https://doi.org/10.33778/kcsa.2023.23.5.165

주요 위협국의 사회공학 공격특징과 대응전략★

김 지 원*

요 약

국가간에 이루어지는 사회공학 공격은 주로 비밀정보, 외교의 협상 또는 미래의 정책 변경에 대해 우위를 확보하기 위해 매우 효율적인 공격이므로 꾸준히 실시되고 있다. 우크라이나-러시아 전쟁이 장기화함에 따라 글로벌 해킹 조직의 활동이 꾸준히 증가하고 있으며, 주요 기반시설 또는 글로벌 기업 대상의 대규모 사이버공격 시도가 지속되므로 이에 대한 대응전략이 필요하다. 이를 위해 다양한 사회공학 공격 모델 중 물리적인 접촉을 배제한 사회공학 사이클이 가장 적합한 모델이라 판단하여 주요 위협국이 선호하는 사회공학 공격 방법을 사례분석을 통해 지정학적 전술과 비교하여 분석하였다. 그 결과 중국은 인해전술과 같은 질보다 양을 선호하는 피싱공격을 러시아는 마치 첩보전을 연상하는 은밀하고 복잡한 스피어 피싱을 선호하며, 북한은 미국과 한국에 대한 공격은 스피어 피싱과 워터링홀로 지정학적 전술을 응용하여 활용하였고 그 외 국가들은 대부분 랜섬웨어로 자금확보를 목표로 하였다. 이에 따라 중국에는 클린패스 정책, 러시아에는 주기적인 의무교육, 북한에는 국제적인 제재 등을 대응전략으로 제시하였다.

Social Engineering Attack Characteristics and Countermeasure Strategies of Major Threat Countries

Jeewon Kim*

ABSTRACT

Nation-state social engineering attacks are steadily being carried out as they are highly effective attacks, primarily to gain an advantage over secret information, diplomatic negotiations or future policy changes. As The Ukraine-Russia war prolongs, the activities of global hacking organizations are steadily increasing, and large-scale cyberattack attempts against major infrastructure or global companies continue, so a countermeasure strategy is needed. To this end, we determined that the social engineering attack cycle excluding physical contact among various social engineering models is the most suitable model, and analyzed the preferred social engineering attack method by comparing it with geopolitical tactics through case analysis. AS a result China favors phishing attacks, which prefer quantity over quality, such as man-made tactics, Russia prefers covert and complex spear phishing reminiscent of espionage warfare, and North Korea uses geopolitical tactics such as spear phishing and watering holes for attacks on the US and South Korea Most of the other countries aimed to secure funds with ransomware. Accordingly, a Clean Pass policy for China, periodic compulsory education in Russia, and international sanctions against North Korea were presented as countermeasure strategies.

Key words : Social Engineering Attacks, North Korea, China, Russia, Geopolitical Tactics.

접수일(2023년 08월 03일), 수정일(2023년 11월 14일), 게재확정일(2023년 12월 01일)

* 상지대학교/군사학과(주저자)

★ 본 논문은 2022년도 상지대학교 교내 연구비 지원에 의해 작성된 것으로, 서울대학교 국제문제연구소 미래전연구센터 워킹페이퍼 No.95(2021.12.14.)로 제출된 내용을 수정보완한 것임.

1. 서 론

사이버공격은 시간이 지남에 따라 변화된 특성을 반영한 저비용 고효율의 공격으로 정치, 군사, 경제, 사회 전 분야로 공격이 확산되고 있으며, 국가기능의 혼란 및 상실을 목표로 한 공격으로 발전하고 있다[1]. 갑자기 발생한 코로나-19(COVID-19) 팬데믹은 국가의 중요업무를 사이버공간으로 신속히 전환하는 계기가 되었고 공격자들은 보안에 취약한 매체나 네트워크를 상대로 공격하는 좋은 기회가 되었다. 또한, 러시아-우크라이나 전쟁이 장기화함에 따라 글로벌 해킹 조직의 활동도 꾸준히 증가하고 있으며, 주요 기반시설 또는 글로벌기업 대상의 대규모 사이버공격 시도가 지속될 것으로 예상된다[23].

특히 다크웹(dark web)에서 유통되는 주된 정보는 도메인 관리자 계정부터 가상사설망(VPN, Virtual Private Network), 원격 데스트톱(RDP, Remote Desktop Protocol)의 계정정보이며 이는 공격자가 공격 난이도를 낮출 수 있어 정교하고 치밀한 공격을 가능하게 만들어준다. 이렇게 탈취한 정보를 이용한 공격 중 사회공학(Social Engineering, 이하 SE) 공격인 피싱(Phishing) 공격의 비율은 2022년 기준 전체 공격 감염률의 41%로 가장 중요한 침해경로로 급부상하였다[3]. 피싱과 같은 특별한 기술을 사용하지 않고 사람을 속여 목표정보를 탈취하는 사회공학 공격은 이메일(e-mail)을 기반으로 하는 전형적인 공격이지만 지금도 여전히 유효한 성공률을 보장받고 있으며, 드라이브 바이 다운로드(Drive by Download) 공격과 결합하여 피해를 가중시킨다.

이처럼 고효율의 사회공학 공격은 사이버보안체계의 가장 취약하지만 없어서는 안 될 사람을 이용하는 공격으로 꾸준히 쓰이고 있으나, 이에 관한 연구는 아직 활발히 이루어지지 않고 있다. 특히, 국가간에 이루어지는 사이버영역의 사회공학 공격은 신뢰관계를 형성하지 않은 공격이 대부분이므로 기존의 연구된 사회공학 모델로는 접근하기가 어렵다. 또한, 국가간의 사회공학 공격은 주로 비밀정보, 외교의 협상 또는 미래의 정책 변경에 대해 우위를 확보하기 위해 꾸준히 실시[10, 24]되고 있기에 이에 대한 대응전략도 필요하다.

이에 본 연구는 국가간 사회공학 공격을 설명할 수 있는 사회공학 사이클을 토대로 주요 사이버위협 국가인 중국, 러시아, 북한의 사회공학 공격의 특징을 분석하고자 한다. 분석방법은 사례분석 방법으로, 사회공학 공격이 알려지기 시작한 2007년부터 공격이 현재까지 물리영역을 제외한 사이버영역에서 발생한 사회공학 공격을 보도자료, 공공기관의 공격보고서(브리핑) 등의 자료를 수집하여 분석한 후, 이를 지정학적 영역에서 사람을 이용하는 전통적 공격전술인 심리전과 비교하여 특징을 분석하고 이에 대한 대응전략을 제시하고자 한다.

2. 이론적 배경

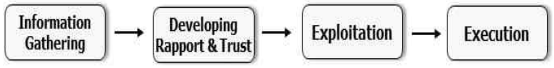
2.1 사회공학 공격의 정의

사회공학은 케빈 미트닉(Kevin D. Mitnick)의 “The Art of Deception : Controlling the Human Element of Security”이라는 제목의 서적으로 널리 알려졌다. 사회공학을 이용한 공격은 사람들을 속여 자신들이 원하는 방향으로 움직이게 하는 심리적인 공격을 의미한다[5]. 국립국어원에서의 사회공학 공격은 시스템이 아닌 사람의 심리를 이용하여 원하는 정보를 얻는 공격기법으로 신뢰할 수 있는 사람으로 위장하여 다른 사람의 전화, 이메일, 메신저 등에 접근하는 해킹 기법[6]으로 정의하였고, 안랩(AhnLab)의 보안용어 사전에서는 IT 기술을 기반으로 공격 대상인 사람의 심리를 파고드는 공격기법으로, 중요정보를 탈취 또는 악성코드 유포를 목적으로 하는 공격, 피싱, 스팸, 보이스피싱 등의 공격기법으로 정의하고 있다[7].

2.2 사회공학 라이프 사이클

케빈 미트닉의 저서에서 다룬 사회공학 라이프 사이클(SE Life Cycle)은 질문, 위장, 속임수, 조작 등의 정보를 수집·활용하여 공격대상자에게 라포 및 신뢰를 발전시켜(Developing Rapport & T

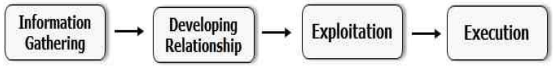
rust)공격에 성공하는 모델로 (그림 1)과 같다. 이 때 정보수집 방법은 사기(fraud) 혹은 첩보수집 활동인 휴민트(HUMINT, HUMan + INTelligence)을 이용한다. 그러므로 라포나 신뢰 발전이 없는 피싱(phishing)과 같은 사회공학 공격에는 이 모델의 한계가 존재한다.



(그림 1) SE Life Cycle [8]

2.3 사회공학 프로세스

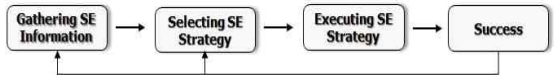
크리스토퍼 헤드네기(Christopher J. Hadnagy) 저서 “The Art of Human Hacking”에서 사회공학 프로세스(SE Process)를 다루고 있다. 이 모델은 사회공학의 심리적 특성을 잘 반영한 공격모델로 사회공학을 연구하는 많은 논문에서 인용하고 있다. 이 모델은 질문, 위장, 속임수, 조작 등 물리적인 접촉을 통한 사회공학 공격인 쓰레기통 뒤지기(Dumpster Diving), 어깨너머 훔쳐보기(Shoulder Surfing)와 같은 공격을 공격대상자와 관계(relationship) 형성 후 취약점을 노려 공격하는 방식으로 (그림 2)와 같다. 이 모델도 관계가 형성되지 않는 사회공학 공격에는 한계를 보인다.



(그림 2) SE Process [9]

2.4 사회공학 사이클

사회공학 사이클(SE Cycle)은 비교적 최근에 연구된 사회공학 모델로 (그림 3)과 같은 과정으로 진행된다. 이 모델에서 사회공학 방략선택(Selecting SE Strategy) 단계는 수집된 정보를 바탕으로 공격대상자의 취약점을 파악한 후 사회공학 공격기술을 선택하는 단계이며, 사회공학 방략실행(Executing SE Strategy)은 선택한 사회공학 공격기술에 알맞은 심리기제를 선택하여 실행에 옮기는 과정으로 공격자가 선택한 사회공학 공격기술이 실제 실행에 옮기기 위해 최적화된 심리적인 방법을 적용하여 목표달성에 기여하는 단계이다. 공격자는 사회공학 공격이 실패하면 정보수집과 사회공학 방략선택 단계로 되돌아가 목표를 달성한다. 이 모델은 케빈 미트닉의 사회공학 라이프 사이클과 윌리엄 시몬의 사회공학 프로세스에서 한계를 보인 신뢰가 형성되지 않는 사회공학 공격이 가능하다.



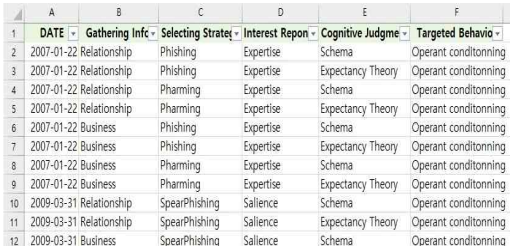
(그림 3) SE Cycle [4]

3. 주요 위협국의 사회공학 공격특징

사이버위협 주요 국가인 중국, 러시아, 북한을 중심으로 국가간에 이루어지는 사회공학 공격의 특징을 분석하기 위해 지정학적 한계인 물리적인 접촉을 배제하고 신뢰관계 없이도 공격이 가능한 사회공학 모델인 사회공학 사이클을 토대로 주요 위협국의 공격특징을 분석하고자 한다.

분석방법은 사례분석 방법으로, 사회공학 공격이 알려지기 시작한 2007년부터 2022년까지 475건의 사례를 사회공학 사이클을 적용해 사이버 영역에서 발생한 사회공학 공격사례를 신뢰도가 높은 주요 언론사의 보도자료, 공공기관의 공격보고서(브리핑) 자료를 수집하여 분석하였다.

수집한 사례는 (그림 4)와 같이 사회공학 사이클의 각 단계에 해당되는 정보요소로 추출하였고 이를 토대로 주요 위협국의 지정학적 전술인 심리전과 비교하여 선호하는 사회공학 공격 특징을 분석하였다.



	A	B	C	D	E	F
1	DATE	Gathering Infc	Selecting Strate	Interest Repon	Cognitive Judgme	Targeted Behavio
2	2007-01-22	Relationship	Phishing	Expertise	Schema	Operant conditonning
3	2007-01-22	Relationship	Phishing	Expertise	Expectancy Theory	Operant conditonning
4	2007-01-22	Relationship	Pharming	Expertise	Schema	Operant conditonning
5	2007-01-22	Relationship	Pharming	Expertise	Expectancy Theory	Operant conditonning
6	2007-01-22	Business	Phishing	Expertise	Schema	Operant conditonning
7	2007-01-22	Business	Phishing	Expertise	Expectancy Theory	Operant conditonning
8	2007-01-22	Business	Pharming	Expertise	Schema	Operant conditonning
9	2007-01-22	Business	Pharming	Expertise	Expectancy Theory	Operant conditonning
10	2009-03-31	Relationship	SpearPhishing	Sallence	Schema	Operant conditonning
11	2009-03-31	Relationship	SpearPhishing	Sallence	Expectancy Theory	Operant conditonning
12	2009-03-31	Business	SpearPhishing	Sallence	Schema	Operant conditonning

(그림 4) 사례수집 추출 결과 예시

3.1 중국

중국의 사회공학 공격은 자국의 개인 PC와 인터넷 보급률이 증가한 2008년을 시작으로 6·25전쟁 시 사용했던 “인해전술”과 유사하게 대량의 공격을 시도하는 것이 특징이다[10]. 또한, 세계 최대의 인구를 자랑하듯 최대의 해커 시스템을 갖추고 있으며, 수많은 PC들은 봇넷(BotNet)으로 활용되어 마치 인해전술의 각개 병사와 같이 마구잡이로 이용되어 사이버 공격이 심각한 수준으로 분석되고 있다[11]. 특히 Nuwar 봇넷은 불특정대상을 상대로 “미국 대통령 사망”과 같은 자극적인 제목으로 이메일에 첨부하기 시작하여 “사담 후세인 처형”, “새 일본수상 선출” 등 사회현안을 활용한 사회공학 공격으로 성공확률을 높였다[12]. 이러한 공격들의 특징은 특정 사이트를 목표로 집요하게 노렸다기보다는 다른 사이트에 비해 상대적으로 보안이 취약한 사이트나 사람을 노린 공격으로 특별한 공격기술은 사용되지 않은 무작위 공격이었다. 또한, 공격의 근원지도 IP주소로 미뤄보아 중국발 공격으로 쉽게 파악되었다.

중국의 지정학적 공격전술 중 인해전술이 그러하듯 사회공학 공격도 질보다는 양으로 승부하는 공격방식을 선호하는 것으로 <표 1>과 같이 분석되었다. 피싱, 파밍, 스미싱, 비싱 공격의 사례가 대다수이며, 피싱공격은 무작위로 해당국의 개인정보를 수집하여 대인관계를 파악한 후 공격하는 방식과 업무내용으로 가장하거나 공격대상 국가에 사회적인 이슈 및 큰 현안 등이 생기면 이를 이용한 것으로 나타났다. 파밍공격은 소셜 네트워크를 탐색하여 개인정보를 수집한 뒤 첨부파일에 사용될 실행파일을 비실행파일로 위장한 후 가족이나

<표 1> SE공격에서 수집된 정보요소 분석결과(중국)

* ( ) : Number of SE attack cases (No.)

Selecting SE factors	Types of Information factors			
	1st	2nd	3rd	4th
Phishing (30)	Relationship (13)	Business (8)	Social issue(5)	Character /Motive (4)
Pharming (14)	Relationship (8)	Business (6)	-	-
SMSfhing (14)	Relationship (6)	Social issue(4)	Business (2) Character /Motive (2)	-
Vishing (4)	Relationship (4)	-	-	-

친지 등 대인관계를 사칭하여 링크 접속을 유도하는 공격방식과 업무내용을 가장한 이메일로 가짜 홈페이지나 유사 홈페이지 등의 접속을 유도하는 방식을 취했다. 스미싱공격은 피싱공격과 같은 방법으로 정보를 수집하지만 스마트폰을 이용하는 점에서 QR코드를 이용하는 등 공격의 차이를 보인다. 마지막 보이스피싱으로도 더 알려진 비싱공격은 주로 대인관계를 이용한 정보를 수집하여 공격하는 것으로 나타났다.

3.2 러시아

러시아는국가의 중대한 국익이 달린 사항이라면 사이버공격을 서슴지 않게 진행한다. 사이버 업무를 구소련의 국가안보위원회(KGB)의 후신인 연방안보국(FSB)과 군사정보국(GRU) 두 기관이 수행하기에 그 형태는 상당히 은밀하고 복잡하며 발전된 형태를 보였다. 러시아의 사이버 공격의 중요성은 이미 전통적 전쟁을 넘어섰으며, 이는 세계적으로 정치·군사적 목적으로 사이버공격을 실시하고 있음을 사례를 통해 보여주었다.

평창올림픽 티켓판매를 가장한 메일을 IOC 관계자에게 보내 첨부파일의 클릭을 유도한 2018년 평창 동계올림픽 조직위원회 홈페이지를 마비시킨 공격은 러시아 군 정보기관소속 해킹팀 팬시 베어(Fancy Bear)의 공격으로 추정되는 이 사례는 북한소행으로 위장하는 치밀함을 보였다[13]. 또한, 러시아-우크라이나 전쟁의 전초전으로 우크라이

<표 2> SE공격에서 수집된 정보요소 분석결과(러시아)

* ( ) : Number of SE attack cases (No.)

Selecting SE factors	Types of Information factors			
	1st	2nd	3rd	4th
Spear Phishing (78)	Relationship (37)	Business (24)	Character /Motive (9)	Facility (4) Culture (4)
Baiting (23)	Character/ Motive(6)	Relationship (12)	Social issu(3)	Facility (4)
Whaling (6)	Relationship (3) Business (3)	-	-	-

나 외교부, 에너지부, 재무부 및 대응 관련 부처 등 70여 개에 달하는 홈페이지를 해킹·마비시키는 사이버공격, 정보수집, 여론조작 등 포괄적인 사이버 공격의 능력도 보여줬다[14]. 이처럼 지정학적 전술의 한 부분인 첩보 및 정보전에 능숙한 러시아는 시설 및 문화요소를 이용한 공격을 감행했으며, 사회공학 공격 사례를 분석과 결과 <표 2>와 같다. 수집된 정보의 발견된 허점을 이용하여 은밀하게 침투하는 스피어피싱 공격과 취약한 대상자를 노린 베이팅 공격과 복종을 자극하는 공격인 웨일링 공격을 주로 이용한 것으로 나타났다. 또한, 러시아는 국가의 정치 외교적 위협에는 공제적인 사이버공격을 감행하는 것이 특징이다.

3.3 북한

북한의 공격전술인 속도전(速度戰)은 코로나-19 팬데믹 같은 사회현안을 빠르게 활용한 피싱 공격을 시도했으며[15], 선제기습전략은 보수성향의 웹사이트를 직접 공격하는 방식보다는 은밀히 기다렸다가 침투하는 워터링홀과 같은 공격방식으로 활용하였다[16]. 또한, 소니픽처스 해킹 사건과 같이 공격할 대상에 대해 미리 선전포고하는 선전공작의 전략을 취하기도 하였다. 2018년 북한 인권단체 관계자와 기자들을 대상으로 한글 문서파일(.hwp)이 첨부된 이메일을 발송하여 첨부파일에 대한 경계심을 낮추는 스피어 피싱 공격을 시도하였다[17].

북한의 스피어피싱 공격은 러시아의 공격방법과 유사한 형태로 시설 및 문화요소를 이용하여 파악된 모든 정보를 이용하여 은밀히 공격하는 스피어피싱 공격을 가장 선호하는 등 <표 3>과 같이 분석되었다. 북한의 사회공학 공격의 특징으로는 대상 목표에 따라 공격형태가 변하는 특징을 보인다. 한국과 미국 또는 이와 관련된 단체, 탈북민 등 자국의 위협국은 정보탈취를 목표로 한 스피어피싱과 워터링홀 공격을 선호하고 그 외 국가는 자금확보를 위한 랜섬웨어 로 주로 공격에 활용한다.

<표 3> SE공격에서 수집된 정보요소 분석결과(북한)

* ( ) : Number of SE attack cases (No.)

Selecting SE factors	Types of Information factors			
	1st	2nd	3rd	4th
Spear Phishing (78)	Relationship (37)	Social issue(24)	Character /Motive (9)	Facility (4) Culture (4)
Watering hole (6)	Character/ Motive(2) Relationship (2) Business (2)	-	-	-
Ransom ware (12)	Relationship (4) Social issue(4)	Business (2) Culture (2)	-	-

4. 대응전략

4.1 중국

대량의 정보탈취를 하는 중국의 사회공학 공격은 네트워크 자체의 보안강화가 중요하다. 미국은 데이터의 안정성을 보장하고자 5G 네트워크를 통해 유입되는 장비 중 신뢰할 수 없는 장비의 사용을 제재한다는 내용으로 클린패스(Clean Path)를 포함한 모바일 앱, 클라우드 등 총 6개 분야에 클린 네트워크(Clean Network)를 선언하였다[18]. 백도어를 설치해 중국으로 데이터를 빼간다는 의혹을 받은 화웨이 5G 장비에 대한 유럽 각국의

대대적인 철거 작업도 시작되었다[19]. 이처럼 미국은 신뢰할 수 없다고 판단한 제품 모두를 자국내 모든 네트워크에서 배제한다는 강한 메시지를 전달하였고 영국을 비롯한 호주, 뉴질랜드 등의 국가들도 동참하였다. 이에 따라 우리나라도 신뢰국과의 공조를 통해 안전하고 신뢰할 수 있는 네트워크 환경을 구축하기 위해 '초신뢰 네트워크[25]'를 구현하고 자료유출방지(Data Loss Prevention, DLP) 정책 프레임워크를 주요 기업 및 기관에 도입하여 민감정보와 같은 데이터 유출을 차단하는 대응전략이 필요하다.

4.2 러시아

러시아는 주로 정부기관을 목표로 스피어 피싱 공격을 시도한 사례가 다수이다. 공격대상자가 상용메일을 업무에 사용하여 공격당하는 사례들은 업무자료 상용메일 유통금지와 같은 기본적인 보안교육에서 피싱메일 식별요령과 같은 전문적인 교육까지 에빙하우스의 망각곡선(Ebbinghaus's Forgetting Curve)을 고려하여 지속적으로 예방교육을 해야한다. 국가사이버안보전략서에는 국민 모두의 사이버 보안문화 정착을 위해 맞춤형 사이버 윤리 및 보안 교육프로그램을 개발·실시[20]하도록 명시한 만큼 정교해진 공격은 구체적인 사례를 제시하여 교육하여야 대응능력을 향상시킬 수 있다. 국가정보보호백서에서는 정보보호의 인식 함양을 위한 교육이 필요하다고 언급은 하였지만, 의무교육에 대한 언급은 없어 각 기업 및 기관의 규정에 의해 자체적으로 진행하고 있다. 주요 정보 및 민감정보를 관리하는 인원들에 대한 사회공학 공격 교육은 보안사고가 아니라 안보위협 차원에서 접근하여 더욱 철저히 강조되어야 한다. 이를 위해 사회공학 공격을 당한 사례와 공격자의 침해 전 징후 등을 분석한 위험 모델 프로그램을 개발해 주기적으로 의무교육하여 은밀하고 치밀한 공격에 대비해야 할 것이다.

4.3 북한

북한은 완강한 국제적인 제재의 우리정부의 실천을 대응전략을 제시하겠다. 사이버공격은 주로 초국가적 형태로 진행되기에 한 나라의 차원으로는 대응의 한계가 있어 국제협력이 불가결하다[21]. 이를 반영하여 2020년 7월 유럽연합 이사회(EU Council)는 EU와 회원국을 대상으로 사이버공격을 감행한 중국・북한・러시아 등 3개국 기관에 대하여 자산을 동결하고 관련자를 입국 금지 조치하는 등 첫 제재를 단행하였다[22]. 이 조치는 EU가 2019년 4월 사이버보안법을 결의한 이후 처음 단행된 조치로 증가하는 사이버공격을 단호히 대처하겠다는 강력한 의지를 반영한 것이다. 이는 사이버안보를 위한 커다란 진전으로 사이버공간에서의 악의적 행위자들에 대한 효과적인 조치가 될 것이다. 또한, 우리나라는 2022년 5월 개최된 한미정상회담에서 미국과 사이버안보 전반에 걸쳐 적극적으로 협력하기로 합의하였다[22]. 그러나 사이버공격의 주체를 식별 및 특정하고 대응하기 위한 국제협력은 적극적이나 사이버공격으로 발생한 피해에 대한 제재를 단행한 사례는 없으므로 무엇보다 국제협력을 통한 제재를 적극적으로 실천하여 사이버 억지력(Cyber Deterrence)을 강화하는 노력이 필요할 것이다.

5. 결 론

주요 위협국이 실시하는 사회공학 공격의 사례를 분석한 결과 지정학적 공격전술인 심리전과 유사한 공격방법을 선호하는 것으로 나타났다. 중국은 질보다 양으로 공격하는 상대적으로 단순한 공격인 피싱공격을 선호하며, 공격에 대한 정보수집은 광대한 네트워크를 반영하듯 더욱 광범위해졌다. 러시아는 지정학적 전술처럼 은밀하고 복잡한 공격을 선호하였고 업무관계를 이용한 스피어 피싱 공격을 주로 시도하였다. 특히 국가주도의 공격인 만큼 대상국가의 국가시설 및 환경에 관한 정교한 정보를 활용해 성공률을 높이는 특징을 보였다. 북한의 사회공학 공격은 대상목표에 따라 공격형태가 변화한 것으로 분석되었다. 미국과 한국에 대해서는 지정학적 전술과 유사하게 스피어 피싱과 워터링홀로 정보탈취를 하는 반면, 그 외

에 국가는 랜섬웨어 공격으로 자금확보를 목표로 하는 특징을 보였다.

이와 같은 주요 위협국의 사회공학 공격의 특징에 따른 사회공학 공격의 대응전략도 위협 국가별로 맞춤형 대응전략을 제시하였다. 중국은 대량의 정보를 탈취하는 공격을 이용한다는 점에서 신뢰할 수 없는 장비의 사용을 제재한다는 내용의 클린패스 정책을 제시하였고 러시아의 스피어 피싱 공격은 망각주기를 고려한 지속적인 의무교육의 정책반영을 제시하였으며, 북한은 사이버공격의 단호한 대처에 대한 강력한 의지를 반영한 국제적인 제제의 실천을 제시하였다.

본 연구의 제한사항은 다음과 같다. 사람이 직접 사례를 사회공학 사이클 모델에 적용하여 분석한 만큼 분석결과에 대한 검증방법을 제시하지 못한 점이다. 그러므로 차후 연구에는 수기로 분석한 본 연구 이후 발생한 사회공학 공격사례를 자연어처리 인공지능 모델과 같은 적합한 모델로 학습시켜 수기 분석한 결과와 동일하게 나오는지 검증하는 연구가 필요하다. 또한, 주요 위협국인 중국, 러시아, 북한 외 해킹그룹에 대한 사회공학 공격도 추가연구가 진행되어야 할 것이다.

이렇게 다양한 국가 및 해킹그룹에서 이루어지는 사회공학 공격사례를 지속적으로 분석한다면 위협주체에 대한 특징적인 사회공학 공격을 분류할 수 있을 것이며, 공격의 변화도 예측할 수 있으리라 기대한다.

참고문헌

[1] 채재병, “국제 사이버공격 전개양상 및 주요국 대응전략,” 국가안보전략연구원, 2019.

[2] 김영희, “다크 웹(Darkj Web) 산업 현황 보고서,” 한국저작권위원회, 2023.

[3] IBM Corporation, “X-Force Threat Intelligence Index 2022,” IBM February 2022, pp. 16, 2022.

[4] 신규용, 김지원, 임현명, 김용주, 유진철, “사회공학 사이버작전 분석모델 정립연구,” 정보보호학회논문지, 제28권 제6호, pp. 1595-1606, 2018.

[5] Christian Nicholson, “Social Engineering Attacks,” SANS Security Awareness, 2020.

[6] 국립국어원, “https://stdict.korean.go.kr/main/main.do,” (검색일 : 2023.08.01.).

[7] 보안용어사전, “https://www.ahnlab.com/kr/site/ securityinfo/dictionary/dictionaryList.do,” (검색일 : 2023.08.01.).

[8] Kevin D. Mitnick and William L. Simon, “The Art of Deception: Controlling the Human Element of Security,” USA: Wiley, 2002.

[9] Hadnagy Christopher, “Social Engineering : The Art of Human Hacking,”Hoboken. NJ. USA: Wiley, 2012.

[10] FireEye, “World War C:오늘날 지능형 사이버 공격 배후 국가들의 동기 이해,” 2014.

[11] Symantic, “2013 Internet Security Threat Report,” pp 8, 2013.

[12] TREND MICRO, “Threat Report and Forecast,” 2008.

[13] 김윤종, “평창올림픽 개막식 주범은 러 軍정보기관(2020.10.21.),” 동아일보, https://www.donga.com/news/ Inter/article/all/20201021/103543224/1 (검색일: 2023.07.10.).

[14] 송태은, “러시아-우크라이나 전쟁의 사이버전: 평가와 함의,” 국립외교원 외교보안연구소, pp.11, 2022.

[15] 최형주, “코로나19정보 위장한 사이버 공격 총정리(2020.03.19.),” CCTV NEWS, https://www.cctvnews.co.kr/news/articleView.html?idxno=160837, (검색일: 2023.08.02.).

[16] 주형식, “북, 0.01초만에 악성코드 심었다(2023.04.19.),” 조선일보, https://www.chosun.com/national/2023/04/19/CMBJFM6II5B6LDYDK2OTHHTFJA/, (검색일: 2023.08.02.).

[17] 보안뉴스, “北 추정 A·B·C 해커그룹의 한글문서 공격 집중분석(2018.03.06.),” https://www.boannews.com/media/view.asp?idx=67270, (검색일: 2023.08.02.)

[18] U.S. MISSION KOREA, “ANNOUNCING THE EXPANSION OF THE CLEAN NETWORK

TO SAFEGUARD AMERICA'S ASSETS," U.S. Embassy & Consulate in the Republic of Korea, 2020.

[19] 인세영, "유럽 전역, 중국 화웨이 5G 철거 시작 (2021.05.21.)," 파이낸스투데이, https://www.fntoday.co.kr/news/articleView.html?idxno=256640, (검색일: 2023.08.02.).

[20] 국가안보실, "국가사이버안보전략서," 2019.

[21] 채재병, 김일기, "사이버안보 역량 강화를 위한 국제협력 방안," 국가안보전략연구원, 2020.

[22] 김보미, 오일석, "북한 사이버위협의 특징과 대응방안: 김정은 시대를 중심으로," 국가안보전략연구원, 2022.

[23] 국가정보원, "2023 국가정보보호백서," 2023.

[24] 외교부, "북한 정권을 위해 정보·기술 탈취해 온 해킹조직 '김수키' 겨눈다," 공동보도자료, 2023.06.02.

[25] 신용희, "국가 지능화를 위한 초신뢰 네트워크," ETRI Insight Report 2019-22, 2019.

[26] 이동휘, 최경호, 이동춘, 김귀남, 박상민, "사회공학기법을 이용한 피싱 공격 분석 및 대응기술," 융합보안논문지, 제6권 제4호, pp. 171-177, 2006.

[27] 박영후, 신동천, "사회공학 공격에 대한 기업 조직의 위험 수준 평가 방안," 융합보안논문지, 제19권 제1호, pp. 103-110, 2019.

〔저 자 소 개〕

김 지 원 (Jeewon Kim)
2002년 2월 동국대학교 학사
2016년 8월 연세대학교 정보보호 석사
2021년 2월 아주대학교 공학박사
2019년 10월 ~ 2021년 11월
국방보안연구소 방산보안실 책임연구원
2022년 3월 ~ 현재
상지대학교 군사학과 조교수
email : phdkjw22@sangji.ac.kr