사회공학 공격 사례를 통한 개선된 사회공학 공격 사이클 연구

박상준*, 김지원**
*아주대학교 장위국방연구소
**상지대학교 군사학과
e-mail: sigpsj13438@naver.com, phdkjw22@sangji.ac.kr

Study on improved social engineering attack cycle through social engineering attack cases

Sangjun Park*, Jiwon Kim**
*Jangwee Research Institute for National Defense, Ajou University
**Dept. of Military Science, Sangji University

요 약

융·복합시대의 사이버 공격은 기술적 방법보다는 피해자를 속여 정보를 유출하는 고효율적인 사회공학적 공격이 주를 이루고 있다. 이러한 공격 방식은 특별한 기술력이 요구되지 않아 더욱 빈번하게 발생하고 있으며, 이에 따라 정보를 취급하는 기관과 조직에 대한 피해가 더욱 커지고 있으므로 공격자들이 다양한 기법과 심리적 메커니즘을 어떻게 활용하는지에 대한 심층적인 연구도 꾸준히 필요하다. 본 연구에서는 과거 성공적인 사회공학적 공격 사례를 공격에 사용된 정보 요소의 빈도와 패턴을 도출 및 분석하여 이를 기반으로 사이버공간 특화 개선된 사회공학 공격 사이클을 제안한다. 이 모델을 적용하여 향후 사회공학적 사이버 공격패턴을 빠르게 예측하여 즉각적으로 방어할 수 있는 체계적인 대응 방안을 마련할 수 있을 것으로 기대된다.

1. 서론

융복합 시대의 도래로 많은 업무가 사이버 공간에서 이루어지며, 이에 따라 사이버 보안이 물리적 보안보다 더 중요해지고 있다. 특히 산업 보안 분야에서는 디지털화와 기술 융합이 가속화되면서 사이버 영역에 대한 선호가 높아지고 있다. 과거 해커들은 호기심이나 과시를 목적으로 시스템에 침입하곤 했으나, 현재는 국가 주도적 해킹 그룹을 제외한 대부분의 해커들이 금전적 이익을 목표로 하고 있다. 이들은 개인의 일탈보다는 조직적인 형태로 활동하며, 점점 더 효율적이고 성공확률이 높은 공격 기법을 선호하는 경향을 보인다.

조직적으로 활동하는 해커들은 사이버 공격의 초기 침투 과정에서 사회공학(Social Engineering, 이하 SE) 공격을 주로 이용한다[1]. 사회공학 공격은 사람의 심리를 조작하여 공격자가 원하는 방향으로 목표를 달성하는 방식이다. 시스템의 취약점은 기술로 방어할 수 있지만, 아무리 완벽히 시스템을 보호하더라도 사람의 개입이 필요한 지점이 반드시 존재하게 된다. 공격자는 이러한 인간적 요소를 노려 사회공학적 기법을 통해 시스템을 침투하는 것이다. 이는 고대 그리스·로마 시절의 “트로이 목마”부터 현재까지 지속적으로 사용되고 있는 공격이다.

사회공학에 관한 기존 연구는 주로 케빈 미트닉(Kevin D. Mitnick, 2002)의 사회공학 라이프 사이클(SE Life Cycle)과 크리스토퍼 헤드네기(Christopher J. Hadnagy, 2012)의 사회공학 프로세스(SE Process)를 중심으로 물리적 접촉을 기반으로 연구가 진행되어 왔다. 대표적인 공격 기법으로는 쓰레기통 뒤지기(Dumpster Diving)나 어깨너머 훔쳐보기(Shoulder Surfing)가 있으며, 이러한 공격들은 주로 신뢰 관계를 형성하는 것을 전제로 한다. 하지만 이러한 모델은 피싱(Phishing), 스미싱(SMSishing), 웨일링(Whaling) 등 신뢰 관계가 없는 공격에는 한계가 존재한다. 또한, 공격자가 목표를 달성하지 못했을 경우 다시 정보 수집 단계로 돌아가 공격을 시도하는 과정도 기존 모델에서는 충분히 설명되지 않는다.

따라서 본 연구는 다양한 사회공학 공격 사례를 수집하고, 공격 기술을 도출한 후, 각 기술의 심리적 영향을 판단하여 기존 연구된 사회공학 공격 사이클에 개선된 사회공학 공격 모델을 제시하고자 한다.

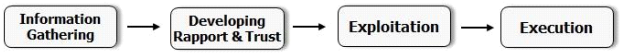
2. 사회공학 모델 분석

2.1 사회공학 라이프 사이클

케빈 미트닉(Kevin D. Mitnick)과 윌리엄 시몬(William L. Simon)의 사회공학 라이프 사이클(SE Life Cycle) 모델은 라포(Rapport) 또는 신뢰(Trust)를 형성하기 위해 정보를 수집

하고, 수집된 정보를 바탕으로 피해자의 취약점을 공격하는 일련의 과정을 포함한 모델이다. 이 과정은 [그림 1]에서 설명된 단계로 구성된다.

이 중 라포 및 신뢰 발전(Developing Rapport & Trust) 단계는 주로 사기(fraud)나 스파이 활동과 같은 첩보 활동(HUMINT: Human Intelligence)을 통해 정보를 수집하는 방법이며, 물리적인 접촉이 요구된다. 이는 공격자가 시간을 두고 신뢰를 발전시키는 방식으로 피해자와 지속적인 관계를 맺고 공격을 수행한다.

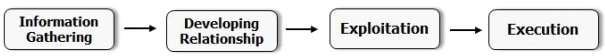


[그림 1] Social Engineering Life Cycle[2]

2.2 사회공학 공격 프로세스

크리스토퍼 헤드네기(Christopher J. Hadnagy)는 사회공학 프로세스(SE Process)를 제안했다. 이 프로세스는 사회공학의 심리적 특성을 잘 반영한 공격 모델로, 보안 전문기관과 학계에서 사회공학 공격을 설명할 때 주로 활용되며, 사회공학 연구와 관련된 많은 논문에서 인용되고 있다.

헤드네기의 모델은 장기적 관계나 신뢰 구축을 중요시 하는 케빈 미트닉의 모델과는 달리, 반드시 신뢰를 형성하지 않고, 일시적 관계(relationship)나 상황적 취약성을 이용하여 공격을 빠르게 진행하는 데 중점을 둔다. 이러한 과정은 [그림 2]에서 설명된 단계로 구성되며, 공격자는 관계 형성의 필요성을 낮추고 공격 기법을 더 유연하게 적용하여 상황에 따라 빠르고 효율적인 공격을 목표로 한다.



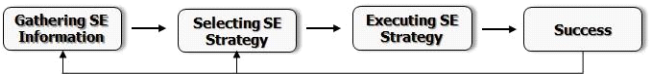
[그림 2] Social Engineering Process[3]

2.3 사회공학 사이클

사회공학 사이클(SE Cycle)은 비교적 최근에 연구된 사회공학 공격 모델로, 공격자가 공격에 실패할 경우, 전략(stratgy) 실행 단계를 제외하고 다시 정보 수집 및 사회공학 방략 선택 단계로 돌아가 목표를 달성하려는 과정을 설명한다. 이러한 과정은 [그림 3]에서 나타낸 것처럼 순환적으로 이루어진다.

이 모델은 간결하고 효율적인 공격 구조, 실패 후 유연한 재시도 가능성, 단순화된 접근 방식, 그리고 각 단계에서 정보를 축적해 최적화된 전략을 적용할 수 있다는 점에서 케빈 미트닉과 크리스토퍼 헤드네기의 모델보다 더 개선된 모델이고 현재의 사회공학 공격과 가장 유사한 패턴을 보인다.

그러나 이 모델은 기술 선택과 심리적 요소를 분리하지 않기 때문에, 공격의 세밀한 계획이나 심리적 취약점을 분석하는 과정에서 한계가 있을 수 있다. 또한, 공격자의 심리적 기제를 고려한 과정이 없으므로, 목표 대상자의 심리적 반응을 세밀하게 고려한 공격 전략을 수립하는 데는 다소 한계가 있다.



[그림 3] Social Engineering Cycle[4]

3. 사회공학 공격 사례 분석 결과

사회공학 공격이 언론 매체에 거론되기 시작한 2007년부터 현재까지의 공격 사례를 수집하였다. 공격 사례는 국내외 주요 언론사 기사와 국가 및 공공기관의 공격 보고서(브리핑 자료)를 기반으로 하여, 총 187건의 주요 공격 사례를 수집하고 분석하였다. 수집된 정보를 바탕으로 공격 기술을 체계적으로 정리한 결과는 [표 1]과 같다. 이러한 과정을 통해 연구의 전문성과 신뢰성을 강화하였다.

[표 1] 정보수집에 따른 사회공학 공격 선택 순위

* () : 사이버 공격 횟수

Gathering Information	Selecting Technology	Rank
Facility (5)	Spear phishing (3)	1
	Baiting (2)	2
Culture (2)	Spear phishing (2)	1
Profile (3)	Spear phishing (2)	1
	Phishing (1)	2
Business (18)	Spear phishing (10)	1
	Phishing (3)	2
	Pharming (2)	3
	SMShihing (1) Whaling (1) Watering hole (1)	etc.
Relationship (28)	Spear phishing (10)	1
	Phishing (4) Pharming (4) Baiting (4)	2
	SMShihing (3)	3
	Whaling (1) Watering hole (1) Vishing (1)	etc.
Character / Movie (10)	Baiting (4)	1
	Spear phishing (3)	2
	Phishing (1) SMShihing (1) Watering hole (1)	etc.
Social issue (6)	Phishing (3)	1
	Baiting (2)	2
	SMShihing (1)	etc.

사회공학 공격은 사람의 심리 요소를 반영한 공격이므로, 이에 적용된 공격 기술을 분석한 결과는 [표 2]와 같다. 공격자들이 자주 사용하는 주요 공격 기법으로는 스피어 피싱, 베

[표 2] 사회공학 공격에 따른 심리선택 순위

* ( ) : 사이버 공격 횟수

Selecting Technology	Selecting Psychology		Rank
	Cognitive Psychology	Social Psychology	
Phishing (18)	curiosity (9)	prospect theory (5)	1
		schema (4)	2
	expertise (4)	prospect theory (2)	-
		schema (2)	
	salience (4)	prospect theory (2)	-
		schema (2)	
	urgency (1)	obedience (1)	
Spear phishing (43)	salience (24)	schema (9)	1
		expectancy theory (6)	2
		responsibility (5)	3
		obedience (1)	-
		compliance (1)	
		prospect theory (1)	
		In-group bias (1)	
	expertise (13)	schema (6)	1
		responsibility (2)	2
		In-group bias (2)	
		expectancy theory (2)	
		obedience (1)	-
	urgency (4)	schema (2)	1
		cognitive miser (1)	
		expectancy theory (1)	
	curiosity (2)	expectancy theory (2)	
Pharming (5)	expertise (8)	schema (4)	-
		expectancy theory (4)	
SMShihing (12)	urgency (7)	expectancy theory (4)	1
		schema (3)	2
	salience (3)	expectancy theory (1)	-
		schema (1)	
		In-group bias (1)	
	expertise (2)	expectancy theory (1)	-
		schema (1)	
Vishing (2)	expertise (2)	schema (1)	-
		obedience (1)	
Watering hole (4)	salience (2)	In-group bias (1)	1
	expertise (1)	expectancy theory (1)	-
	curiosity (1)	expectancy theory (1)	
Whaling (3)	salience (3)	schema (1)	-
		obedience (1)	
		responsibility (1)	
Baiting (22)	salience (7)	expectancy theory (3)	1
		schema (2)	-
		prospect theory (2)	
	curiosity (7)	expectancy theory (5	1
		schema (2)	-
	expertise (4)	prospect theory (2)	1
		schema (1)	-
		expectancy theory (1)	
	urgency (4)	prospect theory (2)	1
		schema (1)	-
		expectancy theory (1)	

이팅, 피싱, 스미싱 순으로 나타났다.

187건의 공격 사례 중 스피어 피싱은 43건(22.9%)으로 가장 많이 발생한 공격 기술로, 현저성(salience)이 가장 중요한 심리 기제로 작용하며, 전문성과 책임성도 주로 사용된다. 현저성은 공격 대상자의 주의를 끌어 특정 정보에 집중하게 만드는 심리적 요소이며, 책임성은 대상자가 다른 사람의 기대에 부응하려는 심리를 자극하여 공격자의 요청에 복종하도록 유도한다.

다음으로 베이팅은 22건(11.7%)으로, 공격 대상의 욕구나 호기심을 기반으로 한 공격 성향을 보였다. 베이팅은 주로 인지 심리학에서의 현저성과 호기심을 활용하며, 사회 심리학의 기대이론(expectancy theory)을 통해 보상 심리를 자극하여 잘못된 판단을 유도하는 패턴을 보였다.

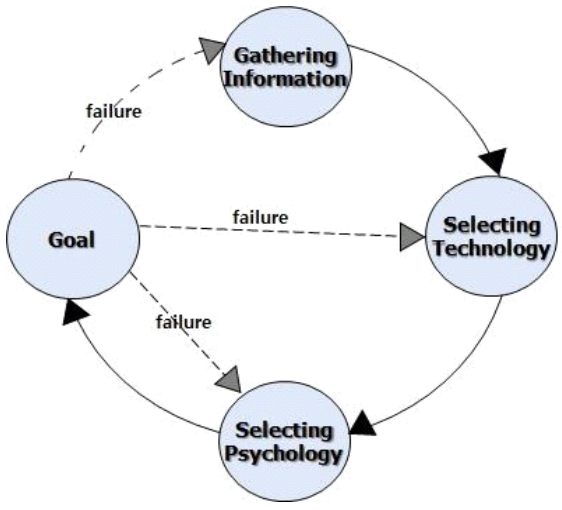
피싱 공격은 18건(9.6%)으로, 공격 대상자의 호기심을 자극하여 관심을 끌어낸 후, 도식화와 기대이론을 활용해 공격을 수행하는 패턴을 보였다.

마지막으로 스미싱은 12건(6.4%)의 빈도로 나타났으며, 주로 급박성을 이용하여 공격하는 특성을 보였다. 스미싱 공격자는 공격 대상의 급박한 심리를 이용하여, 기대이론과 연계된 공격 패턴을 통해 행위에 대한 결과를 기대하게 만드는 방식으로 공격을 수행하였다.

이와 같은 사례 분석을 통해 정보수집에 따른 공격의 기술 선택, 그리고 공격기술에 따른 심리를 선택한 결과는 기존의 사회공학 모델로는 인과관계에 한계가 있음을 알 수 있다.

4. 개선된 사회공학 공격 모델

본 연구에서 제안하는 개선된 사회공학 공격 모델은 [그림 4]와 같다. 개선된 사회공학 공격 모델인 사회공학 사이버 공격 사이클(SE Cyber Attack Cycle)은 물리적 영역을 배제하고 사이버 영역에서 사람을 대상으로 이루어지는 공격을 전제로 한 순환적 구조 모델이다.



[그림 4] Social Engineering Cyber attack Cycle

이 모델은 기존에 제시한 모델에 비해 여러 가지 장점은 다음과 같다.

첫 번째, 유연한 실패의 대응이다. 이 모델의 가장 큰 장점은 공격이 실패했을 때 유연하게 각 단계로 되돌아가 공격을 다시 시도할 수 있다는 것이다. 공격자가 목표 달성에 실패하면, 단순히 종료되는 것이 아니라 정보 수집(Gathering

Information), 기술 선택(Selecting Technology), 또는 심리 선택(Selecting Psychology) 단계로 다시 돌아가 공격을 재조정할 수 있다. 이와 같은 반복적인 피드백 구조는 공격의 성공 확률을 높이는 데 중요한 역할을 한다.

두 번째, 단계적 접근의 명확성이다. 정보 수집, 기술 선택, 심리 선택, 목표 달성의 각 단계를 명확하게 구분하고 있으며, 공격자가 각 단계를 체계적으로 따라가면서 공격 전략을 구체화할 수 있다. 각 단계에서의 성공과 실패를 피드백 루프로 다루기 때문에, 공격자는 다음 단계에서 더 나은 결정을 내리기 위해 필요한 데이터를 확보할 수 있다.

세 번째, 심리적 요소와 기술적 요소의 분리이다. 공격자는 특정 상황에서 심리적 취약점을 공략할 때 필요한 심리적 기제를 선택하면서도, 동시에 공격에 적합한 기술을 선택할 수 있는 유연한 전략을 수립할 수 있다.

마지막 장점으로는 실패에 따른 다중 시도 가능성이다. 공격자가 다양한 경로로 실패에 대응할 수 있다. 예를 들어, 공격이 실패했을 경우, 단순히 정보 수집으로 돌아갈 뿐 아니라, 기술 선택이나 심리 기제 선택 단계를 수정하여 새롭게 시도할 수 있다. 이는 기존 모델들이 주로 단일한 실패 시나리오에 대응하는 것과는 다르게, 다양한 시나리오에 맞춘 다중 시도가 가능하다는 장점을 가지고 있다.

5. 결론

최근 융·복합 기술의 발달과 함께 사이버 공간에서의 업무와 상호작용이 점점 더 복잡해지고 있으며, 이로 인해 사회공학 기법을 활용한 사이버 공격 또한 급격히 증가하고 있다. 이러한 공격들은 점차 교묘해지고 다변화되고 있지만, 기존 사회공학 연구는 기술적 또는 심리적 관점에만 초점을 맞추어 현시점에서 발생하는 복잡한 융·복합 환경의 사회공학 공격을 충분히 설명하지 못하는 한계를 보여주었다.

본 연구에서는 최근 사이버 영역에서 발생하는 사회공학 공격을 더욱 정확하게 분석하기 위해 사회공학 사이버 공격 사이클(SE Cyber Attack Cycle) 모델을 제안하였다. 이 모델은 공격자의 관점에서 실제 공격 사례를 적용하고 분석함으로써, 융·복합 기술이 접목된 환경에서 나타나는 사이버 공격의 의미 있는 패턴을 파악하고자 하였다. 분석 결과, 공격자가 수집한 정보의 유형에 따라 선호하는 공격 기술이 달라지며, 각 공격 기술에서 활용되는 심리적 기제도 명확히 구분할 수 있음을 확인하였다.

따라서 본 연구의 결과는 융·복합 시대의 산업보안에서 사회공학적 사이버 공격의 성공률을 높이는 시나리오를 설계하는 데 활용될 수 있다. 또한, 방어 측면에서 유출된 정보를 신속하게 분석하여 예상되는 공격 유형을 예측하고, 이를 바탕으로 산업 환경에 맞는 효율적인 대응 전략을 마련할 수 있을 것으로 기대된다. 이는 디지털 전환과 산업 보안이 밀접하게 연관된 현대의 보안 환경에서 효과적인 방어체계 구축에 중요한 기여할 수 있을 것이라 기대한다.

참고문헌

[1] Ministry of Science and ICT, “Cyber Security Forecast 2023”.

[2] K. D. Mitnick, W. L. Simon, The Art of Deception: controlling the human element of security, Indianapolis, IN: Wiley, 2002, pp.368.

[3] C. J. Christopher, Social Engineering: the art of human hacking, Hoboken, NJ: Wiley, 2012.

[4] K. Shin, J. Kim, H. Lim, Building an analysis model for social engineering based cyberspace operations, Journal of Korea Institute of Information & Cryptology. 28(6), 2018, pp. 1595-1606.

[5] P. P. Pathy, G. Rajendran, Identification and Prevention of Social Engineering Attack on an Enterprise, International Carnahan Conference on Security Technology (ICCST). IEEE, Oct. 2019, pp. 1-5.

[6] K. Ivaturi, L. Janczweski, A Taxonomy for Social Engineering Attack, International Conference on Information Resources Management. Centre for Information Technology, Organizations, and People, 2011, pp. 1-12.

[7] F. Mouton, L. Leenen, H. S. Venter, Toward an Ontological Model Defining the Social Engineering Domain, In IFIP International Conference on Human Choice and Computers, Springer, Berlin, Heidelberg, 2014, pp. 266-279.

[8] K. Zheng, T. Wu, X. Wang, B. Wu, C. Wu, A Session and Dialogue – based social engineering framework”, IEEE Access, May 2019, pp. 67781-67794.

[9] Fan, Wenjun, K. Lwakatare, R. Rong, Social Engineering: I-E based model of human weakness for attack and defense investigations, International

[10] Journal of Computer Network & Information Security, vol.1, Jun 2017, pp. 1-11.

[11] Jeewon Kim. "Social Engineering Cyberattack Framework." Doctoral Thesis Ajou University, 2021. Gyeonggi-do, South Korea.