# Cyber Kill Chain Framework 기반 APT공격 시나리오 설계 및 구현

신재용*, 최진호*, 이용준*
*극동대학교 해킹보안학과
e-mail:securitykorea@kakao.com, choijinho05@naver.com, 2020032@kdu.ac.kr

# The Design and implement APT attack scenarios based on Cyber Kill Chain Framework

Jae-Yong Shin*, Jin-Ho Choi*, Yong-Jong Lee*
*Department of Hacking Security, Far East University

요 약

美 Lockheedmartin 社는 군사 전략인 Kill Chain 개념을 확장하여 사이버 방어 전략으로 Cyber Kill Chain 7-Step을 제시했다. 이에 본 논문은 시나리오 기반 APT 공격 설계와 구현으로 Cyber Kill Chain 7-Step 단계별 과정을 시나리오를 구축하여 실험했다. Reconnaissance 단계에서 취약한 웹 서버를 탐지하여 취약점을 평가한 결과 디렉터리 리스팅 취약점이 발견됐다. 이후 해당 취약점을 악용하여 Weaponization 단계를 거쳐 최종 악성코드 유포지 및 정보 탈취 경유지로 활용했으며, 최종 악성코드로 연결되는 악성 문서 파일을 첨부하여 Victim 기업 임원진에게 배포했다. 최종 악성코드가 설치되는 Exploitation, Installation 단계를 통해 Victim PC와 C2 Server 간 지속적인 세션 통신으로 기업의 핵심 정보를 탈취했다. 이러한 Cyber Kill Chain Framework 기반으로 APT 공격에 대한 시나리오를 제시하고 실험을 통해 위험성을 검증하였다.

## 1. 서론

美 군수업체인 Lockheedmartin 社는 사이버 공격을 분석하여 사이버 방어 전략인 Cyber Kill Chain 7-Step을 제시했다. Reconnaissance, Weaponization, Delivery 등 7단계를 거쳐 표준화했으며, 공격자는 공격 목표를 달성하기 위해 각각의 단계로 진행된다고 정의했다.

최근 국내 정보 보안 업체에서도 안랩의 지능형 위협 대응 솔루션 MDS와 이글루시큐리티의 통합보안 관제 솔루션 SIEM 등 Cyber Kill Chain 7-Step 방어 전략을 기반으로 보안 위협에 대응하고 있다.

본 논문에서는 공격자 입장에서 Cyber Kill Chain 7-Step 기반으로 APT 공격이 어떤 방식으로 이루어지는지 확인했으며 공격 절차 연구 목적으로 논문을 작성하였다.

## 2. Cyber Kill Chain 7-Step

Cyber Kill Chain 7-Step 설계 및 구현하기에 앞서 Cyber Kill Chain 7-Step 개념에 대해 살펴보기로 한다. 아래의 [표 1]은 Lockheedmartin 社에서 제시한 Cyber Kill Chain 7-Step이다[1].

[표 1] Cyber Kill Chain 7-Step[3]

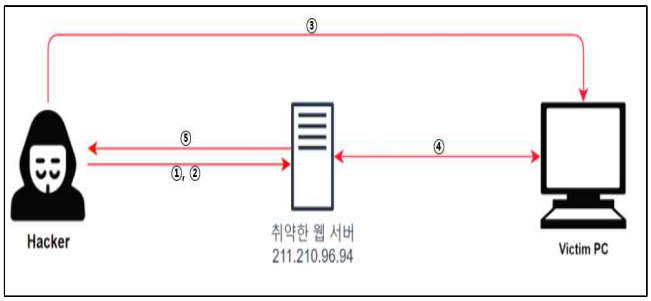
| | |
|---|---|
| Reconnaissance | Harvesting email addresses, conference information, etc. |
| Weaponization | Coupling exploit with backdoor into deliverable payload |
| Delivery | Delivering the weaponized bundle to the victim |
| Exploitation | Exploiting a vulnerability to execute code on victim's system |
| Installation | Install malware on asset |
| Command & Control | Command channel for remote manipulation of victim |
| Action on Objectives | With hands on access, go after objectives |

Reconnaissance 단계는 공격 대상에 대한 탐지, 식별, 선별의 단계로 이메일 주소, 행사 등 정보 조사 단계이다[2]. Weaponization 단계는 취약점과 백도어를 결합하여 Payload에 삽입한다. Delivery 단계는 Weaponization이 된 악성 파일을 이메일, 웹, 저장매체 등을 이용하여 Victim에 전달한다[3]. Exploitation 단계는 Victim PC에서 악성코드를 실행하기 위해 취약점을 이용한다[4]. Installation 단계는 Victim PC에 악성 프로그램을 설치한다. Command & Control 단계는 Victim PC를 원격 조작하기 위해 채널을 열어

지휘한다. Action on Objectives 단계에서는 Victim PC를 완전히 장악하게 된 공격자는 본연의 목적을 달성한다[5].

## 3. 본론

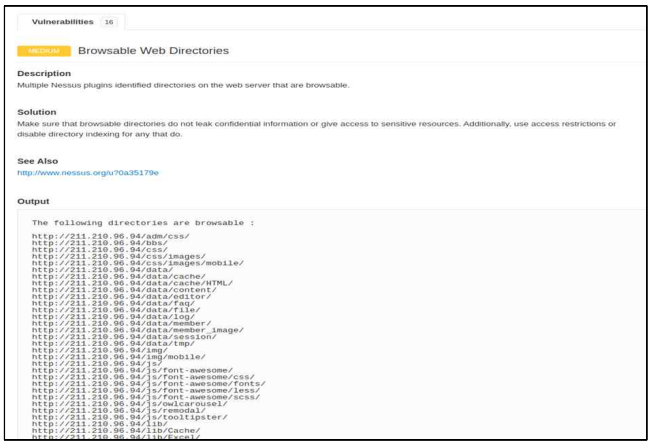
본 논문에서의 공격 시나리오는 [그림 1]과 같이 취약한 웹 서버 취약점을 악용하여 웹쉘 업로드 및 쉘 획득 후 최종 악성코드를 업로드한다. 감염된 C2 Server에 최종 악성코드를 은닉하여 업로드하고, 악성 HWP 문서 파일이 포함된 스피어 피싱 메일을 Victim 기업 임원진에게 전송한다. 악성 HWP 문서 파일에 포함된 링크로 인해 C2 Server로부터 최종 악성코드가 다운로드되고 중요 정보가 C2 Server로 업로드가 되어 Victim PC의 중요 정보를 해커가 다운로드 하게 된다.




[그림 1] APT 공격 시나리오 구성도

### 3.1 Reconnaissance

Victim 기업에 대한 정보 수집과 함께 취약한 웹 서버를 C2 Server로 활용하기 위한 기반을 마련하기 위해 Google 검색과 쇼단(Shodan.io)에서 취약한 웹 서버를 탐색한 뒤, 한국인터넷진흥원 Whois 서비스를 이용해 네트워크 할당 정보와 기관명에 대한 정보를 획득한다.

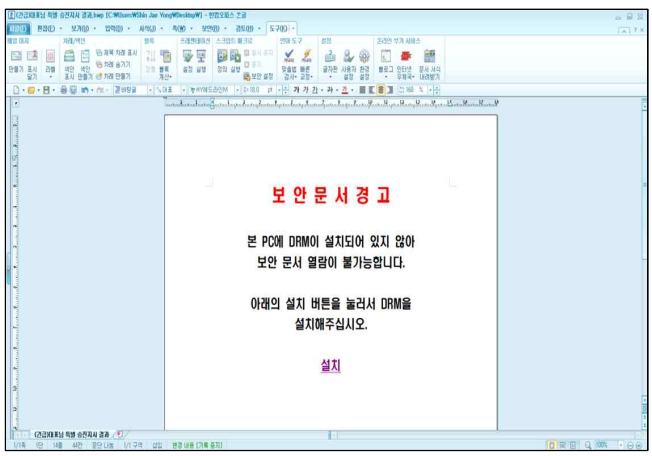



[그림 2] NESSUS로 탐지된 디렉터리 리스팅 취약점

[그림 2]와 같이 취약한 웹 서버 탐지 후 웹 취약점 스캐닝 도구인 Netcraft, Nessus, Burp Suite 등를 사용하여 해당 웹 서버의 취약점을 평가한다. 웹 서버 취약점 평가 결과, 가장 취약성 점수가 높은 취약점인 디렉터리 리스팅 취약점을 악용하였다.

### 3.2 Weaponization

정찰 단계에서 파악한 디렉터리 리스팅 취약점으로 웹쉘 업로드를 시도한다. 본 논문에서는 Kali Linux의 웹쉘 자동화 제작 도구인 Weevely Tool로 난독화되어 Virus total에 검출되지 않는 PHP 웹쉘을 제작하였으며 웹쉘 파일 명을 test.php로 변경하여 업로드한다. 일반적으로 웹 서버 내 파일이 다운로드되는 경로는 확인이 어렵지만 디렉터리 리스팅 취약점으로 업로드된 파일명을 확인할 수 있었다. 웹 서버 내 원본 test.php 파일이 1794477714_320ASfTC_35adea33aa85190f37bbfd570240e07d866d3bc6.php로 파일명이 변경되어 /data/file/free/ 디렉터리로 저장되는 것을 확인했다. 저장 디렉터리와 변경된 파일명을 파악하여 쉘 권한 탈취에 성공했으며 웹 서버 장악 후 C2 Server로 악성코드 유포지 및 정보 탈취 경유지 등으로 활용 가능하게 되었다. 그 후 C2 Server에 최종 악성코드인 fonts_install.exe를 업로드하여 웹 서버 내에 은닉하였으며 아래의 [그림 3]과 같이 한컴오피스 한글 문서에 삽입하였다. Victim이 위장 문서를 실행한 뒤 설치 버튼을 클릭하게 되면 C2 Server에 은닉한 최종 악성코드인 fonts_install.exe가 자동적으로 다운로드하게 된다.




[그림 3] 보안문서경고로 위장한 악성 HWP 문서

### 3.3 Delivery

정찰 단계에서 [그림 4]와 같이 수집한 Victim 기업의 임원진 성명으로 사칭 및 무기화된 악성 문서 파일을 첨부하여 기업 메일로 스피어 피싱 메일을 전송한다.


[그림 4] Reconnaissance 단계에서 수집한 Victm에게 메일 전송

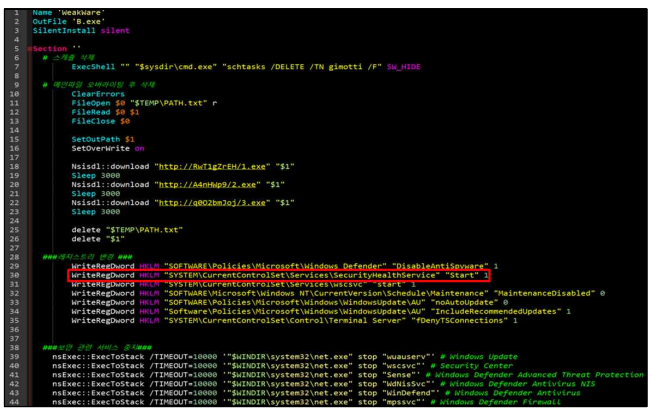
## 3.4 Exploitation

전달 단계에서 [글미 5]와 같이 다운로드한 악성 HWP 문서 파일 내 설치 버튼을 통해 악성 링크로 기업 임직원이 접속하여 최종 악성코드 파일인 fonts_install.exe을 다운로드하게 된다.


[그림 5] 악성 링크를 통해 최종 악성코드 다운로드

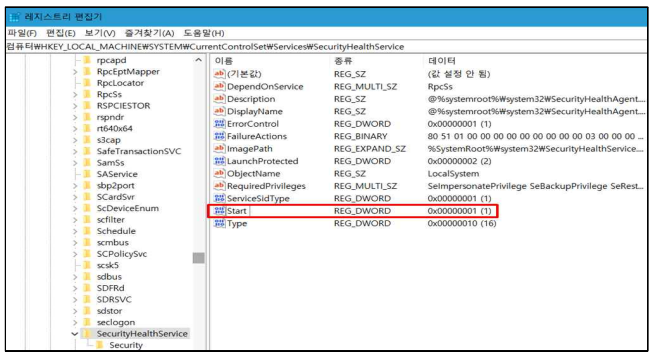
## 3.5 Installation

Victim PC에 최종 악성코드를 설치한다. [그림 6]과 같이 다운로드한 최종 악성코드 파일인 fonts_install.exe의 소스코드를 확인하면 추가 악성파일 다운로드 및 레지스트리, 윈도우 서비스를 오염시키는 코드를 확인할 수 있다.




[그림 6] fonts_install.exe 소스코드 분석

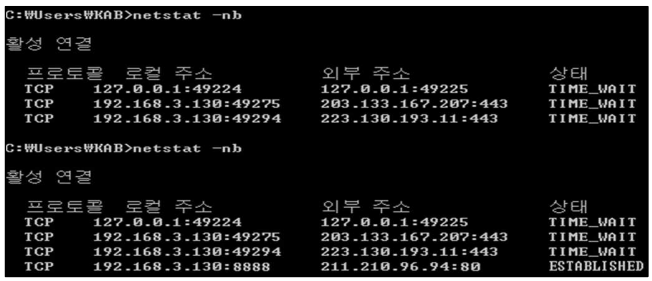
[그림 7]을 통해 실제 악성코드로 인해 감염된 Victim PC의 레지스트리 내 변조된 레지스트리 값을 확인할 수 있다.




[그림 7] Victim PC 레지스트리 변조 확인

## 3.6 Command & Control

공격자는 최종 악성코드 파일로 장악한 Victim PC를 원격 조작하기 위해 세션을 열어 통제한다. 그 후 지속적인 정보 탈취 및 시스템 파괴 목적으로 C2 Server와의 통신을 위해 [그림 8]과 같이 Victim PC의 세션을 유지한다.




[그림 8] Victim PC와 C2 Server 간 세션 유지 확인

## 3.7 Action on Objectives

공격자는 Victim PC와 C2 Server 간 세션 유지로 인한 지속적 정보 유출 혹은 시스템, 데이터 파괴 단계이다. 공격자는 APT 공격 시도 간 본연의 목적인 중요 정보 탈취를 위해 [그림 9]와 같이 지속적인 세션을 유지했다. 마지막으로 추가적인 악성 파일을 다운로드할 수 있도록 악성 파일 유포지인 C2 Server에 업로드함으로써 공격자가 추가적인 악성 행위가 가능한 환경을 구성했다.


[그림 9] C2 Server Victim 내 중요파일 업로드

## 4. 결론

[표 2]에서 본 논문에서 실험한 Cyber Kill Chain 7-Step에 따르는 APT 공격에 대한 시나리오 및 실험 결과를 보여준다. 이처럼 공격자는 웹 서버 취약점을 악용하여 취약한 웹 서버에 웹쉘 업로드 및 쉘을 획득하는 단계를 거쳐 웹 서버 게시판에 최종 악성코드 파일을 은닉하여 업로드했다. 이후 장악한 C2 Server를 운영함과 동시에 악성 문서 파일이 포함된 스피어 피싱 메일을 Victim에게 전송했다. 악성 문서 파일에 포함된 링크로 인해 C2 Server로부터 Victim PC에 최종 악성코드 다운로드가 설치되어 감염되었다. 이로 인해 Victim PC에 존재한 중요 데이터가 지속적으로 C2 Server로 업로드가 되어 탈취된 중요 정보를 공격자가 다운로드 받아 정보 유출이 발생했다.

[표 2] Cyber Kill Chain 7-Step 기반 APT 공격 단계별 수행

| | |
|---|---|
| Reconnaissance | Victim 기업에 대한 이메일 주소 정보 수집<br>취약한 웹 서버 탐색<br>웹 서버 취약점 평가<br>웹 서버 취약점 악용 |
| Weaponization | 웹쉘 제작 및 권한 탈취<br>최종 악성코드 C2 Server 업로드 & 은닉<br>악성 HWP 파일 제작 |
| Delivery | 타겟 기업 임원진에게 악성 HWP 파일 전송 |
| Exploitation | 한컴오피스 취약점을 악용한 악성 문서 파일 열람<br>최종 악성코드 다운로드 및 실행 |
| Installation | Downloader & Dropper 기능이 있는 최종 악성코드로 인한 레지스트리 및 윈도우 서비스 오염 |
| Command & Control | Victim PC와 C2 Server와 세션 연결 후 중요 정보 C2 서버로 전송 |
| Action on Objectives | 지속적인 세션 유지 및 정보 탈취 |

### 참고문헌

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[2] S. Y. Min, C. S. Jung, K. H. Lee, E. S. Cho, T. B. Yoon,S. H. You, “Design of Comprehensive Security Vulnerability Analysis System through Efficient Inspection Method according to Necessity of Upgrading System Vulnerability”, Journal of the Korea Academia-Industrial , Vol.18, No.7, pp.1-8, 2015. DOI: http://dx.doi.org/10.5762/KAIS.2017.18.7.1

[3] K. L. Chiew, K. S. C. yong and C. Tan, "A survey of phishing attacks: their types, vectors and technical approaches", Expert Systems with Applications, vol 106, pp. 1-20, 2018. https://doi.org/10.1016/j.eswa.2018.03.050

[4] I. Qabajeh, F. Thabtah and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishig techniques", Computer Science Review, vol. 29, pp. 44-55, 2018.

[5] J. Y. Kim, S. J. Bu and S. B. Cho, "Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders", Information Sciences, vol. 460, pp. 83-102, 2018. https://doi.org/10.1016/j.ins.2018.04.092