Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.707

사회공학 사이버작전 개념정립 연구*

신 규 용,† 강 정 호, 유 진 철, 김 지 원, 강 성 록, 임 현 명, 김 용 주‡
육군사관학교

A Study on the Concept of Social Engineering Based Cyber Operations*

Kyuyong Shin,† Jungho Kang, Jincheol Yoo, Jeewon Kim, Sungrok Kang,
Hyunmyung Lim, Yongju Kim‡
Korea Military Academy

요 약

최근 사이버 공격기술을 활용해 목표시스템을 직접 공격하는 기술적 사이버작전 대신 목표시스템을 관리하는 사람의 취약점을 이용해 목표시스템에 침입하는 사회공학 기법이 각광을 받고 있다. 이러한 추세에도 불구하고 사이버작전과 사회공학 기법 사이의 연관관계에 대한 명확한 개념이 정립되어 있지 않아 많은 혼란이 있는 것이 현실이다. 따라서 본 논문에서는 사회공학 사이버작전에 대한 명확한 개념정립을 통해 향후 사회공학 사이버작전에 대한 심도 있는 연구를 위한 토대를 마련하고자 한다.

ABSTRACT

Recently, instead of technical cyber operations that directly attack the target information system by using cyber attack techniques, social engineering techniques that indirectly invade the system by exploiting the vulnerabilities of persons who manage the system are being watched. Despite this trend, there is a lot of confusion because there is no clear concept about the relationship between cyber operations and social engineering techniques. Therefore, this paper aims at establishing a clear concept of a social engineering cyber operation, helping future researchers in this literature.

Keywords: Social Engineering, Cyber Operations, Cyber Warfare

I. 서 론

사이버 공간에서의 보안은 크게 기술적 보안과 인적 보안으로 구분할 수 있다. 기술적 보안은 암호, 접근통제, 시스템 보안, 네트워크 보안 기술 등을 통해 목표시스템을 보호하는 것이고, 인적 보안이란 시스템을 관리하는 사람들을 통제하고 보호함으로써 목표시스템을 보호하는 것을 말한다. 전통적으로 사이버 위협에 대한 보안대책은 주로 기술적 보안에 집중되어 왔으며, 인적 보안은 상대적으로 소홀했던 것이 사실이다. 하지만 이와 같은 기술적 보안과 인적 보안 사이의 불균형은 인간을 대상으로 하는 사이버 공격이 증가하게 되는 단초를 제공하였다. 그럼에도 불구하고 인간을 대상으로 하는 사이버 공격에 대한 연구는 상대적으로 미흡한 것이 현실이다[1].

세계적인 해커이자 보안 컨설턴트인 케빈 미트닉(Kevin Mitnick)은 『해킹, 속임수의 예술』에서 처음으로 사회공학(social engineering)이라는 개념을 통해 인간의 감정이나 인지적 특성을 이용한 해킹 사례들을 소개하였다. 여기서 사회공학은 "목표가 되는 사람을 조종해 목표물에게 이익이 될 수도 있고, 아닐 수도 있는 특정 행동을 취하게 하는 기술"을 의

Received(02. 28. 2018), Modified(05. 21. 2018), Accepted(05. 21. 2018)
* 본 논문은 2017년 제4284부대(2017MCM0017호)와 2018년 화랑대연구소의 지원을 받아 수행된 연구성과임
† 주저자, kyshin@kma.ac.kr
‡ 교신저자, kimyong@kma.ac.kr(Corresponding author)

Table 1. Concepts and Examples of War, Warfare, and Operation

Term	Concept[1)]	Examples
War	a situation of fighting between countries, groups, etc.	Korean War, Gulf War, Iraq War
Warfare	ways or means of fighting a war.	Land warfare, Air Warfare, Cyber Warfare
Operation	the coordinated military actions of a state, or a non-state actor, in response to a developing situation.	Operation Chromite, Operation Desert Storm, Operation Iraqi Freedom

미하며, 주로 정보획득, 컴퓨터 접속, 목표물이 특정 행동을 취하게 하는 등의 범주를 포함한다[2].

국내의 경우 2011년에 발생한 농협 전산망 해킹사건을 통해 사회공학에 대한 관심이 증대되었다. 사회공학 기법을 활용한 사이버 공격이 증가함에 따라 완벽한 보안을 위해서는 기술적 보안과 더불어 인적 보안 특히, 사회공학 기법에 대비한 대응 노력이 요구되고 있다. 하지만 기존연구들[1, 3-4, 7-10]을 살펴보면 사회공학 기법 및 사이버작전에 대한 용어와 개념이 혼재되어 있어 심도 있는 연구를 위해서는 명확한 개념정립이 필요한 실정이다. 따라서 본 논문에서 우리는 사회공학 사이버작전의 개념을 명확하게 정립하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 Ⅱ장에서는 사이버작전의 개념정립에 필요한 기본용어를 정의하고, Ⅲ장에서는 Ⅱ장의 용어정리를 바탕으로 사이버작전을 정의한다. Ⅳ장에서는 사회공학 기법의 개념과 종류를 살펴보고, Ⅴ장에서는 사회공학 사이버작전의 개념을 정립한 뒤, 사례를 분석한다. 마지막으로 Ⅵ장에서는 결론을 맺고, 향후 연구방향을 제시한다.

II. 사이버작전 관련 기본용어 정의

이번 장에서는 일반적으로 사용되는 전쟁(戰爭), 전(戰), 그리고 작전(作戰)에 대한 개념을 살펴보고, 이를 바탕으로 사이버작전 개념정립에 필요한 기본용어들을 명확히 정의한다.

1) 위키피디아(http://en.wikipedia.org)

2.1 전쟁(戰爭), 전(戰), 작전(作戰)의 구분

전쟁(戰爭, war)은 둘 이상의 국가 또는 교전 단체 사이에서 어떤 목적을 두고 수행되는 싸움으로 다소 추상적이고 일반적인 개념이다. 반면 전(戰, warfare)은 특정 영역(공중, 지상, 해상, 우주, 사이버 등) 혹은 구체적인 수단(전자, 화생방 등)에 중점을 둔 개념이다. 이에 반해 작전(作戰, operation)은 사전적 의미에서 어떤 일을 이루기 위하여 필요한 조치나 방법을 강구하는 것으로 여러 분야에서 조금씩 다른 의미로 해석되고 있다. 군사적인 의미에서의 작전은 사전적 의미의 내용을 조금 더 구체화하여 군 조직이 군사적 목적을 이루기 위하여 행하는 제반활동(공격, 방어, 훈련, 행정 등)으로 볼 수 있다[3, 5].

따라서 일반적인 국가 또는 집단 간의 무력충돌을 의미할 때는 '전쟁', 구체적인 전쟁의 영역이나 수단에 중점을 두어서 표현할 때는 '전'을, 그리고 군사적 목표를 달성화기 위한 조직적인 군사행동에 중점을 두고자 할 때에는 '작전'이라는 용어를 사용하는 것이 바람직하다. Table 1.은 전쟁, 전, 그리고 작전에 대한 개념과 그 사용 예들을 나타낸 것이다.

2.2 사이버전쟁, 사이버전, 사이버작전의 구분

앞 절에서 설명한 전쟁의 개념을 적용하면 사이버전쟁(cyber war)은 국가 또는 집단의 충돌 발생 시 사이버 무기가 유일한 무력 수단이 되는 경우를 의미한다. 하지만 통상적으로 전쟁은 국가 혹은 집단 간의 총력전 양상을 띠기 때문에 사이버 무기만을 사용하는 전쟁은 상상하기 어렵다. 따라서 사이버전쟁이라는 용어를 보편적으로 사용하

Table 2. Three Layers of Cyberspace[6]

Layer	Examples
Physical Network Layer	· geographic component : land, air, sea, or space · physical network component : hardware, systems software, and infrastructure
Logical Network Layer	· web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator (URL)
Cyber Persona Layer	· some biographical or corporate data, e-mail and IP address(es), Web pages, phone numbers, etc

는 것은 적절하지 않다고 볼 수 있다. 반면 사이버전(cyber warfare)은 사이버공간(cyberspace)이라는 특정 영역에서 사이버 무기라는 특정 도구를 가지고 수행된다는 점에 중점을 두는 표현이라 볼 수 있다. 이러한 의미에서 사이버전은 지금까지 이 분야에서 가장 일반적으로 사용되어 온 용어이다. 사이버작전(cyberspace operations[2])은 사이버전의 개념을 군사적인 목표와 행동의 관점으로 구체화시키는 경우에 사용된다. 따라서 군사 분야에서 작전의 개념으로 사이버전을 수행하는 경우는 사이버작전이라는 용어를 사용하는 것이 타당하다.

III. 사이버작전(cyberspace operations)

이번 장에서는 사이버작전이 수행되는 공간인 사이버공간(cyberspace), 사이버작전의 수단인 사이버역량(cyber capabilities), 그리고 사이버작전의 목표에 대해 자세히 살펴보기로 한다. 이어서 사이버작전의 수행단계 및 (전통적인) 기술적 사이버작전의 제한사항에 대해 알아본다.

3.1 사이버공간(cyberspace)

사이버공간(cyberspace)은 컴퓨터 시스템과 네트워크를 포함하여 정보가 처리, 저장, 유통되는 공간을 의미한다. 구체적으로는 데이터가 전송되는 매체를 의미하는 물리적 네트워크(physical network) 계층, 이것들로부터 추상화되어 연관되어 있는 논리적 네트워크(logical network) 계층, 그리고 디지털 표현을 위해 논리적 네트워크에 적용되는 규칙을 사용하는 사이버 인물(cyber-persona) 계층을 포함한다[6]. Table 2.는 사이버 공간의 3계층을 보여준다.

3.2 사이버역량(cyber capabilities)

사이버작전의 수단으로 사용되는 사이버역량(cyber capabilities)은 기반시설(컴퓨터, 케이블, 라우팅 장치 등), 전자기 스펙트럼(위성, 휴대전화, 무선 등을 포함하는 데이터링크 주파수), 그리고 콘텐츠(데이터, 어플리케이션 등) 등으로 구성된다[9]. 이때 중요한 점은 사이버작전의 수단은 반드시 사이버역량으로만 한정되어야 한다는 것이다. 따라서 일반적으로 사이버 공간에 영향을 미치지만 사이버역량을 사용하지 않는 작전은 사이버작전으로 간주되지 않는다[3]. 이러한 의미에서 적의 사이버 위협에 따른 국가적 손실에 대해 재래식 무기를 이용하여 군사작전을 펼치는 것은 사이버작전이라고 볼 수 없다.

3.3 사이버작전의 목표

사이버작전의 목표는 사이버공간에 대한 지배력을 극대화해서 보안의 3요소(기밀성, 무결성, 가용성)를 보장(또는 파괴)하여 필요한 정보를 적시에 보호(또는 획득)하는 것이다. 즉, 공세적인 측면에서의 사이버작전의 목표는 사이버 공격을 통해서 적의 정보를 알아내거나, 적의 정보를 우리가 원하는 내용으로 수정하거나, 또는 적이 그들의 정보자산에 접근할 수 없도록 만드는 것이다. 반대로 방어적인 측면에서 사이

2) 혹은 간단히 "cyber operations"로 사용하기도 한다.

3) Deputy Secretary of Defense Memorandum, dated 15 October 2008, defined CyberOps.

버작전의 목표는 우리의 정보를 보호하고, 적에 의한 정보의 위·변조를 방지하며, 언제든지 우리의 정보자산을 활용할 수 있도록 보장하는 것이다.

3.4 사이버작전 수행단계

사이버작전 수행단계는 용어의 선택에 따라 조금씩 차이가 있지만 일반적으로 공세적 사이버작전은 Fig.1.에서 보는 바와 같이 4단계로 진행된다[4].

- 1단계인 공격준비(preparation) 단계는 목표시스템에 대한 정보(물리적·논리적 위치, 네트워크 구조, 서비스의 종류와 버전, 시스템 취약점 등)를 수집하는 단계로 관리자 권한을 획득하기 위한 예비단계로 생각하면 된다. 이 단계의 핵심은 적 정보시스템 및 관리자에 대한 정보수집이다.
- 2단계인 목표접근(infiltration) 단계는 대상시스템에 접근할 수 있는 수단과 방법을 찾아 불법접근을 시도하는 단계로 획득한 관리자 권한으로 시스템을 조작 및 제어하여 위협실시를 위한 준비를 완료하는 단계이다.
- 3단계인 위협실시(intimidation) 단계는 사이버 위협도구들을 이용해 실질적인 피해(정보의 불법 유출 및 변경, 시스템 파괴 등)를 가하는 단계로 사이버작전에서의 최종 목표라고 할 수 있다.
- 4단계인 흔적제거(elimination) 단계는 공격자가 3단계 위협실시 단계를 통해 목표를 달성한 후 위협행위에 대한 흔적을 지우고, 향후 추가공격의 용이성을 높이기 위해 백도어(backdoor) 등을 설치하는 단계이다.

Fig. 1. Steps for Performing a Cyber Operation

3.5 기술적 사이버작전의 제한사항

앞에서 제시한 (공세적) 사이버작전 수행단계에서 관심을 가지고 살펴볼 단계는 1단계인 공격준비 단계로 목표시스템에 접근하기 위한 정보수집을 어떻게 하느냐 하는 것이다. 과거에는 패스워드 크래킹, 스니핑, 포트 스캐닝 등과 같은 사이버 공격 기술을 통해서 목표시스템에 침입하기 위한 정보를 획득하였다[4]. 하지만 최근에는 암호시스템 및 보안시스템의 발전, 다양한 보안 소프트웨어의 개발, 그리고 안전한 보안 프로토콜 설계 등을 통해 컴퓨터 시스템과 네트워크에 대한 보호가 이루어지므로 기술적인 공격만으로 목적을 달성하기가 상대적으로 어려워졌다. 따라서 최근의 공격양상은 목표시스템을 직접 공격하기 보다는 시스템을 관리하는 사람을 공격함으로써 목표시스템에 침입하는 방향으로 선회하게 되었다.

IV. 사회공학 기법(social engineering)

이번 장에서는 기술적 사이버작전의 대안으로 각광받고 있는 사회공학 기법에 대해 자세히 알아본다.

4.1 사회공학 기법의 개념

사회공학 기법이란 사람을 속여 자신들이 원하는 방향으로 움직이게 하는 심리적 기법을 의미한다. 즉, 상대를 속여 민감한 정보를 누설하게 하거나 정보와 관련된 보안경계(security perimeter)를 우회할 수 있도록 함으로써 목표를 달성하는 기법들의 총칭이라 할 수 있다[1]. 사이버작전에서 사회공학 기법은 주로 공격준비 단계에서 목표시스템에 접근(침입)하기 위한 정보를 수집하기 위한 목적으로 활용된다. 사회공학기법을 활용해 목표시스템 접근(침입)에 성공한 이후부터는 기존의 기술적 사이버작전을 활용하여 목표를 달성할 수 있다.

4.2 사회공학 기법의 종류

사회공학 기법에서 활용되는 기술들은 도청(eavesdropping), 어깨너머 훔쳐보기(shoulder surfing), 설득(persuasion), 프리텍스팅(pretexting) 등과 같은 전통적 기법에서부터 피싱(phishing), 스피어 피싱(spear phishing), 워터링 홀(watering hole), 파밍(pharming), 베이팅(baiting) 등과 같은 현대적인 기법까지 매우 다양하다[1-3, 7-10]. 본 연구에서는 다양한 사회공학 기

4) 이러한 의미에서 전통적인 사이버작전을 기술적인 사이버작전이라 부른다.

Table 3. Classification of Social engineering

Class	Examples
Physical stratagem	eavesdropping, shoulder surfing, dumpster diving
Social stratagem	persuasion, pretexting, quid pro quo, reverse social engineering
Technical stratagem	phishing, spear phishing, smishing, whaling, pharming, baiting, watering hole
Multi stratagem	tailgating, vishing

법들을 Table 3.에서 보는 바와 같이 물리적 방략[5], 사회적 방략, 기술적 방략, 혼합 방략으로 구분하여 소개하고자 한다.

4.2.1 물리적 방략

물리적 방략은 공격자가 원하는 정보를 획득하기 위해 실시되는 물리적인 행동으로, 먼저 도청은 정보 획득을 위해 도청장치를 설치하거나 옆에서 엿듣는 행위를 말하며, 어깨너머로 훔쳐보기는 사람이 많은 곳이나 장소에서 공격목표가 인지하지 못하게 한 후 비밀번호(password)와 같은 민감한 정보를 알아내는 방법을 뜻한다. 쓰레기통 뒤지기는 목표물에 대한 민감한 자료를 찾기 위해 쓰레기통 혹은 소각장 등에 버려진 자료를 분석하는 것을 의미한다.

4.2.2 사회적 방략

사회적 방략은 민감한 정보를 얻기 위해 사회·심리적 지식을 활용하는 방법을 의미한다. 설득은 사칭된 권위 등을 통해 공격 대상의 심리적인 취약점을 공격함으로써 부적절한 요구에 순응하도록 만드는 공격이다. 프리텍스팅은 목표물을 설득해 정보를 누설하게 하거나 특정한 행위를 하도록 만드는 공격방법이다. 다른 사람을 사칭해 통화기록과 같은 사적인 정보를 입수하는 것이 여기에 해당되는데, 이때 잘 알지 못하는 사람이라면 전화통화를 통해 설득하고, 아는 사람이라면 직접 만나서 간략하고 섬세한 말로 설득하기도 한다. 보상은 “무언가를 위한 것” 또는 “이것을 위한 것”을 의미하는 라틴어인 “quid pro quo”에서 유래하는데, 특정한 문제를 해결해주겠다는 제안으로 문제해결에 필요한 정보를 획득하는 방법이다. 역 사회공학기법은 공격자가 공격 대상이 모르게 미리 특정한 문제를 유발시킴으로써 공격 대상이 자발적으로 공격자에게 도움을 요청하도록 만드는 기법이다.

4.2.3 기술적 방략

기술적 방략은 원하는 정보를 획득하기 위해 인터넷을 통해 수행되는 기술적 행동을 의미한다. 피싱은 개인정보(private data)와 낚시(fishing)의 조합어로 신뢰성 있는 연락처(이메일 등)로 가장하여 개인정보나 민감정보를 탈취하는 속임수의 한 유형이다. 스피어 피싱은 특정대상으로부터 정보를 획득하기 위하여 행해지는 정교한 공격을 의미한다. 피싱이 불특정 다수로부터 개인정보를 탈취하고자 한다면, 스피어 피싱은 특정 대상을 집중적으로 공격해 정밀도를 증가시키고자 하는 방법이다. 스미싱은 문자(SMS)와 피싱(phishing)의 합성어로 문자메시지를 이용하여 특정 홈페이지에 접속하게 하거나 악성코드를 실행하도록 유도한다. 웨일링은 공격 대상의 민감 정보를 목표로 중요한 정보에 대한 권한을 가진 고위직으로 가장하는 방식으로 공격하는 것을 말한다. 파밍은 정당한 사용자가 특정 도메인명에 대한 IP 주소확인을 요구할 때, 가짜 홈페이지나 유사 홈페이지 등 해커가 악의적인 사이트를 제공하거나 유도하는 방식이다. 베이팅은 주로 사회연결망 서비스에 음란정보 혹은 세일정보 등의 유인책을 통

5) 사회공학 기법에서 방략(stratagem)이란 사물과 사상에 관한 정보를 획득·저장·인출·활용하기 위한 인지적 조작과 절차를 계획하고 실행·통제하는 일련의 선택적인 정신 활동이다.(네이버 국어사전)

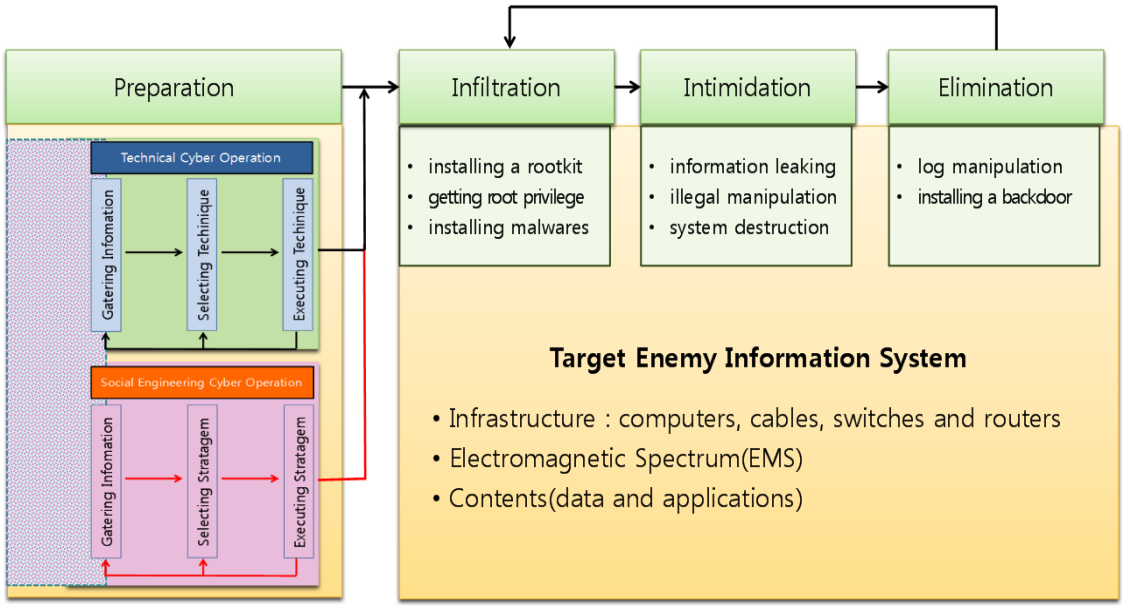

Fig. 2. Technical and social engineering based cyberspace operations

해 악성코드를 유포하는 방식이다. 물리적으로는 USB에 악성코드를 담아 공격목표가 자주 방문하는 장소나 주변에 방치하거나 컨퍼런스 등에서 배포하는 형태로 이루어지며, 온라인상에서는 공공장소에 무료로 핫스팟 등을 생성하여 접속하게 만드는 수법을 사용한다. 마지막으로 워터링 홀은 사용자가 자주 방문하는 웹사이트를 미리 감염시켜 놓은 후 사용자가 해당 사이트를 방문할 때 악성코드가 자동으로 설치되도록 하는 공격이다.

4.2.4 혼합 방략

혼합 방략은 앞서 설명된 다양한 공격 중에서 여러 개를 혼합해서 사용하는 공격 형태로 테일게이팅(tailgating), 비싱(vishing) 등이 있다. 테일게이팅은 인증이 필요한 기관의 출입구나 사무실을 통과할 때 인증된 사람의 뒤를 따라 들어감으로써 신원확인을 회피하는 방법이다. 비싱은 보이스 피싱(voice phishing)의 줄임말로, 사기성 전화번호가 담긴 이메일을 보내거나 인터넷 전화를 이용하여 마치 금융기관에서 거는 것처럼 전화를 걸어 개인 신상 정보나 금융 정보, 비밀번호 등을 불법으로 알아내는 공격기술을 의미한다.

V. 사회공학 사이버작전

이번 장에서는 사회공학 사이버작전의 개념을 정립하고, 사회공학 사이버작전의 수행단계에 대해 살펴본 후, 사회공학 사이버작전의 사례를 분석한다.

5.1 사회공학 사이버작전 개념

사회공학 사이버작전은 목표시스템을 직접 공격하기 보다는 목표시스템을 관리하고 있는 사람의 취약점을 공격해 우회적인 방법으로 목표시스템에 접근(침입)하는 공격이라 정의할 수 있다. Fig.2.에서 보듯이, 사회공학 사이버작전은 주로 공격준비 단계에서 목표시스템에 접근(침입)하기 위해 활용된다.

5.2 사회공학 사이버작전의 수행단계

사회공학 사이버작전의 목표는 시스템을 관리하는 사람의 취약점을 공격해 목표시스템에 침입하는 것이다. 따라서 목표시스템에 대한 침입이 성공하면 사회공학 사이버작전의 목표를 달성하게 되는 것이다. 이때 사회공학 사이버작전의 수행단계는 Fig.2.에서 보는 바와 같이 ① 정보수집, ② 방략선택, ③ 방략실행의 3단계로 구성된다. 사회공학 사이버작전은 인간을 대상으로 하는 작전이라는 측면에서 모든 단계에

걸쳐 다양한 심리적 기제[6]가 활용될 수 있다[11].

5.2.1 정보수집(Gathering Information)

정보수집 단계는 목표시스템에 접근(침입)하거나 그에 필요한 정보를 획득하기 위해 조직 및 관련자 정보를 수집하는 단계이다. 최초에는 공개된 정보를 수집해 활용하고, 이후에는 방략선택 및 방략실행 단계를 통해 획득된 정보들이 누적되어 활용된다. 수집되는 정보는 조직 및 개인 요소를 망라하며, 정보수집의 대상이 되는 개인은 중요정보를 취급하거나 중요정보에 대한 접근(침입)이 가능한 사람이다.

5.2.2 방략선택(Selecting Stratagem)

방략선택 단계는 정보수집 단계를 통해 수집된 정보를 바탕으로 취약대상을 공략하여 목표시스템에 접근(침입)하기 위한 (혹은 그에 필요한 추가적인 정보를 수집하기 위한) 사회공학기법을 선정하는 단계이다. 이때 Ⅳ-2장에서 살펴본 바와 같이, 공격자가 선택할 수 있는 방략은 물리적, 사회적, 기술적, 혼합 방략 등 매우 다양하며, 정보수집 단계에서 파악된 조직이나 개인의 취약점을 가장 효과적으로 공략할 수 있는 방략을 선택하는 것이 중요하다.

5.2.3 방략실행(Executing Stratagem)

방략실행 단계는 방략선택 단계에서 선정한 사회공학기법을 실행하여 목표시스템에 접근(침입)하거나 그에 필요한 정보를 획득하는 단계이다. 이때 선정된 방략을 실행하여 목표시스템 접근(침입)에 성공하거나 접근(침입)에 필요한 정보(예를 들어 관리자 비밀번호 등) 획득에 성공한 경우, 이를 성공으로 간주한다. 반대로 방략을 실행하여 목표시스템에 접근(침입)할 수 있는 정보를 획득하지 못했을 경우에는 실패로 간주되며 정보수집 또는 방략선택 단계로 되돌아간다.

5.3 사회공학 사이버작전 사례분석

사회공학 사이버작전 수행단계에 대한 이해를 돕기 위해 2015년 서울에어쇼에 참가한 방위산업체를 대상으로 한 스피어 피싱 공격 사례를 바탕으로 각 단계에서의 주요 내용을 살펴보고자 한다. 2015년 10월 해커들은 ADEX에 참가하는 방위산업체를 대상으로 항공우주 관련 학회를 사칭하여 악성코드가 포함된 이메일을 발송하였다. 이때 해당 이메일을 열람한 뒤 첨부된 파일(악성코드)을 실행한 다수의 방산업체는 업무망이 해킹되어 내부 자료 일부가 유출되는 등의 피해를 입었다. 본 사례에서 해커들은 방위산업체 내부 업무망을 해킹해서 고가치 방산기술 정보를 획득하기 위해 스피어 피싱을 실시한 것으로 추정된다. 이 사례를 Fig.2.의 사회공학 사이버작전 수행단계에 비추어 분석해보면 다음과 같다.

5.3.1 정보수집 단계

정보수집 단계에서 해커들은 국내 방위산업체 및 업체 종사자들을 정보수집 대상으로 선정한 뒤 이들과 관련된 정보들을 수집하였다. 이를 통해 항공 우주분야의 특정 학회가 방산업체와 업무 관련성이 높다는 것과 해당 학회에서 주관하는 세미나에 방산업체들이 높은 관심을 가지고 있다는 것을 확인하였다. 또한, 방산업체 및 관련자들과 접촉하기 위해 가장 손쉽게 획득해 활용할 수 있는 공개 이메일 주소를 수집하였다.

5.3.2 방략선택 단계

방략선택단계에서 해커들은 획득한 이메일 주소를 활용하여 내부 업무망에 접근하기 위해 기술적 방략 중 하나인 스피어 피싱을 선택하였다. 즉, 방위산업체라는 특정 대상에 대하여 정교한 피싱 메일을 발송함으로써 원하는 정보를 탈취하고자 한 것이다.

5.3.3 방략실행 단계

방략실행단계에서 해커들은 정보수집단계에서 파악한 학회 명칭과 유사한 메일 계정을 만들고, 해당 계정을 활용하여 '항공우주 무기체계 발전 세미나 초청장입니다.'라는 제목으로 메일을 발송하였다. 메일의 본문은 세미나 초청 메일의 형식과 내용을 준수하였고, 관련 분야의 전문용어들을 포함하는 정교함을 보였다. 또한, 초청장을 가장한 악성파일을 첨부하여 실행을 유도함으로써 대상자의 시스템에 악성코드가 설치되도록 하였다. 해커들은 이러한 스피어 피싱을 통해 방산업체

6) 사회공학 사이버작전의 심리적 기제에 대한 연구는 본 논문의 범위를 벗어나므로 향후연구로 남긴다.

내부 업무망에 침입할 수 있었고, 궁극적으로 그들이 원하는 고가치 방산기술 정보를 획득할 수 있었다.

VI. 결론 및 향후 연구방향

사회공학 사이버작전은 기술적 사이버작전이 가지는 한계를 극복하기 위해 고안된 대체방안이다. 사회공학 사이버작전은 전 세계적으로 지속적으로 증가하고 있으며, 그 기법 또한 날로 정교화 되어가고 있다. 이에 완벽한 보안시스템 구축을 위해서는 다양한 사이버 방어기술 및 장비들의 개발뿐 아니라 심리적인 특성을 이용하여 우회적으로 접근하는 사회공학 사이버 공격에 대한 대비책을 강구해야 한다. 이러한 맥락에서 우리는 먼저 사이버작전과 관련된 용어들을 명확히 정의하였고, 이를 바탕으로 사이버작전에 대한 개념을 정립하였다. 또한 최근 유행하고 있는 사회공학 기법에 대한 심도 있는 연구를 통해 기존의 사이버작전에 사회공학 개념을 접목한 '사회공학 사이버작전'의 개념을 명확하게 정립하였다. 나아가 사회공학 사이버작전 개념을 최근 사회공학 사이버 공격에 적용해 분석해봄으로써 활용가능성을 확인하였다.

향후 연구에서 우리는 사회공학 사이버작전에서 핵심적인 역할을 담당하는 다양한 심리적 기제들을 파악하고, 이 심리적 기제들이 사회공학 사이버작전 수행과정 전반에 미치는 영향을 분석함으로써 사회공학 사이버작전 분석모델을 구축할 것이다. 이렇게 구축된 사회공학 사이버작전 분석모델은 다양한 사회공학 사이버 공격 및 방어 시나리오 작성과 사이버작전 사례 분석을 위한 준거의 틀로 활용될 수 있을 것이다.

References

[1] Dong Cheon Shin and Young Hoo Park, "Development of Risk Assessment Indices for Social Engineering Attacks," Journal of Security Engineering, 14(2), pp. 143-156, April 2017.

[2] Kevin D. Mitnick and William L. Simon, The Art of Deception : Controlling the Human Element of Security, John Wiley & Sons, 2003.

[3] Jungho Kang et. al., "A Study on the Relationship between Social Engineering and Cyberspace Operations," Ministry of Defense, Dec. 2017.

[4] Dept. of Computer Science in Korea Military Academy, Korea Naval Academy, Korea Air Force Academy, and Korea Army Academy at Yeong-Cheon, Introduction to Cyber Warfare, 2nd Ed., Yangseogak, Feb. 2016.

[5] ROK Army Training & Doctrine Command, "FM 1-1 Military Terminology," Republic of Korea Army Headquarters, May 2017.

[6] US Joint Chief of Staff, "JP 3-12(R) Cyberspace Operations," Feb. 2013.

[7] Bryan Skarda, Robert F. Mills, Todd McDonald, Dennis Strouble, "Operationalizing Social Engineering for Offensive Cyber Operations," Technical Report, Air Force Institute of Technology, June 2008.

[8] 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, vol. 9, pp. 1-11, Jan. 2017.

[9] Nabie Y. Conteh1 and Paul J. Schmick, "Cybersecurity : risks, vulnerabilities and countermeasures to prevent social engineering attacks," International Journal of Advanced Computer Research, vol 6, no. 23, pp. 31-38, Feb. 2016.

[10] P. S. Maan and Manish Sharma, " Social Engineering: A Partial Technical Attack," International Journal of Computer Science Issues, vol. 9, no. 2, pp. 557-559, March 2012.

[11] John Orbell and Robyn M. Dawes, "A "Cognitive Miser" Theory of Cooperators Advantage," The American Political Science Review, vol. 85, no. 2, pp. 515-528, June 1991.

〈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
〈관심분야〉 분산시스템 보안, 네트워크 보안, 사이버전

강 정 호 (Jungho Kang) 종신회원
1996년 2월: 육군사관학교 공학사(전자공학)
2004년 2월: 서울대학교 석사(전산학)
2015년 2월: 아주대학교 공학박사(정보보호)
〈관심분야〉 사이버전, 가상화체계 보안, 공급망 보안

유 진 철 (Jincheol Yoo) 정회원
1989년 2월: 육군사관학교 이학사(전산학)
1993년 8월: (미)아이오와 주립대 석사(통계학)
2003년 5월: (미)펜실베니아 주립대 공학박사(컴퓨터공학)
1994년 3월~현재: 육군사관학교 컴퓨터과학과 교수
〈관심분야〉 컴퓨터시스템, 사이버전, 컴퓨터구조

김 지 원 (Jeewon Kim) 종신회원
2002년 2월: 동국대학교 공학사(정보통신학)
2016년 8월: 연세대학교 석사(정보보호)
2016년 7월~현재: 육군사관학교 컴퓨터과학과 조교수
2017년 3월~현재: 아주대학교 NCW학과 사이버전전공 박사과정
〈관심분야〉 정보보호, 사이버전, IOT 보안

강 성 록 (Sungrok Kang) 정회원
1996년 3월: 육군사관학교 문학사(심리학)
2001년 2월: 연세대학교 석사(임상심리)
2010년 8월: (미)오리건 주립대(OSU) 박사(HDFS)
2010년 9월~현재: 육군사관학교 심리경영학과 부교수
〈관심분야〉 사회공학, 심리전

임 현 명 (Hyunmyung Lim) 정회원
2007년 2월: 연세대학교 문학사(영어영문학)
2016년 1월: 국방대학교 국방관리대학원 석사
2016년 1월~현재: 육군사관학교 심리학과 조교수
〈관심분야〉 사회공학, 심리전

김 용 주 (Yongju Kim) 정회원
1985년 3월: 육군사관학교 문학사(독일어)
1992년 2월: 서울대학교 심리학 석사
1997년 9월: (독)기센대학교 심리학 박사
1997년 9월~현재: 육군사관학교 심리학과 교수
〈관심분야〉 사회공학, 심리전