으로, 사이버 보안 기술 훈련을 위한 도구 사용하기에는 한계가 있다.

본 논문에 제안하는 CyTEA는 기존 사이버 위협 모의 도구와 달리 단위 공격의 성공/실패의 결과에 따라 실행흐름을 변경할 수 있어 단위위협을 이용하여 로직을 생성할 수 있으며, 위협 프로파일 단위로 위협행위를 모듈화할 수 있어 악성코드 단위 같은 기능 단위로 위협을 생성할 수 있다. 또한, 모의하고자 하는 사이버 위협의 복잡도에 따라 여러 개의 위협 프로파일 간 연동을 통해 점점 복잡해지는 사이버 위협을 보다 실제에 가깝게 모의할 수 있도록 하였다. 기존 사이버 보안 기술 훈련 시스템의 한계였던 시나리오마다 공격을 위한 자재(악성코드, 스크립트 등)를 구축할 필요 없이 한번 단위위협을 위한 코드를 구축하면, 위협 프로파일을 GUI 형태로 저작하여 매번 새로운 공격을 생성할 수 있도록 하였다.

III. CyTEA

1. Overview

사이버 위협을 모델링하고, 이에 따라 사이버 보안 훈련 시스템에서 실제 위협처럼 모의하기 위해 우리는 3개의 모듈[1][2][3]로 CyTEA를 구성하였다. 첫 번째 모듈은 사이버 위협의 절차를 모델링하고 위협이 진행될 시나리오를 저작하기 위한 사이버 위협 모델링 및 시나리오 저작 도구[2], 두 번째 모듈은 저작된 사이버 위협 시나리오를 이해하고 계획이 맞게 위협행위를 실행하며, 위협행위의 실행 결과에 따라 다음으로 분기되어 실행될 위협행위를 선택하는 사이버 모의 위협실행 도구[1]이다. 세 번째 모듈은 사이버 위협이 실행될 수 있는 네트워크 및 호스트, 서비스 등의 환경을 훈련 시나리오에 맞게 구성하고, 사이버 훈련을 수행할 수 있는 제반 환경을 제공하기 위한 사이버 훈련 환경 구축 도구[3]이다. 3가지 도구의 구성은 Fig 1과 같다.

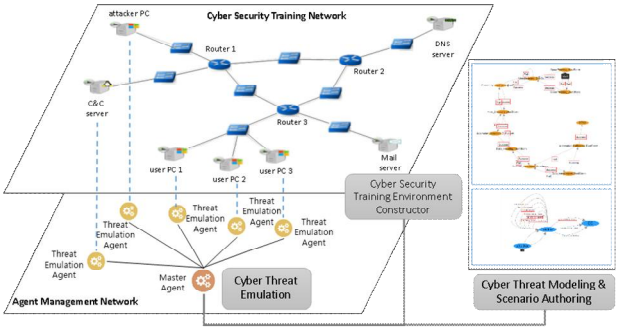


Fig. 1. CyTEA Overview

2. Cyber threat modeling & scenario authoring

사이버 위협 모델링 및 시나리오 저작 도구[2]는 사이버 위협을 모델링하기 위한 최소 행위 단위인 단위위협으로 MITRE의 ATT&CK의 전략(Tactics)과 기술(Technique)을 사용하였다. 개별 단위위협을 실행하는데 필요한 속성 정보는 모의 위협 실행 도구의 스크립트와 맞춰 사전에 정의하고 위협을 저작할 때 입력하여 개별위협의 특성을 반영할 수 있도록 하였다. 모의 위협 저작 도구[2]는 이렇게 생성한 하나하나의 단위위협을 조합하여 사이버 위협을 모델링 할 수 있다. 단위위협 간 연동은 상태 천이 그래프 방식으로 연결된다. 단위위협이 성공 또는 실패할 때 실행될 다음 단위위협을 정하고, 공격을 가하는 호스트, 공격을 당하는 호스트, 결과를 확인하는 호스트를 정의하여 단위위협을 연속적으로 실행하는 방식으로 사이버 위협을 모델링 할 수 있다. 이렇게 저작된 상태 천이 그래프는 하나의 사이버 모의 위협 프로파일이 되며, 단일 위협 프로파일로 사이버 위협을 모델링 할 수도 있고, 다른 프로파일로 천이할 수 있도록 하여 여러 개의 프로파일로 하나의 사이버 위협을 모델링 할 수도 있다.

3. Cyber threat emulation

앞장에서 설명한 모델링과 시나리오를 바탕으로 사이버 모의 위협을 실행하는 사이버 모의 위협 실행 도구[1]는 단위위협을 실행시킬 수 있는 파이썬 기반의 스크립트 코드와 그 실행 결과 수집하고 결과에 따라 다음에 실행될 단위위협을 분기시키는 기능으로 구성된다. 단위위협의 설정된 속성 값은 해당 단위위협의 스크립트 실행 시 입력으로 주어진다. 각 단위위협의 설정 및 실행 스크립트는 플러그인 형태로 사용자가 계속 추가할 수 있도록 개발하였다. 모의 위협 실행 도구는 또한 단위위협의 실행 결과를 수집하는 기능이 있어 결과가 성공인지, 실패인지에 따라 프로파일에서 정의된 다음 단위위협이 실행될 수 있도록 하였다.

사이버 모의 위협 실행 도구는 Fig 1에서와 같이 사이버 훈련 시나리오의 개발 호스트에 설치되어 단위위협을 실행하는 Threat Emulation Agent와 모의 위협에 참여하는 모든 Agent를 관할하고 결과에 따라 실행흐름을 통제하는 Master Agent로 구성된다. 또한, 앞에서 설명한 모의 위협 프로파일에서 설정되는 호스트는 심볼 형태로 정의되며, 모의 위협 실행 도구에서 사이버 훈련 시나리오에서 사용자가 호스트를 각각 지정하면, 심볼을 각 호스트의 정보로 변환하여 실제 모의 위협이 동작될 수 있도록 한다. 이를 통해 다른 네트워크 토폴로지를 갖는 사이버 훈련 시나리오에서도 모의 위협 프로파일을 재사용할 수 있다.

4. Cyber security training environment constructor

사이버 훈련 환경 구축 도구[3]는 사이버 모의 위협이 실행될 수 있는 호스트, 네트워크 및 서비스 등의 환경을 훈련 시나리오 맞게 구성하고, 사이버 훈련을 수행할 수 있는 제반 환경을 제공한다. 사이버 훈련 환경 구축 도구는 사용자가 웹 기반의 캔버스에 호스트 및 네트워크 아이콘을 Drag & Drop으로 배치하고 연결하고, 설정 정보만 입력하면 호스트 및 네트워크 가상화 기술 및 서비스 배포 기술을 이용하여 훈련자가 실제와 유사한 환경을 경험할 수 있는 가상 사이버 훈련환경을 쉽고 빠르게 구축할 수 있도록 하는 도구이다. 또한, 웹 행위, 메일 행위, 자료연동 행위에 대해 사용자를 모의할 수 있는 기능[3]도 제공한다. 이런 사용자 모의 기능을 이용하여 위협을 모의할 때 사용할 수 있다. 이를 통해 사이버 모의 위협 실행 및 전파에서 사용자 취약점으로 활용할 수 있다. 예를 들어 부주의한 메일 열람, 특정 웹페이지 접속을 통한 위협 전파, 망간 접점을 이용한 폐쇄망 침투 등의 모의를 할 수 있다.

IV. Cyber threat modeling and attack emulation method

CyTEA를 이용하여 사이버 위협을 모의하는 과정에서 모의 된 위협과 실제 사이버 위협 간 유사함의 수준과 유효성을 판단하고 개선 방향을 도출하기 위해 본 논문에서는 절차적 유사성과 환경적 유사성, 결과적 유사성의 3가지 정성적 지표를 제시한다. 본 장에서는 사이버 위협을 3가지 지표에 맞춰 모델링 하고 위협 발생을 위한 시나리오를 저작하는 방안에 대해 실제 APT(Advanced Persistence Threat) 형태의 사이버 공격 사례 중 하나인 Operation Dust Storm의 예를 사용하여 제시하였다.

1. Procedural similarity

절차적 유사성은 사이버 위협이 진행된 TTP(Tactical, Techniques, and Procedures) 관점에서의 지표라고 할 수 있다. MITRE ATT&CK Framework에는 실제 있었던 APT 형태의 사이버 공격에 대해 관련 커뮤니티의 공개정보를 기반으로 유사한 TTP를 갖는 여러 Operation Group의 정보를 구축하고 공개하고 있다[6]. 2020년 7월 현재 107개의 Operation Group에 대한 정보를 구축하고 공개하고 있으며[6], 분석되는 커뮤니티에 따라 같은 그룹이 다른 그룹으로 분류될 수 있는 것을 고려하더라도 상당히 많은 사이버 위협에 대한 TTP 분석이 되어 있는 것을 알 수 있다. 여러 커뮤니티에서 분석한 사이버 위협에 대한 TTP 정보와 본 논문에서 모의한 사이버 위협의 TTP를 비교하여 절차적 유사성을 평가할 수 있다.

APT 공격 사례인 Operation Dust Storm[7]의 경우 공격자 호스트와 타겟 호스트 간의 TTP를 간략하게 나타내면 Fig 2(a)와 같다.

2. Environmental Similarity

사이버 위협 별로 사이버 위협이 동작했던 환경과 유사성을 유지할 필요가 있다. 예를 들어 위협코드가 주로 사용하는 도메인 이름이나, C&C 통신에 사용된 IP, 악성코드 유입과 C&C 통신을 위한 기반 환경 등 사이버 위협 별로 달라지는 환경을 분석보고서 등과 비교하여 환경적 유사성을 평가할 수 있다. 하지만, 최대한 유사한 환경으로 구성하되 이를 현재의 사이버 환경, 모의 위협을 사용하는 이유 등을 감안하여 절차적, 결과적 유사성이 확보될 수 있도록 하는 환경적 유사성 평가가 고려되어야 한다. 예를 들어 시간의 흐름에 따라 주로 사용되는 윈도우의 버전이나, 사용되는 취약점은 환경적 유사성보다는 절차적, 결과적 유사성을 고려하여 다른 윈도우 버전, 취약점을 사용하는 것이 더 합당할 것이다.

공격자, 타겟 호스트에 환경적 요소까지 추가하여 Operation Dust Storm에 대한 TTP를 간략하게 표현하면 Fig 2(b)와 같다.

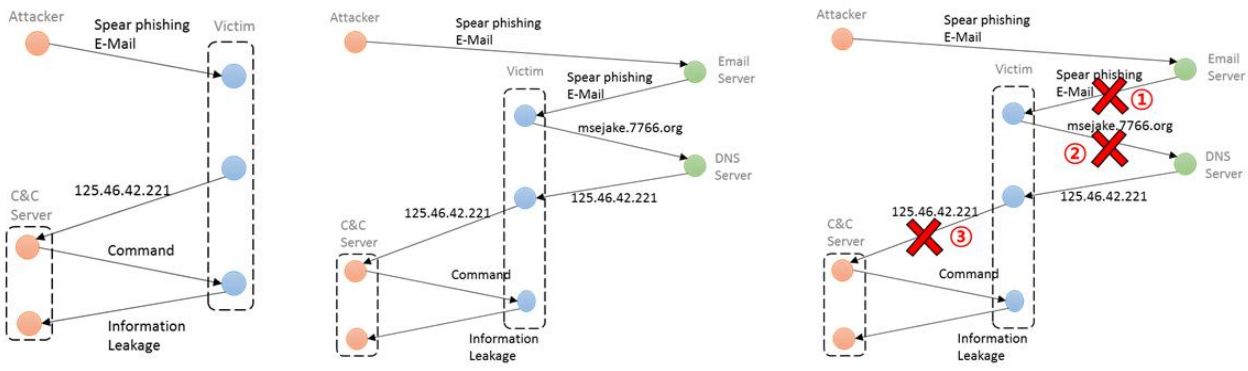
3. Consequential similarity

결과적 유사성은 공격자와 방어자의 관점에서 유사성을 평가할 수 있다. 먼저 공격자 관점의 결과적 유사성은 사이버 공격의 절차에 맞게 수행되면 단계적으로 획득되는 정보나 권한이 실제 사이버 위협과 결과적으로 같아야 하며, 최종적으로는 실제 사이버 위협의 공격 결과와 모의 된 위협의 결과가 같아야 모의가 잘 되었다고 평가할 수 있다.

방어자 관점의 결과적 유사성은 실제 사이버 위협이 있을 때 이를 방어하기 위해 취할 수 있는 방어행위와 이를 통해 얻을 수 있는 결과가 모의 된 위협을 통해서도 같은 행위와 같은 결과를 얻을 수 있어야 한다는 점이다. 대부분의 사이버 위협은 결과적으로 방어행위가 실제 수행되지 못해 실제 결과를 얻을 수 없지만, 그 결과를 예측하는 것은 어렵지 않다.

Fig 2(c)는 Operation Dust Storm에 대해 방어행위를 통해 Operation Dust Storm의 공격행위를 차단할 수 있는 3가지 가장 간단하면서도 보편적으로 실행되는 방어행위를 나타내었다.

①은 Spear phishing E-mail을 사전에 차단, ②는 위협으로 판단되는 도메인을 차단, ③은 정보가 유출되는 목표지 IP를 차단하는 방식이다. 방어행위의 흐름으로 볼 때 IP를 차단(③) 후 해당 도메인을 추적하여 차단(②)하고, 공격코드를 분석하여 공격코드가 유입된 E-mail을 차단(①)하는 방식으로 방어행위가 진행되는 것이 일반적이다고 할 수 있



(a) Attack techniques (b) Procedures including the environment (c) Defense point for the Operation Dust Storm

Fig. 2. Cyber attack and defense procedures of Operation Dust Storm

다. 차단 방법의 효율적인 면이나 범위, 피해를 생각할 때 ①번이 상책, ②번이 중책, ③번이 하책이라고 볼 수도 있어 훈련자 스코어링 등에 이를 반영할 수도 있을 것이다.

사이버 위협을 모의하는 목적은 사이버 보안 기술의 훈련을 위한 것으로 주요 목표가 방어훈련자에게 사이버 공격에 대한 경험과 공격이 진행되는 과정에서 방어행위를 통해 사이버 공격을 무력화하는 경험을 제공하는 것임을 생각할 때 결과적 유사성은 사이버 위협을 모의할 시 가장 중요한 평가 지표라고 할 수 있다.

V. Cyber threat emulation results

CyTEA를 이용하여 모델링한 사이버 모의 위협의 모의 수준과 사이버 방어훈련에서 실제 사이버 위협만큼 유효한지를 확인하기 위해 실제 있었던 APT 공격 중 하나인 Operation Dust Storm 공격에 대해 모델링과 공격 시나리오를 저작하였다. 또 이를 실제 사이버 방어 훈련과 연동하여 훈련자의 방어행위에 따라 기대되는 위협의 차단 효과가 나타나는지는 실험하였다.

1. Cyber threat emulation results for Operation Dust Storm

Operation Dust Storm에 대한 자세한 분석은 [7]을 통해 확인할 수 있으며, MITRE에서도 [7]의 분석 결과를 이용하여 사용되는 기술 리스트와 악성코드 명 등의 정보를 게시하고 있다[6]. 우리는 Operation Dust Storm에 대한 분석보고서와 MITRE에서 게시한 내용을 기반으로 위협행위 순서를 Fig 4와 같이 도출하였다.

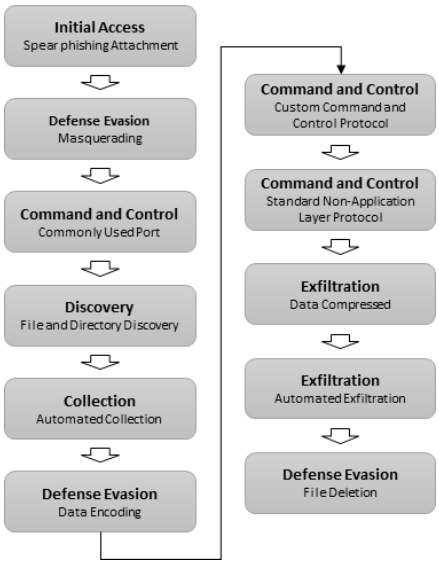


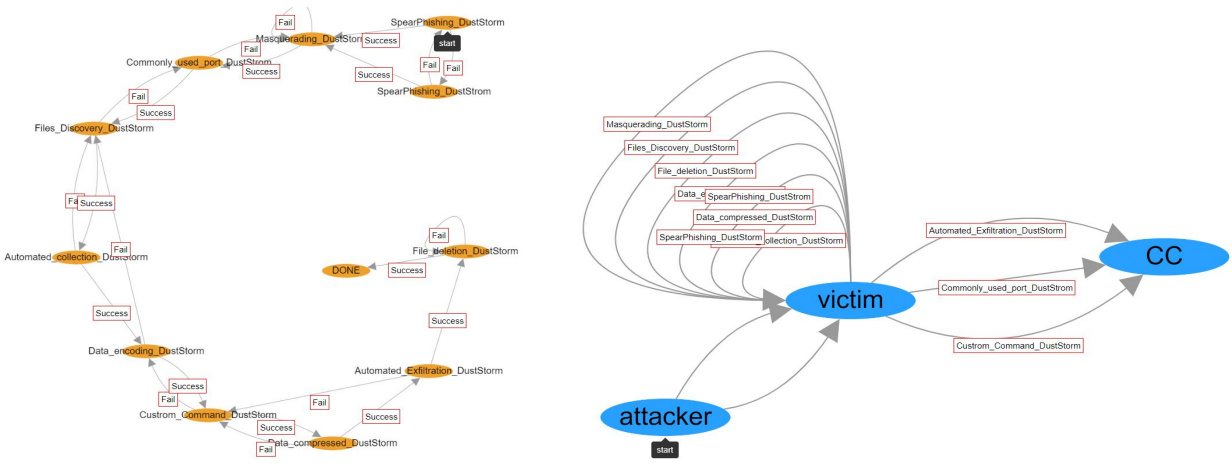
Fig. 4. Unit threat sequence of Operation Dust Storm

Fig 2의 Operation Dust Storm의 타겟 호스트의 외부적 절차뿐 아니라 타겟 호스트 내부적 위협행위까지 분석 결과를 최대한 반영하여 절차적 유사성을 확보할 수 있는 모델링을 수행하였다. 그리고 단위 위협행위 수행결과가 성공이냐 실패이냐에 따라 다음의 위협행위를 달라지도록 하였다.

Fig 4의 Operation Dust Storm의 단위위협 순서를 바탕으로 사이버 위협 모델링 및 시나리오 저작 도구를 이용하여 저작한 결과의 상태 천이 그래프는 Fig 3(a)와 같으며, 호스트 별 단위위협이 실행되는 관계도를 Fig 3(b)와 같다.

2. Cyber security training environment construction results

Operation Dust Storm의 모의 위협이 실행될 수 있는 환경과 이에 대한 사이버 보안 기술의 훈련을 실시할 수 있



(a) State Transition Diagram for Operation Dust Storm (b) host relations for Operation Dust Storm

Fig. 3. Operation Dust Storm modeling result and attack scenario

는 환경을 사이버 훈련 환경 구축 도구[3]를 이용하여 간단히 모의한 결과는 Fig 5과 같다. 보다 현실감을 높이기 위해 필요한 다양한 요소들을 반영할 수 있지만, 사이버 위협 환경 모의 결과에 영향을 미치는 요소로만 구성하였다.

실제 사이버 위협에 대한 방어행위를 수행하는 데 필요한 방어 장비로 Snort 기반 IPS 기능과 iptables 기반의 방화벽 기능을 갖는 UTM 장비를 추가하여 Fig 3에서와 같이 방어훈련자가 보호해야 하는 공격의 타겟 호스트에 대한 침해방지, 침해 후 위협행위를 차단할 수 있는 방어행위를 할 수 있도록 하였으며, 방어 행위에 따라 모의 위협의 결과가 어떻게 달라지는 지를 확인할 수 있도록 하였다.

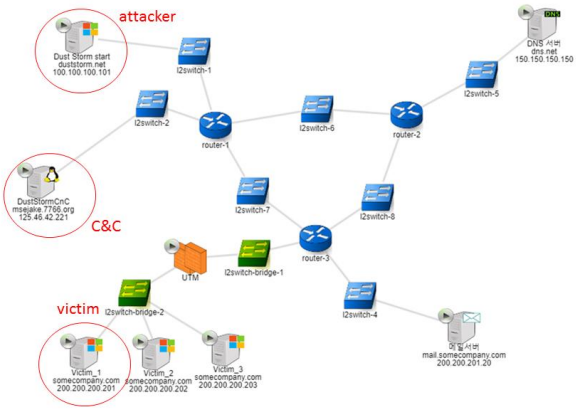


Fig. 5. cyber training environment emulation result

3. Cyber threat emulation results including cyber defense training

3.1 Cyber threat emulation result without defense

사이버 위협과 수행환경에 대한 모의 결과를 이용하여 모의 위협을 실행한 결과는 Fig 7과 같이 정상적으로 동작하는 것을 확인할 수 있었다. 최종적으로 공격 타겟 호스트에 있는 정보를 C&C 통신을 통해 공격자가 탈취한 결과를 C&C 서버 호스트에 제대로 전달한 것을 확인하였다. Fig 6과 7에서 굵은 실선이 위협실행 결과에 따른 흐름이며, 얇은 실선은 실행되지 않은 계획을 나타낸다.

3.2 Result with IP blocking for defense

IP 차단 방어훈련은 Fig 3에서 10번째인 Automated Exfiltration 단계에서 자료가 유출되고 있는 IP를 차단할 수 있는지에 대한 훈련이다. Fig 2(c)에서 ③에 해당하는

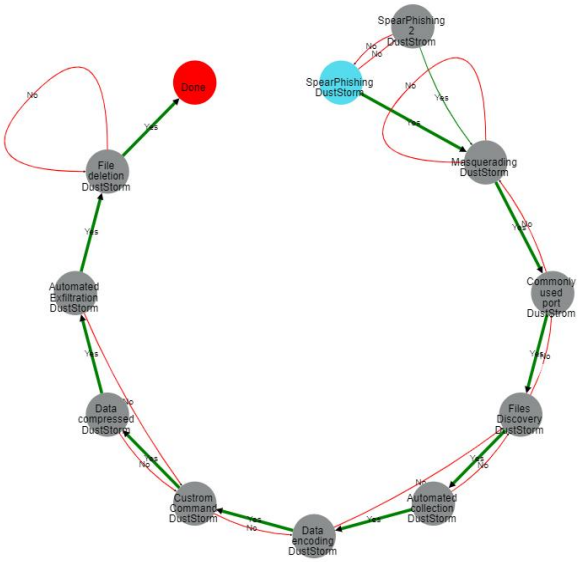


Fig. 7. Treat emulation result for Operation Dust Storm

방어행위로, 방어훈련자는 자료가 유출되는 상황을 탐지하고 자료가 유출되고 있는 IP를 식별하여 차단하는 것으로 [7]에서 분석된 바와 같이 Operation Dust Storm의 악성코드에서 C&C 서버로 사용된 적이 있는 IP인 125.46.42.221을 차단하는 것이다.

이를 위해 Snort 또는 iptables를 이용하여 차단할 수 있으며, 본 논문에서는 UTM 장비에 다음의 차단정책 추가를 통해 차단하였다.

drop tcp any any -> 125.46.42.221 80 (msg:"Target IP Detected"; fast_pattern:only; sid: 1000002)

Fig 8(a)의 모의 위협 결과와 같이 IP가 차단됨에 따라 해당 단위위협이 실패하고, 계획에 따라 Custom Command and Control Protocol 단계로 회귀하여 수행하지만, IP에 대한 차단으로 3회 반복 수행되고 위협행위가 종료되는 것을 확인할 수 있었다.

3.3 Result with domain name blocking for defense

도메인 이름 차단은 Fig 3에서 3번째인 Commonly Used Port를 이용하여 C&C 서버와 처음 통신을 시도하는 단계에서 도메인 이름에 대한 IP를 얻어오는 시점에 위협코드가 사용하는 것으로 판단된 도메인 이름을 차단하는 것이다. Fig 2(c)에서 ②에 해당하는 방어행위로, [7]에서 분석된 바와 같이 Operation Dust Storm에서 사용된

```
Jul  8 18:26:27 osidsips1 snort[1506]: [1:1000002:0] Target Email Detected {TCP} 200.200.201.20:143 -> 200.200.200.201:49976
Jul  8 18:26:32 osidsips1 snort[1506]: [1:1000007:0] Target Domain name Detected {UDP} 200.200.200.201:53315 -> 150.150.150.150:53
Jul  8 18:26:55 osidsips1 snort[1506]: [1:1000008:0] Target IP Detected {TCP} 200.200.200.201:49986 -> 125.46.42.221:80
Jul  8 18:26:55 osidsips1 snort[1506]: [1:1000008:0] Target IP Detected {TCP} 200.200.200.201:49988 -> 125.46.42.221:80
```

Fig. 6. Threat detection messages of Operation Dust Storm on UTM during emulation

적이 있는 것으로 알려진 “msejake.7766.org”라는 도메인 이름을 차단하는 것이다.

DNS 서버로 가는 질의 정보를 차단하기 위해 UTM 장비에 추가되는 차단정책은 다음과 같이 설정하였다.

drop udp any any -> any 53 (msg:“Target Domain name Detected”; content: “msejake.7766.org”; fast_pattern:only; nocase; sid: 1000007)

Fig 8(b)의 결과와 같이 C&C 통신에 실패하고 이전 단계로 회귀하여 실행되지만 정해진 실행 횟수를 초과하여 실패로 종료하는 것을 확인할 수 있었다.

3.4 Result with blocking spear phishing E-mail for defense

Spear phishing은 사회공학적 공격방법 중 하나로 타겟의 흥미를 돋을 수 있는 제목과 내용의 E-mail을 악성링크 또는 첨부파일을 같이 보내는 방식의 공격이다. Spear phishing Attachment 차단은 Fig 3의 첫 번째 단계에서 공격 E-mail이 사용자에게 전달되지 않도록 차단하는 것으로 Fig 2(c)에서 ①에 해당하는 방어행위이다. 구체적으로 E-mail 송신자 또는 첨부파일의 시그니처를 탐지하여 차단할 수 있다.

메일서버에서 또는 UTM에서 차단정책을 추가하여 방어할 수 있으며 이는 훈련 목적에 따라 달라질 수 있으며, 본 논문에서는 UTM 장비에서 차단정책을 추가하였으며, 추가되는 차단정책은 다음과 같이 설정하였다.

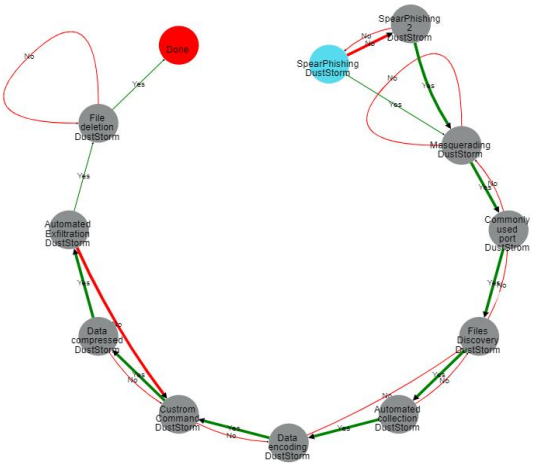
drop tcp 200.200.201.20 any -> any any (msg: “Target Email Detected”; content: “(signature)”; sid: 1000002)

Fig 8(c)의 결과와 같이 Spear phishing이 실패하면 그 이후 어떤 공격도 진행될 수 없으며, APT 공격과 같이 장시간 목표를 갖고 진행되는 공격의 경우, 송신자 메일주소, 메일의 제목과 내용, 첨부파일의 시그니처를 감추고, 바꿔가면서 다른 타겟에게도 공격을 지속할 것이다.

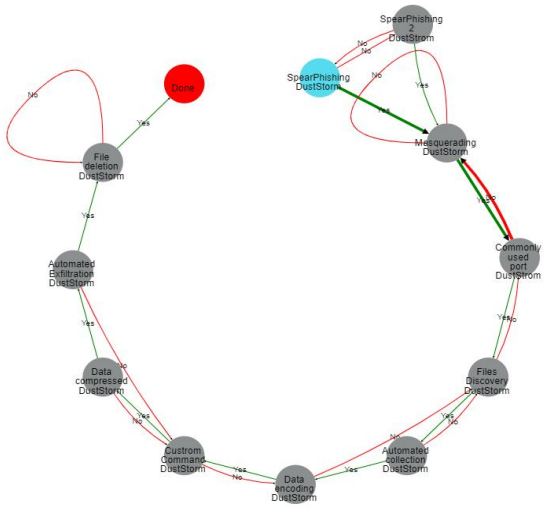
VI. Conclusions

과거 컴퓨터로만 이루어졌던 사이버 공간은 스마트폰, IoT, 생활가전까지 추가되어 우리의 삶에서 뗄 수 없게 되었다. 이런 현실에서 사이버 보안 기술에 대한 교육과 실습, 더 나아가 훈련을 위한 기술 개발이 활발히 진행되고 있다.

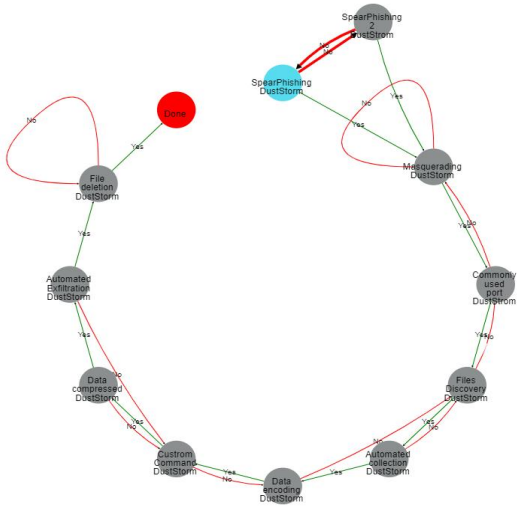
본 논문은 방어 기술에 대한 사이버 보안 기술 훈련을 위해 기존의 수많은 사이버 공격을 기반으로 사이버 위협



(a) Result of IP blocking defense



(b) Result of domain name blocking defense



(c) Result of Spear phishing blocking defense

Fig. 8. Results of defense training

을 모의할 수 있는 도구와 이를 실제 훈련환경에서 실행할 수 있는 도구를 개발하였고 또 이를 실제 사이버 위협의 모의 수준을 가늠하기 위해 절차적, 환경적, 결과적 부분에서 비교하는 평가방안을 제시하였다. 특히 사이버 보안 기술 훈련에 맞게 결과적 부분은 사이버 공격자 관점에서의 결과와 사이버 방어자 관점의 결과를 나누어 비교·분석하는 것을 제안하였다. 또한, 실제 발생하였던 APT 형태의 사이버 공격 중 하나인 Operation Dust Storm에 대한 사례분석을 통해 우리가 개발한 사이버 위협 모의 기술이 실제 사이버 방어 기술을 훈련할 때 실제 위협과 유사한 경험을 제공할 수 있으며, 실제 방어행위를 통해 사이버 위협을 차단할 수 있음을 확인하였다.

ACKNOWLEDGEMENT

This work was supported by Institute of Civil Military Technology Cooperation(UM17312RD3)

REFERENCES

[1] Hong, Suyoun, Kwangsoo Kim, and Taekyu Kim. "The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training." Journal of the Korea Institute of Military Science and Technology Vol. 22, No. 6, pp. 797-805, Nov. 2019

[2] Hyunjin Lee, Youngu Kim, Myung Kil Ahn, “Method for Cyber Attack Scenario Composition using MITRE ATT&CK”, Annual Conference of IEIE 2020, Vol 42, pp. 1103-1104, Jeju, Korea, Jun. 2019

[3] D. H Kim, Y. H. Kim, W. S. Cho, D. S. Kim, J. Y. Kim, Y. H. Kim, M. K. Ahn, C. W. Lee, D. H. Lee, “Software Design Description(SDD) for LVT of Cyber warfare Modeling Technology using LVC(CMT)”, Agency for Defense Development, 314pages, 2017

[4] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. Technical report.

[5] ATT&CK framework, *https://attack.mitre.org/*

[6] Cyber attack group, *https://attack.mitre.org/groups/*

[7] Cross, J. “Operation Dust Storm, Feb. 2016

[8] Bruskin S., Zilberman P., Puzis R., Shwarz S., “SoK: A Survey of Open Source Threat Emulators”, arxiv preprint arXiv:2003.01518, 2020

[9] Red Team Automation, *https://github.com/endgameinc/RTA*

[10] Lee, J.Y., Moon, D.S., Kim, I.K., "Technological Trends in Cyber Attack Simulations", Electronics and Telecommunications Trends, 35(1), pp. 34-48, 2020

[11] Andy Applebaum, Doug Miller, Blake Strom, Chris Korban, and Orss Wolf, “Intelligent, Automated Red Team Emulation”, In Proceedings of the 32nd Annual Conference on Computer Security Applications, ACSAC ‘16, pp 363-373, 2016

[12] Atomic Red Team, *https://atomicredteam.io/*

[13] Ferguson, Bernard, Anne Tall, and Denise Olsen, “National cyber range overview”, In 2014 IEEE Military Communications Conference, pp. 123-128, IEEE, 2014

[14] Pham, Cuong, Dat Tang, Ken-ichi Chinen, and Razvan Beuran, “Cyris: A cyber range instantiation system for facilitating security training.”, In Proceedings of the Seventh Symposium on Information and Communication Technology, pp. 251-258, 2016

[15] Yoo, J. D., Park, E., Lee, G., Ahn, M. K., Kim, D., Seo, S., & Kim, H. K. “Cyber Attack and Defense Emulation Agents”, Applied Sciences, 10(6), 2140, 2020

[16] AttackIQ, *https://attackiq.com/*

[17] Cymulate, *https://cymulate.com/*

Authors

Donghwa Kim received the B.S., M.S. degrees in School of Electrical Engineering from Korea University, Korea, in 2004, 2007. He is currently pursuing the Ph.D. degree in the Department of Computer and Radio Communications Engineering, Korea University. He is currently a senior researcher in Agency for Defense Development. Seoul, Korea. He is interested in cyber security and cyber training system.

Yonghyun Kim received the B.S. and M.S. in Electronic Engineering from Kwangwoon University, Korea, in 1993, in 1995 respectively. He received a Ph.D. in Electronics & Communications Engineering form Kwangwoon University, Korea, in 2013. Since 1995, he has worked in Agency for Defense Development as a Principal Researcher. His research interests include Cyber Security and Wireless Sensor Network.

Myung-Kil Ahn received the B.S. degree in Information and Communication Engineering from the Chungnam National University, in 1997, and M.S. degree in Computer Engineering from the Sogang University, Seoul, Korea in 2003. She is currently pursuing the Ph.D. degree in School of Electrical and Electronics Engineering, Chung-Ang University. She is currently a principal researcher at 2nd R&D institute, Agency for Defense Development, Seoul, Korea. Her research interests include computer security and cyberwarfare modeling&simulation.

Heejo Lee received the B.S., M.S., and Ph.D. degree in Computer Science and Engineering from POSTECH, Koera. He is and Editor of the Journal of Communications and Networks, and the International Journal of Network Management. He is a Professor in the Department of Computer Science and Engineering, Korea University, Korea. Before joining Koera University, he was at AhnLab, Inc. as the CTO from 2001 to 2003. From 2000 to 2001, he was a Post-doctorate Researcher at CERIAS Purdue University, and was a visiting professor at CyLab/CMU in 2010.