*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.28, NO.5, Oct. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.5.1247

# 사회공학 사이버작전을 고려한 사회공학 사이버킬체인 개념정립 연구*

신 규 용,† 김 경 민, 이 종 관‡
육군사관학교 사이버전 연구센터

# A Study on the Concept of Social Engineering Cyber Kill Chain for Social Engineering based Cyber Operations*

Kyuyong Shin,† Kyoung Min Kim, Jongkwan Lee‡
Cyber Warfare Research Center at Korea Military Academy

요 약

록히드 마틴社에서 제안한 사이버킬체인은 사이버 공격절차를 7단계로 표준화하고, 각 단계별로 적절한 대응방안을 제시함으로써 궁극적으로 공격자가 공격목적을 달성하지 못하도록 하는 사이버작전 수행 간 방어에 대한 방법론을 제공한다. 이와 같은 사이버킬체인 모델을 활용하면 기존의 방법들로는 대응하기 어려웠던 지능형 지속공격(APT)에 보다 효과적인 대응이 가능하다는 장점이 있다. 하지만 최근의 사이버작전은 목표시스템을 직접 공격하는 기술적 사이버작전보다는 목표시스템 관리자나 사용자의 취약점을 통해 목표시스템을 우회적으로 공격하는 사회공학 사이버작전의 비중이 늘어가고 있는 추세이다. 이런 상황에서 기술적 사이버작전을 방어하기 위한 기존의 사이버킬체인 개념만으로는 사회공학 사이버작전에 효과적으로 대응할 수 없다. 따라서 본 논문에서 우리는 사회공학 사이버작전에 효과적으로 대응할 수 있는 사회공학 사이버킬체인에 대한 개념을 정립하고자 한다.

ABSTRACT

The Cyber Kill Chain originally proposed by Lockheed Martin defines the standard procedure of general cyber attacks and suggests tailored defensive actions per each step, eventually neutralizing the intent of the attackers. Defenders can effectively deal with Advanced Persistent Threat(APT)s which are difficult to be handled by other defensive mechanisms under the Cyber Kill Chain. Recently, however, social engineering techniques that exploits the vulnerabilities of humans who manage the target systems are prevail rather than the technical attacks directly attacking the target systems themselves. Under the circumstance, the Cyber Kill Chain model should evolve to encompass social engineering attacks for the improved effectiveness. Therefore, this paper aims to establish a definite concept of Cyber Kill Chain for social engineering based cyber attacks, called Social Engineering Cyber Kill Chain, helping future researchers in this literature.

**Keywords:** Cyber Operations, Social Engineering, Cyber Kill Chain, Social Engineering Cyber Kill Chain

## I. 서 론

최근 우리군은 북한의 핵·미사일 공격에 대비해 한국형 3축 체계 구축을 위해 노력하고 있다[1]. 한국형 3축 체계는 핵·미사일 공격 징후가 명확할 경우 미사일 발사 시설들에 대한 선제타격을 위한 킬

Received(05. 17. 2018), Modified(1st: 07. 03. 2018, 2nd: 08. 03. 2018), Accepted(08. 10. 2018)
* 본 논문은 2018년 화랑대연구소의 지원을 받아 수행되었음

† 주저자, kyshin@kma.ac.kr
‡ 교신저자, jklee64@kma.ac.kr(Corresponding author)

체인(Kill Chain), 이미 발사된 미사일에 대해서는 지상에 도달하기 전에 요격하기 위한 한국형 미사일 방어(Korea Air and Missile Defense, KAMD), 그리고 북한이 핵·미사일을 사용했을 경우 김정은을 포함한 북한의 주요 인물 및 핵심시설에 대한 보복을 위한 대량응징보복(Korea Massive Punishment & Retaliation, KMPR) 등을 포함한다. 이와 같이 우리 군은 북한의 핵·미사일 공격에 대해서는 공격 단계별로 명확한 개념을 정립하고 대응책을 제시하고 있다. 하지만 북한의 핵·미사일 공격만큼 중요한 사이버 공격에 대한 대비가 상대적으로 미흡한 실정이다.

증가하는 사이버 공격에 대한 대응책과 관련해 최근 록히드 마틴(Lockheed Martin)社는 사이버킬체인(Cyber Kill Chain)을 제안하여 많은 주목을 받고 있다[2, 3]. 록히드 마틴社의 사이버킬체인은 사이버 공격의 경우 일반적으로 정찰, 무기화, 유포, 취약점 공격, 설치, 명령 및 제어, 표적 대상 행동 등의 7단계를 거쳐 이루어진다고 보고 있다. 이때 방어자는 위 7단계 중 어느 한 단계만 차단해도 공격자가 다음 단계로 넘어갈 수 없어 공격목적을 달성할 수 없다는 점에 착안해 각 단계별로 탐지, 차단, 방해, 완화, 기만, 파괴의 6가지 유형의 해결책을 제시하고 있다[4-6].

앞서 설명한 사이버킬체인 모델은 대부분의 사이버작전의 공격단계를 7단계의 일반화된 절차로 정형화하고, 각 단계별로 6가지 유형의 대응책을 제시함으로써 대부분의 사이버작전에 대한 효율적인 대처가 가능토록 했다는데 그 의의가 있다[6]. 하지만 지금까지의 사이버킬체인 상의 대처방안으로 제시된 방안들은 침입탐지시스템(IDS), 침입방지시스템(IPS), 안티바이러스(AV), 방화벽(firewall), 데이터 실행방지(DEP) 등 (전통적인) 기술적 사이버작전에 대한 대응책이 대부분이다[2, 3]. 하지만 이러한 기술적 사이버작전에 대한 대응책만으로는 목표시스템 관리자나 사용자를 대상으로 하는 사회공학 사이버작전(Social Engineering based Cyber Operations)에 대한 대응이 어렵다는 단점이 있다. 예를 들어 시스템 관리자가 공격자의 불법접근을 막기 위해 강력한 패스워드를 설정하였다손 치더라도 해당 패스워드를 포스트잍(post-it)에 작성 후 키보드 뒤에 붙여 놓는다면 '어깨 너머로 훔쳐보기(shoulder surfing)' 혹은 '쓰레기통 뒤지기(dumpster diving)' 등의 사회공학 기법을 활용한 공격에 매우 취약할 수밖에 없다[7-9]. 하지만 기존의 록히드 마틴社의 사이버킬체인 모델의 대응책에는 이러한 사람의 부주의 혹은 취약점을 극복할 수 있는 대응방안이 명확히 제시되어 있지 않다.

한편 최근 연구결과에 의하면 사회공학 기법을 활용한 사이버작전은 꾸준히 증가하고 있다. 예를 들어 대표적인 사회공학 공격기법 중의 하나인 피싱(phishing) 공격은 2017년 3분기와 4분기 사이에 무려 전 세계적으로 74%나 증가한 것으로 알려져 있다[10]. 또한 Roger A. Grimes은 한 사설[11]에서 "패치(patch) 되지 않은 소프트웨어와 사회공학 공격이 우리가 노출된 위협의 거의 전부다."라고 얘기할 정도로 사회공학 사이버작전은 대단히 현실적인 문제이다. 하지만 불행히도 현재까지 제시된 사이버킬체인 상의 대응책은 기술적 사이버작전에만 초점이 맞추어져 있으며 사람을 대상으로 하는 사회공학 사이버작전에 대한 대응책은 상대적으로 미흡한 실정이다. 따라서 본 논문은 사회공학 사이버작전에 효과적으로 대응할 수 있는 사회공학 사이버킬체인(Social Engineering Cyber Kill Chain)에 대한 개념을 정립하고 적용방안에 대해 논의한다.

본 논문의 구성은 다음과 같다. 먼저 Ⅱ장에서는 사이버킬체인과 사회공학 사이버작전의 개념 및 의의에 대해 살펴본다. Ⅲ장에서는 사회공학 사이버킬체인의 개념을 정립하고, Ⅳ장에서는 사회공학 사이버킬체인 적용방안에 대해 논의한다. 마지막으로 Ⅴ장에서는 본 논문의 결론을 맺고, 향후 연구방향을 제시한다.

## Ⅱ. 관련연구

이번 장에서는 Ⅲ장에서 사회공학 사이버킬체인 개념을 정리하기에 앞서 사이버킬체인과 사회공학 사이버작전의 개념과 의의에 대해 살펴보기로 한다.

### 2.1 사이버킬체인의 개념 및 의의

록히드 마틴社의 사이버킬체인은 본래 미 공군의 킬체인 개념을 사이버작전 분야에 적용한 개념으로 침입 킬체인(Intrusion Kill Chain)이란 이름으로 제안되었으며 Fig. 1에서 보는 바와 같이 공격절차와 방어절차로 구분된다[2].

| | Phase | Detect | Deny | Disrupt | Degrade | Deceive | Destroy |
|---|---|---|---|---|---|---|---|
| | | → DEFENCE | | | | | → |
| ↓ ATTACK | Reconnaissance | Web analytics | Firewall | - | - | - | - |
| | Weaponization | NIDS | NIPS | - | - | - | - |
| | Delivery | Vigilant user | Proxy filter | In-line AV | - | - | - |
| | Exploitation | HIDS | Patch | DEP | - | - | - |
| | Installation | HIDS | "chroot" jail | AV | - | - | - |
| | C & C | NIDS | Firewall ACL | NIPS | Tarpit | DNS redirect | - |
| ↓ | Actions on Obj. | Audit log | - | - | QoS | Honeypot | - |

Fig. 1. The Course of Defensive Actions in Different Stages of Cyber Kill Chain(Lockheed Martin[2]).

#### 2.1.1 록히드 마틴社 사이버킬체인 공격절차

록히드 마틴社의 사이버킬체인 공격절차는 정찰, 무기화, 유포, 취약점 공격, 설치, 명령 및 제어, 표적 대상 행동 등의 7단계로 구분되는데, 이는 미군이 1990년대 초 걸프전을 수행하면서 적의 스커드 미사일 등 시한성 긴급표적을 효과적으로 처리하기 위해 개발된 킬체인 개념을 사이버작전에 응용한 개념이다[4]. 정찰(Reconnaissance)은 표적에 대한 조사, 식별, 선정을 위한 단계로 이메일 주소, 사회적 관계, 혹은 특정기술에 대한 정보 등을 수집하기 위해 컨퍼런스 웹사이트나 메일링 리스트 등을 탐색하는 단계이다. 다음으로 무기화(Weaponization)는 자동화된 도구를 배달 가능한 첨부 형태로 원격 트로이 목마(trojan)와 결합해 사이버무기를 준비하는 단계이다. 이때 배달 가능한 첨부문서 형태로는 아도비社의 pdf 파일이나 마이크로소프트社의 오피스 파일이 주로 이용된다. 유포(Delivery)는 만들어진 사이버무기를 목표시스템으로 전송하는 것을 말하는데, 주로 이메일, 웹사이트, 혹은 USB 등이 이용된다. 취약점 공격(Exploitation)은 사이버무기가 목표시스템으로 배달된 후 공격자가 의도한대로 코드(code)가 실행되는 단계로 주로 어플리케이션이나 운영체제의 취약점이 이용된다. 설치(Installation) 단계는 원격접근 트로이목마 혹은 백도어(backdoor)를 희생자 컴퓨터에 설치함으로써 공격자로 하여금 표적시스템 내부 환경에 지속적으로 머무를 수 있는 환경을 조성하는 단계이다. 명령 및 제어(Command and Control, C2) 단계는 공격자가 감염된 시스템을 외부에서 제어할 수 있는 채널을 만들어 원격으로 제어하는 단계이다. 일단 명령 및 제어를 위한 채널이 만들어지면 공격자는 시스템 내부환경에 대한 제어권을 갖게 된다. 마지막으로 표적 대상 행동(Actions on objective)은 앞선 6단계를 통해 제어권을 확보한 이후 계획했던 목적을 달성하기 위한 행동을 취하는 단계이다. 이때 공격자의 목표는 데이터에 대한 기밀성, 무결성, 가용성을 훼손하는 것이다.

#### 2.1.2 록히드 마틴社 사이버킬체인 방어절차

록히드 마틴社는 앞서 설명된 사이버킬체인 공격단계 중 어느 단계라도 차단되면 공격자의 목적이 달성될 수 없다고 보고 각 단계에서 탐지, 차단, 방해, 완화, 기만, 파괴의 6가지 유형의 대응책을 제시하고 있다. 이때 각 유형별로 사용할 수 있는 기술은 Fig. 1에서 보는 바와 같다. 대응책 중 탐지(Detect)는 침입탐지시스템 등을 활용해 적의 공격을 사전에 발견하는 것이고, 차단(Deny)은 침입방지시스템(IPS) 혹은 접근통제리스트(ACL) 등을 통해 적의 공격을 예방하는 것이다. 방해(Disrupt)는 하드닝(hardening), 안티바이러스, 데이터 실행방지 등을 통해 적의 공격을 지연시키는 것으로 주로 적이 공격할 수 있는 시스템 취약점을 감소시킴으로써 실현된다. 완화(Degrade)는 타르핏(tarpit) 등을 활용해 서비스를 의도적으로 지연시킴으로써 공격행위의 효율을 감소시키는 방법이며, 기만(Deceive)은 허니팟(honeypot) 등을 활용해 공격자가 잘못된 판단을 하게 하는 방법이다. 마지막으로 파괴(Destroy)는 공격자 혹은 공격도구가 본래의 기능을 하지 못하도록 무력화시키는 것을 의미한다.

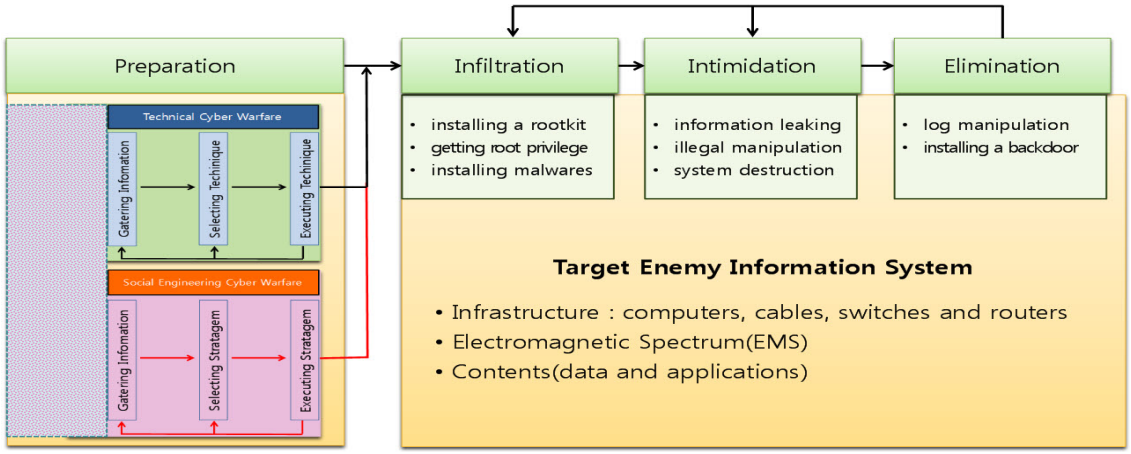


Fig. 2. The Procedure of Technical and Social Engineering Cyber Operations[8].

### 2.1.3 록히드 마틴社 사이버킬체인의 의의 및 제한점

지금까지 설명한 록히드 마틴社의 사이버킬체인 모델은 대부분의 사이버작전 공격단계를 7단계의 일반화된 절차로 정형화하고, 각 단계별로 6가지 유형의 대응책을 제시함으로써 사이버작전에 대한 효율적인 대처가 가능토록 했다는데 그 의의가 있다[6].

이러한 록히드 마틴社의 사이버킬체인 모델도 정찰단계에서 이메일 주소, 사회적 관계, 혹은 특정 기술에 대한 정보 등을 수집하고, 무기화 단계에서 그런 정보들을 효율적으로 활용할 수 있는 사이버 무기를 선택한다는 측면에서 일부 사회공학 사이버작전 요소를 포함하고 있다. 하지만 방어자의 입장을 고려할 때 공격자가 목표시스템을 직접 공격하는 기술적 사이버작전을 수행하고 있는지, 아니면 목표시스템을 관리하는 인원이나 조직을 공격하는 사회공학 사이버작전을 수행하고 있는지에 따라 방어대책이 달라질 수 있기 때문에 사이버작전 공격단계에서 이를 명확히 구분하는 것이 유리하다. 예를 들어 공격자가 이메일을 통한 스피어 피싱(spear phishing)을 하는 경우 기술적 사이버작전 측면에서만 대응한다면 해당 이메일이 목표시스템의 보안솔루션(침입탐지시스템, 침입방지시스템, 안티바이러스 등)만 통과하면 공격에 성공할 수 있다. 하지만 사회공학 사이버작전 측면에서 평소 사용자 교육을 통해 의심되는 메일을 받았을 때의 행동요령 등을 사전에 교육했다면 사용자들이 무분별하게 첨부문서를 클릭하지 않을 것이기 때문에 보다 효과적으로 방어할 수 있다. 또한 2.2.3장에서 보는 바와 같이 일부 사회공학 사이버작전 공격에 대해서는 기존의 록히드 마틴社의 사이버킬체인의 방어대책만으로는 방어가 어려울 수도 있다. 따라서 사회공학 사이버작전 공격절차에 대한 정형화와 이에 대한 대응책을 제시할 필요가 있다.

## 2.2 사회공학 사이버작전의 개념 및 의의

사이버작전의 목표는 적 정보시스템에 침입해 정보를 탈취(기밀성 공격) 하거나, 정보를 불법적으로 변경(무결성 공격) 하거나, 혹은 정보 혹은 정보시스템을 파괴(가용성 공격)하는 것이다[12, 13]. 이러한 목표를 달성하기 위해서 공격자는 기술적 사이버작전과 사회공학 사이버작전을 병행할 수 있다[8]. 이때 본 논문에서는 기존연구[8]의 사이버작전 정의를 준용해 Fig. 2에서 보는 바와 같이 공격준비-목표접근(침입)-위협실시-흔적제거 전체를 (전통적인) 기술적 사이버작전 영역으로 본 뒤 목표시스템을 관리하는 개인이나 조직의 취약점을 공격해 목표시스템에 접근(침입)하는 사이버 공격을 사회공학 사이버작전으로 한정한다[1]. 이러한 측면에서 포트스캐닝 등을 통해 목표시스템의 취약점을 발견한 뒤 패스워드 크래킹 툴을 이용해 시스템의 패스워드를 해킹해 목표시스템에

1) 본 논문에서 사회공학 사이버작전의 목표를 목표시스템에 대한 침입으로 한정한 이유는 대부분의 사회공학 사이버작전 공격무기가 기술적인 요소와 결합되어 있기 때문에 사람 혹은 조직의 취약점을 이용해 시스템에 대한 접근(침입)이 성공한 이후에는 기술적인 사이버작전과 결합해 사이버작전 목표를 달성할 수 있기 때문이다.

침입하는 경우는 전통적인 기술적 사이버작전이라 할 수 있다. 반면에 기술적 사이버작전을 통해 패스워드를 알아내기 어려워 '어깨 너머로 훔쳐보기(shoulder surfing)' 혹은 '쓰레기통 뒤지기(dumpster diving)' 등의 사회공학 공격기법을 통해 관리자의 패스워드를 알아내 목표시스템에 침입하는 경우라면 이는 사회공학 사이버작전이라 할 수 있다.

#### 2.2.1 사회공학 사이버작전의 개념

사회공학 사이버작전은 목표시스템을 기술적으로 직접 공격하기 보다는 목표시스템 관리자나 사용자의 취약점을 우회적으로 공격해 목표시스템에 접근하는 공격이다[7-9, 12-13]. 전술한 바와 같이 사회공학 사이버작전은 목표시스템에 침입하기 위해 활용된다. 이때 만일 기술적인 사이버작전을 통해서 목표시스템에 쉽게 침입할 수 있다면 굳이 사회공학 사이버작전을 수행할 필요가 없을 것이다. 하지만 최근에는 각종 보안기술 및 암호장비 등을 통해 목표 시스템과 컴퓨터 네트워크에 대한 다층보호가 이루어지므로 기술적 사이버작전만으로는 목표시스템에 대한 침입이 어려워졌다. 따라서 목표시스템을 직접 공격하기 보다는 상대적으로 취약한 목표시스템 관리자나 사용자를 공격하는 방향으로 선회하게 되었다[8].

#### 2.2.2 사회공학 사이버작전 수행단계

이 논문의 선행연구[8]의 결과를 준용하여 볼 때 사회공학 사이버작전은 Fig. 2에서 보는 바와 같이 기술적 사이버작전과 병행해 수행되거나 혹은 독립적으로 수행될 수 있다. 이때 공격자는 기술적 사이버작전과 사회공학 사이버작전을 수행하기 이전에 목표시스템 전반에 대한 정보 수집을 수행한다. 이러한 의미에서 사회공학 사이버작전이 수행되는 시점에서는 목표시스템에 대한 정보가 어느 정도 획득되어 있다고 보는 것이 타당할 것이다. 이러한 가정 하에서 사회공학 사이버작전은 Fig. 2에서 보는 바와 같이 ① 정보수집 ② 방략(Stratagem)선택 ③ 방략실행 순으로 수행된다.

사회공학 정보수집(Gathering Information) 단계는 목표시스템 접근에 필요한 정보를 획득하기 위해 목표시스템 관리자나 사용자 정보를 수집하는 단계이다. 사회공학 방략선택(Selecting Stratagem) 단계는 사회공학 정보수집 단계에서 획득된 정보를 바탕으로 목표시스템 관리자나 사용자의 취약점을 공격하기 위해 사회공학 공격기법(즉, 방략)을 선정하는 단계이다. 이때 공격자가 활용 가능한 방략에는 물리적(도청, 어깨너머로 훔쳐보기, 쓰레기통 뒤지기), 사회적(설득, 프리텍스팅, 보상, 역사회공학), 기술적(피싱, 스피어피싱, 스미싱, 파밍, 베이팅, 워터링 홀), 그리고 혼합적(테일게이팅, 비싱) 방법이 있다[7-9]. 사회공학 방략실행(Executing Stratagem) 단계는 사회공학 방략선택 단계에서 선정한 사회공학 공격기법(즉, 방략)을 실행하여 목표시스템에 접근하거나 목표시스템 침입에 필요한 정보를 획득하는 단계이다. 이때 실행된 방략이 실패한다면 정보수집 혹은 방략선택 단계로 돌아간다.

#### 2.2.3 사회공학 사이버작전의 의의

사회공학 사이버작전의 경우 공격자가 선택하는 방략에 따라 기존의 기술적 사이버작전에 대응하기 위한 사이버킬체인 방어대책을 우회할 수 있다. 예를 들어 공격자가 사회공학 사이버작전 기법의 하나인 '설득(persuasion)'을 사용하는 경우를 생각해보자. 만일 공격자가 사적인 영역에서 시스템 관리자 혹은 사용자를 설득해 목표시스템에 저장되어 있는 기밀문서를 복사해 공격자에게 이메일을 통해 전달하도록 만드는데 성공했다고 가정해보자[2]. 이러한 사회공학 사이버작전 공격의 경우 기존의 록히드 마틴社의 사이버킬체인 모델로는 방어가 어렵기 때문에 현 시점에서는 매우 효과적인 공격이 될 수 있다. 이러한 이유 때문에 최근에는 사회공학 사이버작전을 활용한 공격이 지속적으로 증가하고 있다[10].

## III. 사회공학 사이버킬체인 개념 정립

이번 장에서 우리는 기술적 사이버작전뿐만 아니라 사회공학 사이버작전을 아우를 수 있는 사회공학 사이버킬체인 모델을 제안한다.

### 3.1 가정사항(Assumptions)

사회공학 사이버킬체인 모델을 정립함에 있어서 우리는 다음과 같은 두 가지 가정을 한다. 첫째, 현

2) 이러한 종류의 공격은 내부자공격으로 불리기도 하는데 엄밀한 의미에서 내부자공격 또한 사회공학 사이버작전 공격기법의 하나라 할 수 있다.

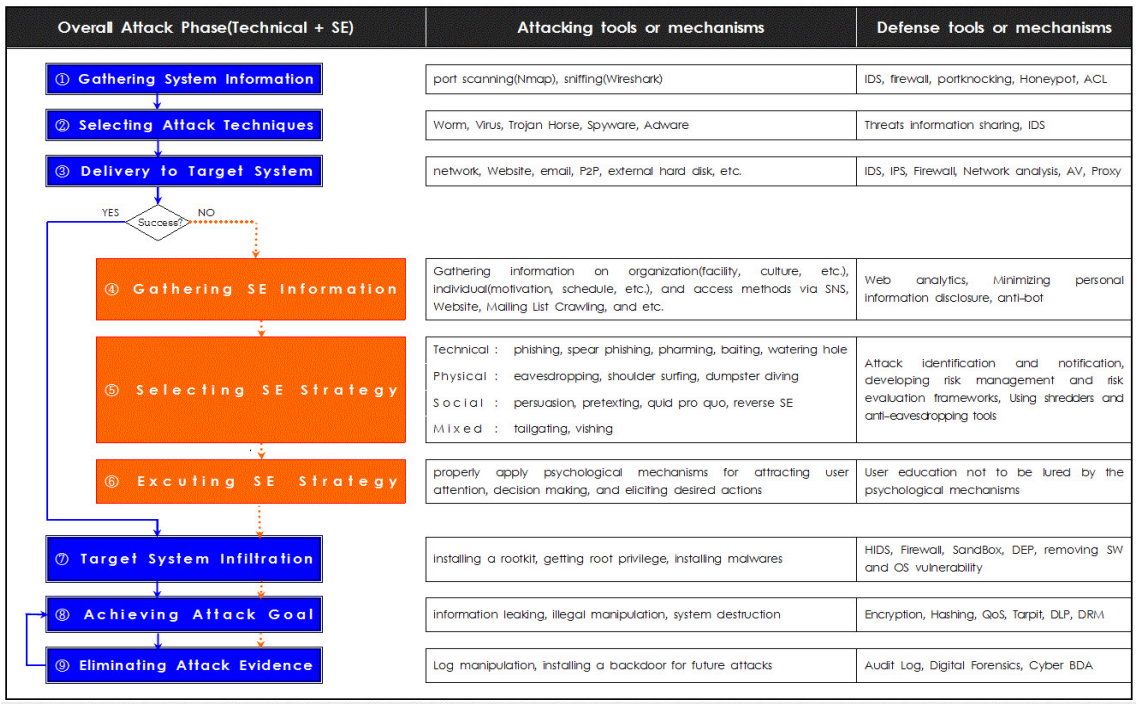


Fig. 3. The Concept and Procedure of the Social Engineering Cyber Kill Chain Model

대의 사이버작전은 물리전과 연계하여 하이브리드전(hybrid warfare)의 일환으로 수행되기 때문에 사이버작전의 목표는 정보작전(Information Operations)을 통해서 이미 어느 정도 구체화가 되어 있다고 가정한다[14]. 따라서 기술적인 사이버작전의 정보수집 단계는 목표시스템의 취약점을 찾기 위한 용도로 수행된다. 둘째, 공격자가 기술적 사이버작전 수행만으로 데이터 탈취, 데이터 불법변경, 목표시스템의 파괴 등과 같은 사이버작전의 목표를 달성할 수 있다면 굳이 사회공학 사이버작전을 수행할 필요가 없다. 즉, 사회공학 사이버작전은 기술적 사이버작전을 통해 목표시스템에 대한 직접적인 공격이 어려울 때 목표시스템 관리자나 사용자의 취약점을 활용해 목표시스템을 우회적으로 공격하고자 할 때 활용된다고 가정한다[8].

### 3.2 사회공학 사이버킬체인 모델

본 논문에서 제안하는 사회공학 사이버킬체인 모델은 Fig. 3에서 보듯이 기술적 사이버작전과 사회공학 사이버작전을 모두 포함한다. 이때 기술적 사이버작전은 ① 시스템 정보수집, ② 공격기술 선택, ③ 목표시스템 배달, ⑦ 목표시스템 침입, ⑧ 공격목표 달성, ⑨ 공격흔적 제거 순으로 수행되며, 사회공학 사이버작전은 ①~③단계에서 기술적 사이버작전이 실패한 경우 ④ 사회공학 정보수집, ⑤ 사회공학 방략선택, ⑥ 사회공학 방략실행, ⑦ 목표시스템 침입, ⑧ 공격목표 달성, ⑨ 공격흔적 제거 순으로 수행된다.

#### 3.2.1 기술적 사이버작전 공격단계

먼저 ① 시스템 정보수집(Gathering System Information) 단계는 nmap과 같은 포트 스캐닝 도구(port scanning tools)나 와이어샤크(wireshark)와 같은 스니핑 도구(sniffing tools)를 활용해 목표시스템에 대한 정보를 수집하는 단계이다. 이때 정보수집의 주안점은 불필요하게 열려서 공격루트로 활용될 수 있는 포트번호(port number)나 사용자 ID와 비밀번호가 포함된 패킷 등 목표시스템의 취약점이다. 다음 ② 공격기술 선택(Selecting Attack Techniques) 단계는 시스템 정보수집 단계를 통해 확보된 목표시스템의 취약성을 공격하기 위한 공격기술을 선택하는 단계이다. 이때 선택 가능한 공격기술에는 웜(worm), 바

이러스(virus), 트로이 목마(trojan horse), 애드웨어(adware), 스파이웨어(spyware) 등 다양하다. 목표시스템의 취약성을 공격할 수 있는 도구가 선택되었다면 ③ 목표시스템 배달(Delivery to the Target) 단계를 통해 해당 공격도구를 목표시스템으로 보내야 한다. 이때 활용할 수 있는 배달 수단으로는 웹사이트(website), 앱(APP), 이메일, P2P, 외장하드, USB, 스틱PC, 카메라, 스마트폰, 무선공유기 등의 물리적 연결 장치들이 있다. 만일 ①~③ 단계를 통해 ⑦ 목표시스템 침입(Target System Infiltration)이 성공해 관리자 권한을 획득하거나, 루트킷(rootkit)이나 원하는 멀웨어(malware) 설치에 성공한다면 공격자는 목표시스템에 대한 제어권을 확보할 수 있다. 따라서 ⑧ 공격목표 달성(Achieving Attack Goal) 단계에서 정보탈취, 불법변경, 시스템 파괴 등 자신이 원하는 공격목표를 달성할 수 있다. 마지막으로 ⑨ 공격흔적 제거(Eliminating Attack Evidence) 단계는 1차적인 공격목표를 달성한 공격자가 향후 같은 시스템에 대한 추가 공격을 용이하게 만들기 위해 백도어(backdoor)를 설치하거나, 공격에 대한 책임추궁을 면하기 위해 공격의 흔적을 지우는 등의 행동을 취하는 단계이다.

### 3.2.2 사회공학 사이버작전 공격단계

과거에는 보안기술이나 보안장비 등이 잘 개발되어 있지 않아서 간단한 기술적 사이버작전 공격도구만으로도 목표시스템에 대한 침입이 가능하였다. 하지만 최근에는 침입탐지시스템, 침입방지시스템, 방화벽, 통합위협관리(UTM), 데이터 유출방지(DLP), 데이터 실행방지, 각종 암호화 기술 등 다양한 보안장비 및 보안기술의 발달로 기술적인 사이버작전만으로 목표시스템을 공략하는 것이 어려워졌다. 이러한 상황에서 목표시스템을 직접 공략하기보다는 목표시스템 관리자나 사용자의 취약점을 통해 목표시스템을 우회적으로 공략하기 위해 사회공학 사이버작전이 활용된다. 이때 사회공학 사이버작전은 앞서 2.2.2절에서 언급한 바와 같이 사회공학 정보수집, 사회공학 방략선택, 사회공학 방략실행 순으로 수행된다[8].

사회공학 사이버작전의 첫 번째 단계는 ④ 사회공학 정보수집(Gathering SE Information) 단계이다. 이때 사회공학 정보수집 단계는 목표시스템에 침입(Target System Infiltration)하기 위해 목표시스템 관리자나 사용자에 대한 정보를 획득하는 단계로 시설 및 문화(조직요소), 개인성격, 동기, 신상, 일정, 대인관계, 업무, 사회현안(개인요소), 그리고 물리적 접촉 여부(접촉요소) 등에 대한 정보를 수집한다. 사회공학 정보수집 단계를 통해 해당 목표시스템 관리자나 사용자에 대한 취약점을 발견하면 그 취약점을 가장 효과적으로 공격할 수 있는 사회공학 공격기법(즉, 방략)을 선택하는 ⑤ 사회공학 방략선택(Selecting SE Strategy) 단계로 넘어간다. 이때 사용 가능한 방략은 Fig. 3에서 보는 바와 같이 피싱, 스피어 피싱, 워터링 홀, 스미싱, 웨일링, 파밍, 베이팅 등의 기술적 방략, 도청, 어깨너머 훔쳐보기, 쓰레기통 뒤지기 등의 물리적 방략, 설득, 프리텍스팅, Quid Pro Quo, Riverse SE 등의 사회적 방략, 그리고 마지막으로 테일게이팅, 비싱 등의 혼합 방략 등이 있다. 목표시스템 관리자나 사용자를 공략하기 위한 사회공학 방략이 선택되면 ⑥ 사회공학 방략실행(Executing SE Strategy) 단계에서는 해당 방략을 실행해 목표시스템에 침입하여야 한다. 이때 사회공학 방략이 효과를 발휘하기 위해서는 목표시스템 관리자나 사용자의 관심을 유도할 수 있어야 하고, 결심과 행동을 이끌어 낼 수 있는 심리기제(psychological mechanisms)를 적절히 활용해야 한다[15]. 만일 사회공학 방략실행 단계를 통해 목표시스템 침입이 성공한다면 ⑦~⑨ 단계는 기술적 사이버작전 공격단계와 동일하게 수행 된다[3]. 하지만 사회공학 방략 실행이 실패한다면 사회공학 정보수집 단계 혹은 사회공학 방략선택 단계로 돌아가 새로운 사회공학 사이버작전을 수행해야 한다.

### 3.2.3 사회공학 사이버킬체인 방어단계

사회공학 사이버킬체인 방어는 Fig. 3에서 보는 바와 같이 각각의 사회공학 사이버 공격단계에 대응하는 다양한 방어 메커니즘을 활용할 수 있다.

먼저 1단계 시스템 정보수집 단계에 대해서는 기본적으로 침입탐지시스템, 방화벽, 포트 노킹(port knocking), 허니팟(honeypot), 접근제어목록

3) 앞서 설명한 바와 같이 대부분의 사회공학 방략이 기술적인 요소를 포함하고 있기 때문에 사용자 혹은 조직의 행위에 의해 목표시스템에 대한 침입이 성공한 이후의 일련의 절차는 (전통적인) 기술적 사이버작전으로 간주해도 무방하다.

(ACL) 등을 통해 정보수집과 불법접근을 차단하고, 경우에 따라서는 사이버 정보·감시·정찰(Cyber ISR)을 통해 선제적으로 대응하여야 한다[4]. 2단계 공격기술 선택 및 3단계 목표시스템 배달 단계에 대해서는 실시간으로 위협정보를 공유하고, 침입탐지시스템, 침입방지시스템, 방화벽, 네트워크 분석, 안티바이러스, 프록시 서버(proxy server) 등을 통해 여건이 보장되는 한 심층방어대책을 구축해야 한다. 4단계 사회공학 정보수집 단계에 대해서는 웹 분석(web analytics) 등을 통해 어떤 공격자가 어떤 정보를 수집하고 있는지 분석해 대응하고, 온라인(웹이나 소셜 네트워크 서비스) 상에 공개하는 개인정보를 최소화함으로써 공격자가 수집할 수 있는 정보를 제한해야 한다. 5단계 사회공학 방략선택 및 6단계 사회공학 방략실행 단계에서 공격자는 목표시스템의 관리자나 사용자의 취약점을 노린다. 따라서 조직적인 측면에서 시스템 관리자는 위협관리 및 위협평가 프레임워크(framework) 등을 구축함으로써 (조직의) 구조적 취약점을 최소화하여야 한다. 사용자 측면에서는 이미 알려진 사회공학 사이버작전 기법 등에 대한 주기적인 교육을 통해서 인적 취약점을 줄여야 한다. 또한 사회공학 사이버작전 발생 시 이를 신속히 발견하고 전파함으로써 피해를 최소화하여야 한다. 나아가 공격자들이 사용자들을 유혹하고 결심하여 행동하게 만드는 심리적 기제들의 동작원리에 대해 사전에 교육함으로써 공격자의 심리적 공격에 대한 내성을 길러야 한다. 실제로 최근 연구동향을 보면 사회공학 사이버작전 공격에 대해 사회공학에 대한 사용자들의 인식증진을 가장 효과적인 대응책으로 제시하고 있다[17. 18]. 7단계 목표시스템 침입단계는 공격자가 목표시스템에 침입해 루트킷 등을 설치함으로써 관리자 권한을 획득하는 단계이므로 호스트 기반 침입탐지(HIDS), 방화벽, 샌드박스(sandbox), 데이터 실행방지 등을 통해 최대한 방어하여야 한다. 또한 이 단계에서 이루어지는 대부분의 공격이 소프트웨어나 운영체제의 취약점을 이용하기 때문에 주기적인 패치(patch) 업데이트를 통해 해당 취약점을 보완해야 한다. 8단계 공격목표 달성 단계에서는 데이터에 대한 암호화, 데이터 손실방지(DLP), 디지털 저작권 관리(DRM) 등을 통해 데이터를 보호하고, 해시함수를 등을 활용해 데이터의 무결성을 보장하며, 품질보증(QoS) 및 타르핏 등을 통해 시스템의 가용성을 확보하여야 한다. 마지막으로 9단계 공격흔적 제거 단계에서는 디지털 포렌식(digital forensics) 기술을 활용해 공격자의 흔적을 찾고, 공격자를 특정할 수 있는 증거를 확보해 추후 책임을 물을 수 있는 근거를 마련해야 한다. 또한 필요할 경우 사이버 전투피해평가(Cyber BDA)를 통해 적의 사이버작전이 아군에게 미친 영향을 분석하고, 피해복구 방안을 마련해야 한다. 또한 공격자의 경우 공격이 성공한 이후에도 향후 공격을 위해 백도어(backdoor)를 설치하는 경우가 많으므로 불필요하게 열려있는 포트와 동작 중인 프로세서 등을 수시로 점검함으로써 백도어를 찾아 제거해야 한다.

## IV. 사회공학 사이버킬체인 적용(안)

이번 장에서는 사이버작전 상황에 대한 사회공학 사이버킬체인 모델 적용가능성을 확인하기 위해 최근에 발생했던 사이버작전 사례를 사회공학 사이버킬체인 모델을 활용해 분석해본다.

### 4.1 사이버 공격 시나리오

국내 유수의 의류판매업체인 A회사와 B회사는 서로 강력한 경쟁관계에 있다. 최근 B 회사는 최신브랜드의 런칭(launching)을 통해 대대적인 성공을 거두었고, 상대적으로 A회사는 어려움에 직면하였다. 이런 상황을 타개하기 위해 A회사는 해커(hacker) K씨를 고용해 B회사의 고위급 임원들에 대한 사원정보를 탈취한 후, 획득된 정보를 바탕으로 B회사의 핵심인력을 회유하기로 결정하였다.

A회사로부터 고용된 해커 K씨는 전통적인 기술적 사이버작전을 통해 B회사 내부 네트워크에 침입할 목적으로 포트스캐너와 스니퍼 등을 활용해 정보를 수집(1단계 시스템 정보수집 단계 실행)하였으나 평소 보안을 중시하는 B회사 CEO의 지시에 의해 B회사의 내부 네트워크는 최신 보안장비 및 보안기술들로 방어되고 있어 기술적 침투가 어렵다는 결론(2단계 공격기술 선택 단계 및 3 단계 목표시스템 배달 단계 실행 및 실패)을 얻었다. 이에 해커 K씨는 B회사의 인사정보를 관리하는 데이터베이스(DB) 서버에 직접 침투하기보다는 사회공학 사이버작전을 통해 인사실무자의 개인 컴퓨터를 통해 우회공격을 감행하기로 결정하였다. 이에 따라 사회공학 사이버작전을 위해 정보를 수집(4단계 사회공학 정보수집 단계 실행)하던 중 해커 K씨는 최근 B회사가 인력을 확충하기 위해 신규사원을 모집하는 것을 알게 되었고, 신규사

원 모집공고를 통해 해당 인사담당자의 이메일 정보를 쉽게 확보할 수 있었다. 이는 입사지원 절차 및 지원 양식 등 B회사의 문화적인 조직요소와 입사지원 담당자의 업무관련성에 대한 정보를 토대로 非물리적인 접촉을 위해 이메일 주소를 수집한 결과라 볼 수 있다. 다음으로는 여러 가지 선택 가능한 사회공학 방략 중에서 이메일 주소를 활용해 해당 인사담당자에게 원격 통제 트로이 목마(Remote Access Trojan)와 같은 악성코드가 담긴 이메일을 보내는 스피어 피싱(spear phishing)을 선택(5단계 사회공학 방략선택 단계 실행) 하였다. 해커 K씨는 B회사 인사담당자의 역할도식[15] 특성과 업무관련성 정보를 이용해 메일을 열람토록 유도하기 위해 메일 제목을 '안녕하세요 열심히 하겠습니다~'라고 작성했으며 '지원합니다.egg'라는 압축파일을 첨부하였다. 이때 해당 압축파일에는 '신분증 사본.jpg'이라고 하는 일반적인 사진파일과 함께 '문의사항(김민지).doc.lnk'라고 하는 트로이 목마 자동실행파일이 숨겨져 있었다[4]. 인사담당자는 별다른 의심 없이 '문의사항(김민지).doc.lnk' 파일을 클릭하였고, 그 결과 해커 K씨가 의도한 원격 통제 트로이 목마가 자동으로 설치되었다(6단계 사회공학 방략실행 단계 실행 및 성공). 이후 해커 K씨는 원격접속을 통해 해당 인사실무자(피해자)의 컴퓨터에 어떤 운영체제(OS)와 보안 소프트웨어가 설치되어 있는지 파악할 수 있었고, 나아가 로컬 IP 주소, 프락시 서버, 네트워크에 연결되어 있는 다른 컴퓨터에 대한 접근정보도 확인할 수 있었다[15]. 스피어 피싱이라고 하는 사회공학 방략을 성공적으로 실행해 B회사의 인사실무자 컴퓨터에 침투한 해커 K씨는 인사실무자 계정정보를 활용해 B회사 인사정보관리 데이터베이스에 접속해 고위급 임원들에 대한 사원정보를 탈취할 수 있었다(8단계 공격목표 달성 단계 실행 및 성공). 마지막으로 해커 K씨는 자신이 B회사 인사정보관리 데이터베이스와 인사담당자의 컴퓨터에 침입했다는 흔적을 지우기 위해 자신의 침입과 관련된 모든 기록(log)을 삭제하였다. 단 향후 동일한 시스템에 침입할 필요가 있을 경우를 대비해 인사담당자의 컴퓨터에는 백도어(backdoor) 프로그램은 남겨두었다(9단계 공격흔적 제거 단계 실행).

4) http://www.boannews.com/media/view.asp?idx=56704

### 4.2 사회공학 사이버킬체인을 활용한 공격 분석

A회사에서 고용한 해커 K씨는 최초 기술적인 사이버작전을 통해 ①~③ 단계를 수행했으나 기술적 사이버작전에 대한 B회사의 보안장비 및 보안기술들이 탄탄해 실패하였다. 따라서 목표시스템을 직접 공격하기 보다는 목표시스템 관리자나 사용자의 취약점을 통한 우회공격인 사회공학 사이버작전을 선택하였다. 때마침 B회사의 채용공고가 있었고, 채용담당 인사실무자를 공격대상으로 사회공학 정보수집을 통해 이메일 주소를 획득한다. 획득된 정보를 바탕으로 볼 때 특정 인사담당자를 공격하는 것이 타당하므로 사회공학 방략으로 스피어 피싱을 선택하였다. 이때 B회사 인사담당자의 관심을 유도하고, 결심과 행동을 이끌어 낼 수 있는 심리기제를 잘 활용해 이메일 문구를 작성함으로써 해당 인사실무자가 첨부파일을 클릭하게 되었고, 결과적으로 원격 통제 트로이 목마를 설치하는데 성공하였다. 사회공학 사이버작전을 통해 인사담당자의 컴퓨터에 성공적으로 잠입한 해커 K씨는 해당 인사담당자의 아이디와 패스워드를 알아내 B회사 인사정보관리 데이터베이스에 접속해 최종 목표인 고위급 임원들에 대한 사원정보를 탈취할 수 있었다. 결국 이번 공격은 B회사 인사담당자(내부인원)의 부주의로 인해 회사의 중요정보를 탈취당한 사회공학 사이버작전 사례라 할 수 있다.

### 4.3 사회공학 사이버킬체인을 활용한 방어 분석

이번 사회공학 사이버작전은 B회사 인사담당자의 이메일을 활용한 스피어 피싱이다. 물론 인사담당자가 신규사원을 모집하는 과정에서 자신의 이메일을 공개하는 것은 어쩔 수 없는 과정이므로 사회공학 정보수집단계에 대한 방어에는 문제가 있다고 볼 수 없다. 단, 사회공학 방략실행 단계에서 메일을 수신한 인사담당자가 아무런 의심 없이 메일에 첨부된 '문의사항(김민지).doc.lnk' 파일을 클릭한 것은 문제라 할 수 있다. 이런 부주의로 인한 사회공학 사이버작전의 피해를 줄이기 위해서 B회사의 보안담당자는 인사담당자를 포함한 조직원들에게 정기적인 보안 교육을 통해 스피어 피싱 공격의 위험성을 주지시켜야 한다. 또한 조직원들에게 주기적으로 연습용 스피어 피싱 메일을 보내는 모의 침투훈련[16]을 통해 경각심을 고취시켜야 한다. 인사담당자 개인적인 측면에서도 송신자의 메일주소

Table 1. The Difference between Lockheed Martin and Proposed Cyber Kill Chain for the Scenario

| Lockheed Martin Cyber Kill Chain | | Proposed Social Engineering Cyber Kill Chain | |
|---|---|---|---|
| Phase | Attack Success? | Phase | Attack Success? |
| ① Reconnaissance | YES | ① Gathering System Information | YES |
| ② Weaponization | YES | ② Selecting Attacking Techniques | YES |
| ③ Delivery | NO (detected by IDS) | ③ Delivery to Target System | NO (detected by IDS) |
| ①′ Reconnaissance(optional) | YES | ④ Gathering SE Information | YES |
| ②′ Weaponization(retry) | YES (attached file obfuscation) | ⑤ Selecting SE Strategy | YES |
| ③′ Delivery(retry) | YES (click the attached file) | ⑥ Executing SE strategy | NO (not click the attached file) |
| ④ Exploitation | YES | ⑦ Target System Infiltration | NO |
| ⑤ Installation | YES | | |
| ⑥ C&C | YES | ⑧ Achieving Attack Goal | NO |
| ⑦ Actions on Obj. | YES | | |
| – | – | ⑨ Eliminating Attack Evidence | NO |

를 자세히 확인하고, 메일에 포함되어 있는 첨부문서나 URL에 대해서는 꼼꼼히 이상유무를 확인한 뒤 실행하는 습관을 생활화하여야 한다.

### 4.4 제안한 사회공학 사이버킬체인 장점 분석

지금까지 살펴본 바와 같이 B회사는 최신 보안장비 및 보안기술들로 다층방어를 실시하고 있기 때문에 기술적 사이버작전에 대한 방어는 상대적으로 우수한 것으로 평가할 수 있다. 이러한 경우 기존의 록히드 마틴社의 사이버킬체인 방어절차를 적용하더라도 해당 스피어 피싱 이메일에 포함되어 있는 첨부문서에 대한 점검을 통해 일부 사회공학 사이버작전을 차단할 수도 있다. 하지만 최근 스피어 피싱 공격동향을 보면 첨부문서를 활용함에 있어 일반적인 실행파일 형태인 .exe 파일을 사용하는 경우 보안솔루션에 의해 쉽게 탐지되므로 압축파일 형태인 .lzh, .rar, .zip 파일에 비밀번호를 걸어 보안 솔루션을 우회하는 기법들이 많이 사용된다[16]. 이러한 경우 기존의 록히드 마틴社 사이버킬체인 방어절차만으로는 첨부문서 형태 변환 및 비밀번호 적용을 통한 공격에 대응하기 어렵다는 단점이 있다.

하지만 본 논문에서 제안하는 사회공학 사이버킬체인을 적용하는 경우 해당 인사담당자가 사회공학 사이버작전(즉, 스피어 피싱) 공격을 이미 예상하고 있기 때문에 충분히 대응할 수 있다. 즉, 해당 스피어 피싱은 인사담당자가 그 이메일에 관심을 갖고, 아무런 의심 없이 첨부파일을 클릭할 때에만 성공할 수 있으므로 인사담당자에 대한 사전 보안교육과 모의침투훈련[16] 등을 통해 의심되는 이메일에 첨부된 문서를 함부로 클릭하지 않도록 평소에 교육한다면 얼마든지 방어할 수 있다.

Table 1.은 앞서 설명된 스피어 피싱 시나리오에 대해 록히드 마틴社의 사이버킬체인과 우리가 제안하는 사회공학 사이버킬체인을 적용하였을 때의 차이점을 보여준다. 즉, 록히드 마틴社의 사이버킬체인을 적용하였을 경우 사회공학적 대응이 부족하기 때문에 스피어 피싱 메일 제목, 내용, 그리고 첨부되는 악성코드 형태를 적절히 조정하는 경우 기술적 보안솔루션을 우회해 공격에 성공할 수 있다. 하지만 본 논문에서 제안하는 사회공학 사이버킬체인 모델을 적용하는 경우 사전에 인사담당자를 포함한 조직원들에게 스피어 피싱에 대한 대응절차를 미리 교육함으로써 인사담당자가 첨부문서를 부주의하게 클릭하는 행동을 방지할 수 있기 때문에 충분히 방어가 가능하다. 이때 사용자 교육은 2.2.2절에서 설명된 모든 사회공학 방략들에 대해서 맞춤형 대응 콘텐츠를 제작해 활용할 필요가 있다.

## V. 결론 및 향후 연구방향

본 논문에서 우리는 기술적인 사이버작전과 사회공학 사이버작전 모두에 대응할 수 있는 사회공학 사이버킬체인 모델을 제안하였다. 제안된 사회공학 사이버킬체인 모델 하에서 사이버 공격은 ① 시스템 정보수집, ② 공격기술 선택, ③ 목표시스템 배달, ④ 사회공학 정보수집, ⑤ 사회공학 방략선택, ⑥ 사회공학 방략실행, ⑦ 목표시스템 침입, ⑧ 공격목표 달성, ⑨ 공격흔적 제거 순으로 진행되며, 기술적인 사이버작전만으로 목표를 달성할 수 있는 경우에는 사회공학 사이버작전 단계(④~⑥)가 생략될 수도 있다. 또한 각 단계별로 맞춤형 방어 메커니즘을 제시함으로써 공격자가 목표를 달성하기 이전에 어느 단계에서라도 공격을 차단하면 적의 의도를 분쇄할 수 있도록 했다.

본 논문에서 제안한 사회공학 사이버킬체인 모델의 경우 록히드 마틴社 등에서 제안한 다른 사이버킬체인 모델들에 비해 사회공학 사이버작전 단계를 명확히 구분함으로써 점차 증가추세에 있는 사회공학 사이버작전에 효과적으로 대응할 수 있도록 했다는데 그 의의가 있다. 향후 우리는 본 논문에서 제안한 사회공학 사이버킬체인 모델을 군사작전에 활용할 수 있도록 [6]에서 제안한 것과 유사하게 방어단계를 작전계획-작전수행-작전종료로 구분해 사이버방어작전 프레임워크를 구체화할 것이다. 또한 사회공학 사이버킬체인 모델을 물리적인 군사작전과 연계해 하이브리드전 수행개념으로 발전시켜 나갈 것이다.

## References


[1] Kang-nyeong Kim, "The Direction and Tasks of Moon Jae-in's Administration's Defense-Military Policy toward North Korea," Korean Association Of Unification Strategy, 2017.

[2] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin, 2011.

[3] Ireneusz Tarnowski, "How to use cyber kill chain model to build cybersecurity?," Case Study, Wroclaw University of Science and Technology, Poland, 2017.

[4] Younghwan Kim and Soojin Lee, "Cyber Kill Chain Strategy for Offensive and Integrated Cyber Operations," Journal of Security Engineering, 2016.

[5] Kwang-Je Kim, Taek-Shin Kang, Jae-Hong Kim, Seunghoon Jung, Jong-Bae Kim, "Cyber Defense Developement Plan based on Cyber Kill Chain," Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, 2017.

[6] Taejong Son and Youngbong Kim, "Cyber kill chain concept and defense application directions," KIDA Weekly, no.1653, 2017.

[7] Wenjun Fan, Kevin Lwakatare and Rong Rong, "Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations," Computer Network and Information Security, pp. 1-11, Jan. 2017.

[8] Kyuyong Shin et. al., "A Study on the Concept of Social Engineering based Cyber Operations," Journal of The Korea Institute of Information Security & Cryptology, vol. 28, no. 3, pp. 707-716, Jun. 2018.

[9] Dong Cheon Shin and Young Hoo Park, "Development of Risk Assessment Indices for Social Engineering Attacks," Journal of Security Engineering, 2017.

[10] Virocom, "18 Cyber Security Trends We Are Watching in 2018," 2018. https://www.vircom.com/blog/18-cyber-security-trends-we-are-watching-in-2018/

[11] Roger A. Grimes, "5 computer security facts that surprise most people," 2017. https://www.csoonline.com/article/3239644/data-breach/5-computer-security-facts-that-surprise-most-people.html

[12] Republic of Korea Joint Chiefs of Staff, "Joint Cyberspace Operations," Joint Field Manual 3-24, 2016.

[13] Joint Publication 3-12, "Cyberspace Operations," 2013.

〔14〕 Young-Tack Park, "The Possibility of N.K.'s Hybrid Warfare and the Development of the Phases," Journal of Defense Policy Studies, 2011.
〔15〕 Jungho Kang et. al., "A study on the relationship between social engineering and cyberspace operations," ROK Cyber Command Technical Report, 2017.
〔16〕 Yu-seung Sohn, Kil-hyun Nam, Sung-cheol Goh, "On the administrative security approaches against spear phishing attacks," Journal of the Korea Institute of Information and Communication Engineering, 2013.
〔17〕 Michael Alexander, "Methods for Understanding and Reducing Social Engineering Attacks," SANS Institute, Apr. 2016.
〔18〕 David Airehrour, Nisha Vasudevan Nair, and Samaneh Madanian, "Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model," Information, May. 2018.

## 〈저자소개〉

신 규 용 (Kyuyong Shin) 종신회원
1996년 03월: 육군사관학교 이학사(전산학)
2000년 02월: 한국과학기술원(KAIST) 공학석사(전산학)
2009년 12월: (미)노스캐롤라이나 주립대(NCSU) 공학박사(전산학)
2010년 02월~현재: 육군사관학교 컴퓨터과학과 교수
2018년 06월~현재: 사이버전 연구센터 사이버전 개념연구실장
〈관심분야〉 분산시스템 보안, 네트워크 보안, 사이버전

김 경 민 (Kyoung Min Kim) 정회원
2003년 03월: 육군사관학교 이학사(운영분석)
2008년 08월: (미)어번(Auburn)대 공학석사(컴퓨터공학)
2016년 12월~현재: 육군사관학교 컴퓨터과학과 교수
2018년 06월~현재: 사이버전 연구센터 연구원
〈관심분야〉 사이버전, 정보화정책, 사물인터넷, 증강현실

이 종 관 (Jongkwan Lee) 정회원
2000년 02월: 육군사관학교 공학사(전자공학)
2004년 02월: 한국과학기술원(KAIST) 공학석사(전자공학)
2014년 02월: 아주대학교 공학박사(NCW공학)
2017년 12월~현재: 육군사관학교 컴퓨터과학과 교수
2018년 06월~현재: 사이버전 연구센터 기획총괄장교
〈관심분야〉 전술네트워크, 사이버전, 그룹키 관리