https://doi.org/10.33778/kcsa.2020.20.4.091

APT 공격 사례 분석을 통한 사이버 킬체인과 TTP에 대한 연구★

윤 영 인*, 김 종 화**, 이 재 연**, 유 석 대**, 이 상 진***

요 약

과거 해외에서 발생한 APT 공격사례를 사이버 킬체인 모델과 TTP 모델로 분석하였다. 분석 결과 사이버 킬체인 모델은 전체적인 윤곽을 파악하는데 효과적이지만 구체적인 방어 전략을 수립하는 데에는 부적합하며, TTP 모델로 분석해야만 실질적인 방어 체제를 구비하는데 적합함을 알 수 있었다. 이러한 분석 결과를 바탕으로 사이버 공격을 대비하는 관점에서 심층 방어선 구축에 적합한 TTP 모델 관점에서 방어 기술 개발이 필요함을 제시한다.

A research on cyber kill chain and TTP by APT attack case study

Youngin Yoon*, Jonghwa Kim**, Jaeyeon Lee**, Sukdea Yu**, Sangjin Lee***

ABSTRACT

We analyzed APT attack cases that occurred overseas in the past using a cyber kill chain model and a TTP model. As a result of the analysis, we found that the cyber kill chain model is effective in figuring out the overall outline, but is not suitable for establishing a specific defense strategy, however, TTP model is suitable to have a practical defense system. Based on these analysis results, it is suggested that defense technology development which is based on TTP model to build defense-in-depth system for preparing cyber attacks.

Key words : Cyber kill-chain, TTP, APT, Incident Response, Digital Forensics

접수일(2020년 09월 29일), 게재확정일(2020년 10월 23일)

★ 이 논문은 2019년도 한화시스템(주)의 재원을 지원받아 수행된 연구임.

* 고려대학교 (주저자)
** 한화시스템(주)
*** 고려대학교 (교신저자)

1. 서 론

최근 사이버 공격은 과거와 양상이 달라졌다. 과거에는 공격자 개인의 만족이나 금전적인 이익을 위해 불특정 다수를 대상으로 하는 공격이 주를 이루었다면, 최근에는 정치적, 외교적, 군사적, 문화적, 금전적 이익 등 다양한 목적을 달성하기 위해 특정 공격 표적을 집요하게 공격하는 지능형 지속 위협(Advanced Persistent Threat, APT) 공격[1]이 주를 이루고 있다.

APT 공격은 은밀한 공격을 위해 기존 보안제품을 우회하거나 아직 보고되지 않은 취약점을 악용하는 등 고도화된 공격 기법이 사용된다. 공격에 사용되는 악성코드의 탐지 및 분석이 어렵도록 패킹을 하거나 난독화 기술을 사용하며, 네트워크 보안 시스템 우회를 위해 암호 통신을 사용한다. 이러한 특징을 통해 APT 공격은 고도의 기술과 대규모의 예산을 보유한 국가 수준의 조직에 의해 수행된다고 추정할 수 있으며 APT 공격 대응은 이제 국가 안보 차원에서 다루어야 할 만큼 중요한 사안[2]이 되었다.

APT 공격 빈도가 늘어남에 따라 일련의 공격을 표현하는 모델링 기법도 다양하게 제안되고 있다. 사이버 킬체인 모델[3]은 공격자의 관점에서 공격 수행 단계를 7단계로 구분하여 서술하는 것이고 TTP 모델[4]은 공격자의 목적과 그 목적을 이루기 위해 적용된 공격 기법으로 분류하는 것이다.

본 논문에서는 과거에 발생한 해외 APT 공격 사례를 조사하여 사이버 킬체인 모델과 TTP 모델로 분석한다. APT 공격을 방어하는 관점에서 두 모델을 비교하고 침해사고 대응에 더 적합한 모델을 제시한다.

본 논문의 구성은 다음과 같다. 2절에서는 사이버 킬체인 모델과 TTP 모델에 대해 알아보고 해당 모델과 관련된 연구를 제시한다. 3절에서는 과거에 발생한 APT 공격 사례를 사이버 킬체인 모델과 TTP 모델로 분석한다. 4절에서는 두 모델을 비교하고 침해사고 방어 측면에서 평가한다.

2. 배경 지식 및 관련 연구

국방 분야에서 핵 위협에 대응하기 위해 도입한 킬체인은 핵이나 미사일 공격의 징후가 보이면 해당 시설에 대한 탐지와 타격을 하는 공격형 방어시스템이다. 킬체인의 의미를 현대 사이버전에 확대 적용하여 사이버 킬체인이라는 용어를 록히드 마틴 사[3]에서 최초로 정의하였다. 사이버 킬체인은 사고가 발생하기 이전에 미리 감지하고 선제적으로 대응에 나서 침해 시도나 정보 유출 자체를 원천 차단하는 기술을 일컫는다. 사이버 킬체인은 총 7단계로 구성되며 순서대로 정찰(Reconnaissance), 무기화(Weaponization), 전달(Delivery), 공격 거점 생성(Exploitation), 설치(Installation), 명령 및 제어(Command&Control), 목적 수행(Actions on Objecitves) 단계로 구성된다.

정찰 단계에서는 공격 목표와 표적을 조사, 식별 및 선정한다. 무기화 단계는 자동화된 사이버 무기를 준비하는 과정이며, 전달 단계는 표적 시스템에 사이버 무기를 배포하는 과정이다. 공격 거점 생성 단계에서 사이버무기가 최초로 작동되며, 설치 단계에서 표적 시스템에 악성 프로그램이 설치된다. 이후 명령 및 제어 단계에서 공격자와 표적 시스템을 연결하는 원격 제어 채널이 구축되고, 마지막 목적 수행 단계에서 표적 시스템의 정보 수집, 혹은 시스템 파괴 등의 공격을 수행한다. 최근 공격에 빈번히 사용되지만, 사이버 킬체인으로는 표현이 어려운 사회공학적 공격 요소를 접목하여 개선시키는 연구가 진행되었으며[5], 사이버 킬체인 분석을 이용하여 사이버 공격의 원점지를 파악하고 타격하는 연구[2]도 진행되었다.

TTP 모델은 Tactics, Techniques, Procedures 모델의 약자로 공격 목적(Tactics)과 그 목적을 이루기 위한 공격 방식(Techniques), 그리고 그 공격 방식을 달성하기 위한 상세 기법(Procedures)으로 분류한다. MITRE 사[6]에서는 이 TTP모델을 이용해 2017년 MITRE ATT&CK 프레임워크를 제안하였다. 이 프레임워크는 공격자의 목적을 11개로 분류하였고 각각의 목적에 대해 적용 가능한 공격 방식을 정리하였다. 정리된 공격 기법을 적용하여 실제 발생한 공격을 모의하고 이를 통해 새로 등장할 공격에 대한 시스템 위협 분석 방안[7]이 제시되었다, 또한 사이버전을 대비

하여 훈련 목적의 모의 위협 발생기도 ATT&CK 프레임워크를 이용하여 구축[8]하는 등 사이버 공격 방어대책 수립 목적의 연구가 활발히 이루어지고 있다.

3. APT 공격 사례 분석

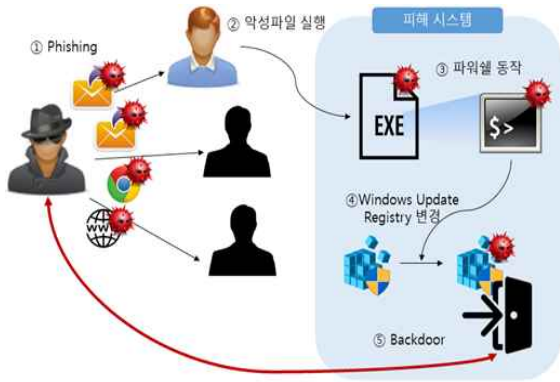
APT 공격은 국가 안보와 관련된 이득을 취하기 위해 일반 사이버 공격에 비해 고도화된 복합적인 기법들을 사용하고 있다. 기본적으로 알려지지 않은 취약점을 사용하거나 보안장비를 우회하고 있으며 휴먼에러를 이용한 스피어 피싱, 워터링 홀 공격과 같은 기법들이 주로 사용된다. 국내의 경우 최근 랜섬웨어 공격과 함께 방위산업체를 대상으로 한 APT 공격이 발생하고 있는 상황이다. 현재까지 분석된 공격 행위를 통해 APT 공격은 더욱 고도화 될 것으로 보인다.

본 절에서는 과거 해외에서 발생한 APT 사례 중에서 4건을 선정하였다. 선정한 APT 사례는 차밍키튼, 폰스톰, 씨엠스타, 블랙오아시스이며, 각 사례에 대한 공격 흐름을 파악한 후 사이버 킬체인 관점 및 TTP 관점으로 분석하였다.

3.1 차밍키튼 APT 공격 사례

이란의 공격자가 미국의 방송사인 HBO를 해킹한 후 미방영 에피소드를 유출하겠다고 협박하면서 6백만 달러를 요구한 사건[9]이다. 이 공격자는 후에 이란의 사이버 단체인 차밍 키튼 소속이라고 밝혀지면서 공격 이름이 차밍키튼으로 명명되었다. 이 해커 조직은 2014년부터 활동해왔으며 이란 내 다양한 단체들과 미국, 이스라엘, 영국 등 타 국가의 단체들을 지속적으로 공격해온 것으로 추정되었다.

공격자는 공격 대상자의 이메일, SNS 계정 등을 사전에 파악하였고, 공격 대상자 혹은 대상그룹이 자주 방문하는 웹사이트를 모방한 피싱 사이트를 사전에 구성하여 피싱 사이트 혹은 피싱 이메일을 이용하여 백도어 실행파일을 다운로드 받도록 유도하였다. 공격 대상자가 백도어 파일을 실행할 경우 악성코드가 동작하기 시작하며 파워쉘을 통해 레지스트리를 변경하여 윈도우 운영체제의 시작 프로그램인 업데이트 서비스를 감염시키는 방식으로 작동한다. 악성코드는 감염된 PC의 정보를 주기적으로 C&C 서버에 보내며 해당 시스템에 상주하면서 공격자가 원하는 공격 행위를 저지른다. 차밍키튼 공격의 흐름도는 (그림 1)과 같다.



(그림 1) 차밍키튼 공격 흐름도

3.1.1 사이버 킬체인 분석

차밍 키튼 공격 사례에서 공격자는 공격 대상의 이메일 주소, 소셜 네트워크 서비스 계정, 자주 방문하는 웹사이트 등의 정보를 정찰 단계에서 수집하였다. 이후 공격자는 악성 페이로드를 포함하는 자바스크립트를 작성하여 문서에 삽입하는 방식으로 무기화하였고, 이를 정찰 단계에서 수집한 공격 대상의 이메일과 소셜 네트워크 서비스 계정으로 전송하였다. 공격 대상이 해당 첨부파일을 실행하면 내부의 악성 자바스크립트 및 페이로드가 활성화 되어 공격 대상의 시스템이 공격자의 거점이 된다. 공격자는 공격 거점을 통해 백도어를 설치하며 지속적으로 통신하여 호스트 이름, 시리얼 번호 등 피해 시스템의 정보를 전송받는다. 공격자는 지속적으로 정보를 수집하며 기밀 데이터에 접근하였고 이를 탈취하였다. 차밍키튼 공격의 사이버 킬체인 분석 내용은 <표 1>과 같다.

3.1.2 TTP 분석

공격자는 공격 대상에 접근하기 위해 대상의 이메일 주소를 수집하여 해당 메일로 피싱 메일을 전송하였다. 공격 대상이 악성코드를 직접 실행하도록 하였

<표 1> 차밍키튼 공격의 사이버 킬체인 분석

사이버 킬체인 단계	단계별 행위
정찰	- 대상의 이메일 수집 - SNS 계정 수집 - 자주 방문하는 웹사이트 수집
무기화	- 악성 페이로드를 포함하는 자바 스크립트 제작
전달	- 악성문서를 첨부한 이메일 전송 - 소셜 네트워크 서비스 계정으로 피싱 메시지 전송
공격거점 생성	- 악성 페이로드 실행
설치	- 페이로드 실행 - 백도어 생성 및 실행
명령&제어	- C&C 서버와 통신 - 호스트 이름, 시리얼 번호 탈취
목적 수행	- 내부 자료 탈취

다. 악성코드가 실행되면 공격 지속성 확보를 위해 윈도우 레지스트리와 시스템 프로세스를 수정하여 시스템 부팅 시 자동으로 악성코드가 동작하도록 만들었다. 이후 알려지지 않은 취약점을 사용하여 권한을 상승하였다. 동작 중인 악성코드가 백신 등 공격 방어수단에 탐지되지 않도록 하기 위해 공격자는 공격 중 생성된 파일을 모두 지우거나 숨김 속성을 부여하였다. 또한 파일 내용을 암호화하거나 인코딩하여 쉽게 알아볼 수 없게 하였다. 공격 대상에 침투한 악성코드는 시스템에 남아있는 크리덴셜 정보를 획득하여 여러 서비스의 인증에 사용하며 공격 대상의 시스템 정보, 네트워크 연결 정보, 사용 중인 서비스 등을 조사하였다. 또한 공격 범위를 넓히기 위해 내부 네트워크에 연결되어 있는 다른 시스템으로 원격 연결을 시도하였다. 공격자는 원격 접속 소프트웨어를 사용하여 원격으로 명령을 내렸고 수집한 정보를 압축하여 원격으로 탈취하였다. 차밍키튼 공격의 TTP 분석 내용은 <표 2>와 같다.

3.2 폰스톰 APT 공격 사례

러시아의 사이버 스파이 그룹으로 알려진 폰스톰이 2017년 미국 국회의원들을 대상으로 공격한 사례[10]

<표 2> 차밍키튼 공격의 TTP 분석

Tactics (목적)	Techniques (방법)
공격 대상 접근	- 사회공학 기법 이용 피싱 - 유효한 계정 사용
악성코드 실행	- 사용자의 실행 유도
공격 지속성 확보	- 부팅 및 로그온 시 자동 실행 - 악성 프로세스 생성 및 수정
권한 상승	- 유효한 계정 사용 - 알려지지 않은 취약점 사용
공격 탐지 회피	- 공격관련 파일 삭제 - 공격관련 파일 및 폴더 숨김 - 공격관련 파일 및 정보 난독화
크리덴셜 획득	- 크리덴셜 덤핑
공격 관련 정보 조사	- 시스템 정보 수집 - 시스템 네트워크 수집 - 시스템 서비스 수집
공격 확산	- 내부자 사회공학적 피싱 - 원격 서비스 사용
데이터 수집	- 수집한 데이터 압축 - 공격 로컬 시스템의 데이터 획득
시스템 명령 및 제어	- 원격 접속 소프트웨어 사용
데이터 유출	- C2 채널 사용한 유출

이다. 공격 대상자를 설정하여 피싱 이메일과 피싱 사이트를 구성해 크리덴셜을 훔치는 간단한 공격이나, 한 번 크리덴셜이 유출되면 추가 공격이 이어지기 때문에 그 위험성이 높다. 금전적 보상이나 테러보다는 정치적 목적으로 공격하는 것이 특징이다.

공격 대상인 정치인 혹은 그 주변인이나 조직에 피싱 이메일을 보내는 방식으로 공격한다. 비밀번호가 종료되니 교체하라는 권고가 담긴 피싱 이메일이나 클라우드에 새로운 파일이 추가되었다는 메일을 보낸 후 로그인 크리덴셜을 획득하는 공격이다. 공격자는 Microsoft Exchange 서버의 계정이 만료되니 갱신하라는 메시지를 보냈으며, OneDrive 시스템에 로그인하도록 유도하는 등 수차례 크리덴셜 획득을 시도하는 움직임을 보였다. 폰스톰 공격의 흐름도는 (그림 2)와 같다.

(그림 2) 폰스톰 공격 흐름도

3.2.1 사이버 킬체인 분석

공격자는 사전에 공격 대상, 혹은 주변 인물들의 이메일 주소를 수집하였고 공격 대상을 속이기 위한 피싱 웹사이트와 피싱 이메일을 생성하였다. 이후 공격 대상에게 피싱 사이트에 회원가입 및 로그인 하도록 유도하였고, 회원가입 시 작성한 이메일 주소로 메일을 보내 악성 첨부파일을 실행하도록 유도했다. 이를 통해 공격 대상이 피싱용 웹사이트에 로그인 할 때 생성된 크리덴셜 정보를 획득하였고 이를 협박, 폭로 등 2차 공격에 활용하였다. 폰스톰 공격의 사이버 킬체인 분석 내용은 <표 3>과 같다.

3.2.2 TTP 분석

공격자는 공격 대상에 접근하기 위해 공격 대상이 사용하는 웹 서비스를 조사하고 그와 유사한 외형의 피싱용 웹 페이지를 제작하였다. 공격 대상이 위조된 서비스를 사용하려고 하면 클라이언트의 취약점을 적용한 악성코드가 실행된다. 또한 공격을 지속하기 위해 웹 브라우저의 확장 프로그램에 위조된 서비스를 등록하였고 이를 원격으로 관리하였다. 공격자는 피싱용 웹 페이지에서 획득한 공격 대상의 계정을 이용하여 공격에 필요한 권한을 획득하였다. 해당 계정을 정상 서비스로 로그인하여 유효한 크리덴셜을 획득 및 탈취했다. 이후 공격 대상의 계정 정보를 이용하여 대상이 사용 중인 또 다른 네트워크 서비스를 찾아내

<표 3> 폰스톰 공격의 사이버 킬체인 분석

사이버 킬체인 단계	단계별 행위
정찰	- 공격 대상의 이메일 주소 수집 - 대상 주변 인물들의 정보 수집
무기화	- 피싱 웹사이트 구성 - 피싱 이메일 제작
전달	- 피싱 사이트 로그인 유도 - 피싱 이메일을 통한 악성 첨부파일 실행 유도
공격거점 생성	-
설치	-
명령&제어	-
목적 수행	- 내부 자료 탈취

<표 4> 폰스톰 공격의 TTP 분석

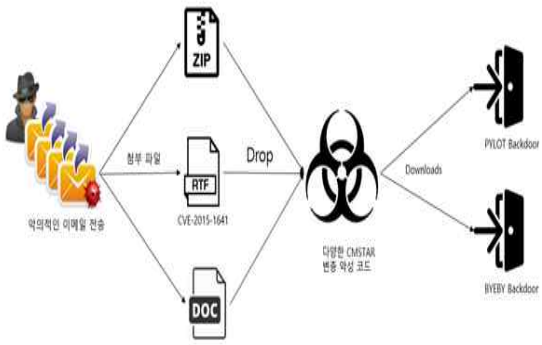
Tactics (목적)	Techniques (방법)
공격 대상 접근	- 사회공학 기법 이용 피싱
악성코드 실행	- 알려지지 않은 취약점 이용
공격 지속성 확보	- 웹 브라우저 애플리케이션 사용 - 원격 서비스 사용
권한 상승	- 유효한 계정 사용
공격 탐지 회피	- 클라우드 기반 서비스 이용
크리덴셜 획득	- 액세스 토근 탈취
공격 관련 정보 조사	- 계정 정보 수집 - 네트워크 서비스 수집
공격 확산	- 내부자 사회공학적 피싱 - 원격 서비스 사용
데이터 수집	- 이메일 관련 정보 수집
시스템 명령 및 제어	- 프록시 사용
데이터 유출	- 웹 서비스를 이용한 유출

면서 공격 범위를 넓혔다. 공격자는 프록시 서버를 기반으로 공격 대상의 웹 메일을 비롯하여 민감한 웹 활동 내역을 탈취하였다. 폰스톰 공격의 TTP 분석 내용은 <표 4>와 같다.

3.3 씨엠스타 APT 공격 사례

2017년 6월부터 8월 사이에 벨로루시 정부에 20개의 피싱 메일이 전송되었고 이를 시작으로 정부 시스템이 장악된 사례[11]이다. 내용은 벨로루시 군대의 전략적 군사 훈련에 대한 메일로 첨부파일 열람을 유도하였다. 메일에 첨부된 파일은 씨엠스타라는 이름의 악성 페이로드를 포함하는 압축파일 및 문서파일 이였다.

씨엠스타는 Microsoft Word 프로그램의 매크로 기능을 통해 전파된다. CVE-2015-1641 취약점을 적용한 문서를 열람할 시 매크로 기능이 자동으로 실행되며 내부 페이로드가 실행된다. 이후 원격 C&C 서버에서 PYLOT, BYEBY 이름의 백도어 프로그램을 다운로드받아 피해자 PC에 설치함으로써 해당 시스템을 장악한다. 씨엠스타 공격의 흐름도는 (그림 3)과 같다.



(그림 3) 씨엠스타 공격 흐름도

3.3.1 사이버 킬체인 분석

공격자는 정찰 단계에서 공격 대상인 정부 기관 직원의 메일을 수집하였다. 또한 어도비 플래시 취약점을 적용한 악성 문서파일을 제작하였고 이를 압축하였다. 공격자는 공격 대상에게 악성 문서와 압축된 파일을 이메일로 전송하여 열람을 유도하였고 공격 대상이 악성 문서를 실행하면 악성 페이로드가 실행되면서 공격 거점이 된다. 이후 백도어가 설치 및 실행되며 이후 주기적으로 C&C 서버와 통신하면서 공격 거점이 된 호스트를 제어하였다. 최종적으로 벨라루스 정부 및 군 기관의 정보를 탈취하였다. 씨엠스타 공격의 사이버 킬체인 분석 내용은 <표 5>와 같다.

<표 5> 씨엠스타 공격의 사이버 킬체인 분석

사이버 킬체인 단계	단계별 행위
정찰	- 공격 대상의 메일 수집
무기화	- 어도비 플래시 취약점을 이용한 악성 문서 및 압축파일제작
전달	- 이메일로 악성 문서 및 압축 파일 전송 - 악성 문서 열람 유도
공격거점 생성	- 악성 문서 열람 시 백도어 생성
설치	-
명령&제어	- C&C 서버와 통신하여 감염 PC 제어
목적 수행	- 공격 대상의 기밀 탈취

3.3.2 TTP 분석

공격자는 공격 대상에 접근하기 위해 사전에 수집한 메일 주소로 악성코드가 첨부된 피싱 메일을 보낸다. 공격 대상이 해당 메일을 열람하고 첨부파일을 실행하면 악성코드가 동작하게 된다. 이후 공격을 지속하기 위해 시스템이 부팅되거나 로그온 시 자동으로 구동되도록 악성코드를 제작하였고 시스템 프로세스로 등록하였다. 또한 필요한 권한을 획득하기 위해 기존에 알려지지 않은 취약점을 악성코드에 적용하였다. 또한 공격이 탐지되는 것을 피하기 위해 정상 프로세스에 주입되어 동작했으며 공격에 사용된 파일과 폴더는 숨김 속성을 적용하거나 쉽게 알아보지 못하도록 난독화 과정을 진행하였다. 악성코드는 시스템에

상주하면서 시스템 정보와 계정 정보, 파일 및 폴더 구조를 모두 조사하였다. 공격자는 공격 확산을 위해 최초 감염 시스템에서 획득한 크리덴셜을 이용하여 원격 접근하였다. 원하는 정보를 획득한 공격자는 설치되어있는 원격 연결 백도어를 이용하여 데이터를 탈취하였다. 씨엠스타 공격의 TTP 분석 내용은 <표 6>과 같다.

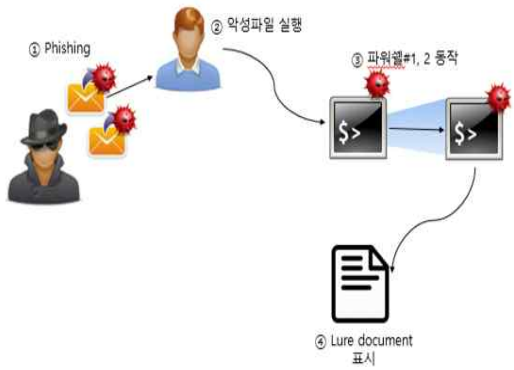
<표 6> 씨엠스타 공격의 TTP 분석

Tactics (목적)	Techniques (방법)
공격 대상 접근	- 사회공학 기법 이용 피싱
악성코드 실행	- 사용자의 실행 유도
공격 지속성 확보	- 부팅 및 로그온 시 자동 실행 - 악성 프로세스 생성 및 수정
권한 상승	- 알려지지 않은 취약점 사용
공격 탐지 회피	- 프로세스 인젝션 - 공격관련 파일 및 폴더 숨김 - 공격관련 파일 및 정보 난독화
크리덴셜 획득	- 알려지지 않은 취약점 사용
공격 관련 정보 조사	- 계정정보 수집 - 파일 및 폴더구조 수집 - 시스템 정보 수집
공격 확산	- 원격 서비스 사용
데이터 수집	- 수집한 데이터 압축 - 공격 로컬 시스템의 데이터 획득
시스템 명령 및 제어	- 데이터 인코딩 - 원격 접속 소프트웨어 사용
데이터 유출	- C2 채널 사용한 유출

3.4 블랙오아시스 APT 공격 사례

블랙오아시스 그룹[12]은 주로 Adobe Flash 및 Microsoft Office 취약점을 이용하여 공격을 수행하는 그룹이다. 2017년 10월 새로운 Adobe Flash 제로데이 취약점을 이용하여 제작한 악성코드를 공격 대상자에게 피싱 메일의 첨부파일로 전송하여 실행을 유도하였다. 이 공격에서 사용된 FinSpy 페이로드는 CVE-2017-11292 및 CVE-2017-8759 취약점을 적용한 페이로드를 사용하였다,

공격 대상자가 이메일을 통해 다운로드 받은 문서 파일을 실행하게 되면 두 개의 파워쉘 스크립트가 실행되어 외부 서버로부터 백도어를 다운로드 받게 되고 자동으로 실행된다. 이 백도어는 C&C서버와 통신하며 추가 악성코드를 다운로드 받고 공격을 수행한다. 블랙오아시스 공격의 흐름도는 (그림 4)와 같다.



(그림 4) 블랙오아시스 공격 흐름도

3.4.1 사이버 킬체인 분석

공격자는 정찰 단계에서 공격 대상의 메일 정보를 수집하였다. 무기화 단계로는 어도비 플래시 취약점을 이용한 악성 페이로드를 생성하였고 이를 문서에 삽입하였다. 전달 단계에서 공격자는 이 악성 문서를 정찰 단계에서 수집한 공격 대상의 이메일로 전송하였고 열람과 다운로드 및 실행을 유도하였다. 악성 문서가 실행되면 내부에 포함되어 있는 악성 페이로드가 파워쉘을 통해 실행된다. 페이로드는 웹에서 백도어를 다운로드하고 실행하여 피해 시스템을 공격 거점으로 만든다. 공격자는 공격 거점의 백도어를 통해 추가 공격에 필요한 악성코드를 다운로드 받은 뒤 확산 및 공격을 진행한다. 다른 PC에 대한 추가 공격은 백도어로 연결된 C&C 서버와 통신하면서 진행된다. 최종적으로 공격자는 C&C 서버로 전송되는 감염된 PC들의 행위 정보를 입수하며 지속적으로 피해 시스템을 감시하게 된다. 블랙오아시스 공격의 사이버 킬체인 분석 내용은 <표 7>과 같다.

3.4.2 TTP 분석

공격자는 공격 대상에 접근하기 위해 사전에 수집

<표 7> 블랙오아시스 공격의 사이버 킬체인 분석

사이버 킬체인 단계	단계별 행위
정찰	- 공격 대상의 메일 주소 수집
무기화	- 어도비 플래시 취약점을 이용한 악성 문서 제작
전달	- 이메일로 악성 문서 전송 - 악성 문서 열람 유도
공격거점 생성	- 파워쉘 코드 실행 - 백도어 다운로드 및 실행
설치	- 백도어를 통해 추가 악성코드 설치
명령&제어	- C&C 서버와 통신하여 감염 PC 제어
목적 수행	- 감시 활동 수행

<표 8> 블랙오아시스 공격의 TTP 분석

Tactics (목적)	Techniques (방법)
공격 대상 접근	- 사회공학 기법 이용 피싱
악성코드 실행	- 사용자의 실행 유도
공격 지속성 확보	- 부팅 및 로그온 시 자동 실행 - 악성 프로세스 생성 및 수정
권한 상승	- 알려지지 않은 취약점 사용
공격 탐지 회피	- 프로세스 인젝션 - 공격관련 파일 및 폴더 숨김 - 공격관련 파일 및 정보 난독화
크리덴셜 획득	- 알려지지 않은 취약점 사용 - 크리덴셜 덤핑
공격 관련 정보 조사	- 계정정보 수집 - 파일 및 폴더구조 수집 - 시스템 정보 수집
공격 확산	- 원격 서비스 사용
데이터 수집	- 수집한 데이터 압축 - 공격 로컬 시스템의 데이터 획득
시스템 명령 및 제어	- 데이터 인코딩 - 원격 접속 소프트웨어 사용
데이터 유출	- C2 채널 사용한 유출

한 메일 주소로 악성코드가 첨부된 피싱 메일을 보낸다. 공격 대상이 해당 메일을 열람하고 첨부파일을 실행하면 악성코드가 동작하게 된다. 또한 공격을 지속하기 위해 시스템이 부팅되거나 로그온 시 자동으로 구동되도록 악성코드를 제작하였고 시스템 프로세스로 등록하였다. 이후 필요한 권한을 획득하기 위해 기존에 알려지지 않은 취약점을 악성코드에 적용하였다. 또한 공격이 탐지되는 것을 피하기 위해 정상 프로세스에 주입되어 동작했으며 공격에 사용된 파일과 폴더는 숨김 속성을 적용하거나 쉽게 알아보지 못하도록 난독화 과정을 진행하였다. 악성코드는 시스템에 상주하면서 시스템 정보와 계정 정보, 파일 및 폴더 구조를 모두 조사하였다. 이후 공격 확산을 위해 최초 감염 시스템에서 획득한 크리덴셜을 이용하여 다른 시스템에 원격 접근하였다. 원하는 정보를 획득한 공격자는 설치되어있는 원격 연결 백도어를 이용하여 데이터를 탈취하였다. 블랙오아시스 공격의 TTP분석 내용은 <표 8>과 같다.

4. 사이버 킬체인 모델과 TTP 모델 비교

사이버 킬체인 모델은 사이버 공격을 대응하는 측면에서 제안된 모델로 사이버 공격을 7단계로 분류한 뒤 하나의 단계를 차단하여 연결 고리를 끊어버리는 개념이다. 그러나 사례 분석을 수행한 결과 7단계로 명확하게 구분하기가 쉽지 않았다. 명확하게 7단계로 분류되는 경우는 차밍키튼과 블랙오아시스 공격 사례였다. 또한 하나의 공격 행위가 여러 단계에 걸쳐있는 경우도 존재하는 등 명확하게 분류하기 어려웠다.

한편 사이버 킬체인으로는 악성코드가 동작하는 방식에 대한 표현이 어렵다. 사이버 킬체인에는 악성코드가 동작한 결과만 표현되고 어떠한 방식으로 악성코드가 동작하였는지는 표현하기 어렵다. 사이버 킬체인으로는 침해사고의 공격 흐름과 결과 등 침해사고 전체을 서술하는 데에는 효과적이지만 침해사고에 대응하는 관점에서는 악성코드의 상세 동작정보 및 적용된 기술을 식별할 수 없어 구체적인 대응방안을 모색하기 어렵다.

TTP 모델은 사이버 킬체인에서 7단계로 명확히 구분짓기 어려웠던 것과는 다르게 11개 택틱에 대하여 테크닉를 서술할 수 있었다. 또한 4개 사례의 TTP가 대체적으로 유사한 내용으로 분석되었다. 공격 대상 접근을 위해 공통적으로 피싱 기법을 사용하였고 피싱을 통해 악성코드를 유포하면서 공격 대상이 직접 악성코드를 실행하도록 유도하는 경향을 보였다. 또한 공통적으로 공격을 지속하기 위해 레지스트리나 자동실행 목록, 시스템 프로세스 등에 악성코드를 등록하였다.

APT 공격 방어 관점에서 기관이나 기업은 MITRE ATT&CK에서 분류한 400여개 테크닉에 대하여 각각을 탐지하는 기술과 대응하는 기술을 확보하고 APT 공격 대응 매뉴얼을 구축할 수 있다. 예를 들어, 공격자는 공격의 지속성 확보를 위해 레지스트리의 자동실행목록에 악성코드를 등록한다. 이것은 레지스트리의 자동실행목록을 지속적으로 모니터링 함으로써 탐지가 가능하며 탐지되었을 때 그것을 삭제하는 것으로 대응할 수 있다. 또한 공격자는 악성코드 혹은 악성 스크립트를 실행시키기 위해 파워쉘을 이용한다. 파워쉘 사용 흔적은 윈도우 이벤트 로그와 파워쉘 자체 로그에 남기 때문에, 해당 로그를 분석하여 공격에 사용된 스크립트의 내용과 그 결과 등을 파워쉘 사용 여부로 알아낼 수 있으며 스크립트 확보가 가능한 경우 공격자의 정보를 확인할 수 있다.

이처럼 특정 테크닉에 대하여 방어 수단이 구비가 된다면 해당 테크닉을 이용하는 공격을 방어할 수 있는 가능성이 생기며 방어 가능한 테크닉이 많아질수록 공격이 성공할 확률은 점점 낮아진다. TTP모델을 이용하면 APT 공격에 대하여 심층방어(defense-in-depth)[13]를 구축할 수 있고 이는 방어 대책 수립에 있어 사이버 킬체인 모델에 비해 더 용이하다고 할 수 있다.

5. 결론

사이버 킬체인은 사이버 공격이 수행되기 위한 과정을 7단계로 분류하는 것이며 그 중 하나 이상의 단계를 막으면 공격을 차단하는 것이 가능하다는 점에 착안한 사이버 공격 대응 모델이다. 그러나 최근 발생한 APT 공격에 대해 사이버 킬 체인 관점에서 분석한 결과 APT 공격을 사이버 킬 체인 단계로 나누는 것은 개념적인 것이며 각 공격이 모두 7단계로 분류되는 것은 아님을 확인하였다. 또한 공격에 대해 방어하기 위해 각 단계 별로 대응방안을 모색하는 것이 아닌 적용된 공격 기법에 맞춰 대응하는 것이 효율적, 효과적으로 대응할 수 있을 것으로 예상된다.

따라서 APT 공격 사례를 사이버 킬체인 모델이 아닌 TTP 모델을 이용한 분석을 통해 공격 단계별 분석이 아닌 공격 기술별 분석을 함으로써 그에 해당하는 방어 기술을 모색하여 효과적으로 방어할 수 있을 것이다. 특히 현대 사이버전을 대비해 한국형 TTP 모델을 이용한 심층방어선을 구축하는 등 국가안보에 이바지할 수 있을 것으로 기대한다.

참고문헌

[1] Seon-Hak Ji, Ji-Yun Park, and Jae-Woo Lee, "은닉형 악성코드를 활용한 공격 사례 분석과 대응 방안에 대한 고찰," 정보보호학회지 Vol. 26, no. 1, pp.92-98, 2016.

[2] Jae-won Yoo, and Dea-woo Park."Cyber kill chain strategy for hitting attacker origin,"한국정보통신학회논문지 Vol. 21, No. 11 pp. 2199-2205, 2017.

[3] Lockheed Martin Corporation, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 2011 Available: "https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf".

[4] Stech F.J., Heckman K.E., and Strom B.E. "Integrating Cyber-D&D into Adversary Modeling for Active Cyber Defense," Cyber Deception: Building the Scientific Foundation, pp.1-22, 2016.

[5] Kyuyong Shin, Kyoung Min Kim, and Jongkwan Lee "A Study on the Concept of Social Engineering Cyber Kill Chain for Social Engineering based Cyber Operations," 정보보호학회논문지 Vol. 28, no. 5, pp.1247-1258, 2018.

[6] MITRE, "Finding Cyber Threats with ATT&CK-Based Analytics," 2017 Available: "https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with% 20att%26ck-based-analytics.pdf"

[7] Myung Kil Ahn, and Jung-Ryun Lee, "Research on System Architecture and Methodology based on MITRE ATT&CK for Experiment Analysis on Cyber Warfare Simulation," 한국컴퓨터정보학회논문지 Vol. 25, no. 8, pp.31-37, 2020.

[8] Hong Suyoun, Kim Kwangsoo and Kim Taekyu, "The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training," 한국군사과학기술학회지 Vol. 22, no. 6, pp797-805, 2019.

[9] Clearsky Cyber Security, "Iranian cyber espionage against human rights activists, academic researchers and media outlets and the HBO hacker connection," 2017 Available: "https://www.clearskysec.com/charmingkitten"

[10] Trend Micro, "Update on Pawn Storm: New Targets and Politically Motivated Campaigns," 2018 Available: "https://www.trendmicro.com/en_us/research/18/a/update-pawn-storm-new-targets-politically-motivated-campaigns.html".

[11] Palo Alto Networks, "Threat Actors Target Government of Belarus Using CMSTAR Trojan," 2017 Avaliable: "https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan".

[12] Kaspersky, "BlackOasis APT and new targeted attacks leveraging zero-day exploit," 2017 Available: "https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732".

[13] NSA/CSS(National Security Agency/Central Security Service) "Defense In Depth", 2010 Available: "https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm".

〔저자소개〕

윤 영 인 (Youngin Yoon)
2015년 2월 고려대학교 컴퓨터통신공학 학사
2015년 3월 ~ 현재 고려대학교 정보보호대학원 박사과정
email : yyi0028@korea.ac.kr

김 종 화 (Jonghwa Kim)
2009년 2월 고려대학교 전기전자전파공학 학사
2009년 1월 ~ 현재 한화시스템 재직
email : jonghwa3.kim@hanwha.com

이 재 연 (Jaeyeon Lee)
2002년 2월 가톨릭대학교 정보통신학사
2004년 2월 광주과학기술원 정보통신석사
2004년 2월 ~ 현재 한화시스템 재직
email : jaeyeon46.lee@hanwha.com

유 석 대 (Sukdea Yu)
2000년 2월 전북대 컴퓨터과학 학사
2002년 2월 전북대 전산통계학 석사
2007년 2월 전북대 컴퓨터통계정보학 박사
2007년 9월 ~ 2009년 9월 Purdue University CS Dept. 박사후 연구원
2010년 4월 ~ 현재 한화시스템 재직
email : sukdea.yu@hanwha.com

이 상 진 (Sangjin Lee)
1989년 10월 ~ 1999년 2월 ETRI 선임 연구원
1999년 3월 ~ 2001년 8월 고려대학교 자연과학대학 조교수
2001년 9월 ~ 현재 고려대학교 정보보호대학원 교수
2008년 3월 ~ 현재 고려대학교 디지털포렌식연구센터 센터장
email : sangjin@korea.ac.kr