북한 사이버 공격 변화에 따른 향후 전망과 대응[1)]

김성진 | 한국수출입은행 차장 | sungjin.kim@koreaexim.go.kr

Ⅰ. 머리말

비대칭 전력은 상대적으로 군사력이나 자원이 열악한 국가나 특정 세력이 자신들보다 우세한 상대를 대상으로 사용하는 비정규적이고 비균형적인 공격 수단으로 대량 살상 및 기습 공격, 게릴라전이 가능한 무기체계를 의미한다. 비대칭 전력 활용한 공격은 예상하지 못한 의외성을 바탕으로 공격을 시도하기 때문에 공격받는 입장에서는 신속하게 대처하기 어려운 상황에 직면한다.[2)] 대표적인 비대칭 전력으로는 핵・미사일(ICBM, SLBM 등), 생화학 무기 등을 언급할 수 있으며, 최근에는 IT 기술이 발전하면서 새로운 비대칭 전력으로 사이버 공격(해킹, SNS 등을 통한 심리전 등), 드론 및 무인기를 활용한 공격이 주목받고 있다. 특히, 사이버 공격은 일상생활에 필요한 서비스들이 인터넷을 기반으로 작동하고 있는 현대 사회에서 가장 큰 피해를 유발할 수 있는 비대칭 전력이다. 또한 사이버 공격은 핵무기, 생화학 무기와 비교했을 때 상대적으로 적은 비용으로 운용이 가능할 뿐 아니라 실제 공격 주체의 신원이 명확하게 드러나지 않는다는 점에서 공격 시도에 대한 보복 공격이 발생할 가능성이 낮은 장점으로 가장 많이 사용되고 있는 비대칭 전력이다.

북한은 사이버 공격을 위해 국가 차원에서 해킹 그룹을 육성하고 관리하고 있다. 북한의 해커들이 본격적으로 사이버 공격을 전개하던 초기(2000년대)에는 주로 남한, 미국 등을 대상으로 사회적 혼란 유발과 정보 탈취를 목적으로 공격을 시도했다. 그러나 대북제재가

1) 본고는 다음 논문을 요약하였다. 김성진, 「북한의 가상자산 탈취 및 자금세탁 방법 변화 양상에 대한 연구"를 요약 및 보완」, 『평화학연구』, 제26권 제2호, 2025, pp.31~52.
2) Montgomery Meigs, ed. US Army War College Editorial Board, "Unorthodox Thoughts about Asymmetric Warfare," *Parameters: Journal of the US Army War College*, Carlisle, PA: US Army War College, 2003, p.4.

강화되면서 대외무역, 해외 노동자 파견 등 주요 외화 벌이 사업에 제약이 생기면서 사이버 공격의 성격도 변화하고 있다. 최근 북한은 국가 차원에서 해킹 그룹을 구성하고, 수익을 목적으로 하는 다양한 사이버 공격을 전 세계 불특정 다수를 향해 시도하고 있다. 특히, 전통적인 금융시스템과 비교할 때 상대적으로 보안이 취약하고, 자금세탁이 용이한 가상자산을 목적으로 하는 사이버 공격이 증가하고 있는 모습을 보이고 있다.

다만, 미국을 중심으로 가상자산 및 관련 산업들이 제도권으로 편입되고, 이를 관리할 수 있는 다양한 법・제도가 구축되고 있다는 점에서 북한의 사이버 공격 방식의 변화가 예상된다. 따라서, 본고에서는 북한의 사이버 공격 진행 현황과 공격 방식의 주요 특징을 살펴보고 이를 바탕으로 향후 북한의 사이버 공격이 변화할 방향을 예측하고 이에 대한 대응 방안을 모색해 보고자 한다.

Ⅱ. 북한 사이버 공격 변화 과정

북한의 사이버 공격 준비는 1986년 김일성의 지시로 미림대학을 설립하고 100여 명의 컴퓨터 전문 요원을 양성하면서 시작했다. 이후, 1991년 발생한 걸프전에서 미국이 다양한 전자 장비를 활용한 사이버 공격을 통해 이라크군의 방공망을 무력화시키는 모습이 전 세계에 중계되면서 본격적으로 사이버 공격을 위한 준비를 시작한다. 걸프전 이후 김정일은 인민군 총참모부 산하에 '지휘자동화국'을 창설하고, 심리전을 포함한 다양한 사이버 공격을 수행할 수 있는 인력과 관련 프로그램을 개발하는 전문 인력 양성에 집중하기 시작했다.[3)]

북한의 해커들은 2000년대에 들어서면서 본격적으로 사이버 공격을 활용한 광범위한 대남 도발을 실시한다. 당시 북한 사이버 공격의 주목적은 인터넷 기반에서 제공되는 서비스를 불능 상태로 만들어 남한 사회 전반에 혼란을 유도하고, 이를 바탕으로 광범위한 대남 심리전을 실시하는 것이었다.[4)] 북한은 남한 사회에서 사용 빈도가 높은 정부의 홈페이지 및 민간 포털 사이트 등을 주요 공격 대상으로 정하고, 디도스(Distributed Denial of Service Attack: DDoS)[5)] 공격을 통해 서비스 이용에 장애를 발생시킴으로써 사회적 혼란을 유도했다.

2009년 북한이 남한과 미국을 대상으로 실시한 대규모 디도스 공격인 '7.7 디도스 대란'은

3) 고명현, 「북한의 사이버 전력(戰力)과 금융범죄」, 『KDI 북한경제리뷰』, 10월호, 2021, p.56.
4) 상대적으로 인터넷 보급률이 저조하던 과거에는 주요 정부 기관의 웹사이트가 공격 대상이었으나 IT기술의 발달로 일상의 많은 영역이 온라인상에서 진행됨에 따라 금융기관 및 민간 포털 사이트 등 광범위한 사이버 공격이 진행되었다.
5) 분산 서비스 거부 공격(Distributed Denial of Service Attack: DDoS)은 공격자가 최대한 많은 PC를 악성코드에 감염시킨 뒤 특정 서버, 사이트 등에 동시접속을 함으로써 과도한 트래픽을 발생시켜 정상적인 서비스 제공이 불가능하도록 하는 공격방법이다.

국내 주요 22개 사이트와 미국의 14개 사이트를 마비 시켰다. 당시 공격을 받은 국내 사이트들은 최대 72시간까지 접속 장애를 겪었으며, 공격에 사용된 악성코드는 감염된 PC의 하드디스크를 자동으로 파괴하도록 설정된 프로그램이 포함되어 있어서 많은 피해를 발생시켰다. 2009년 대규모 디도스 공격을 시작으로 북한은 지속적으로 사이버 공격 방법을 고도화 시키면서 국내 주요 기관들을 대상으로 사이버 공격을 통한 교란 및 정보 탈취를 시도했다.

2016년을 전후하여 북한의 사이버 공격은 기존과 다른 양상으로 전개된다. 이러한 변화는 주요 물품에 대한 수・출입 제한 및 SWIFT 시스템에서 퇴출 등 대북제재가 강화되면서 기존 외화 벌이 사업에 많은 제약이 발생한 것이 원인으로 추정된다. 이 시기 북한의 사이버 공격의 성격은 불특정 다수를 대상으로 수익 추구를 강화하는 모습으로 변하기 시작한다.

북한의 사이버 공격이 수익성 추구로 변화한 초기에는 주로 금융기관들을 대상으로 외화 탈취를 시도했다. 북한이 2015~19년 동안 17개국을 대상으로 은행의 SWIFT 시스템과 ATM 단말기 네트워크 해킹 공격을 통해 약 20억달러를 탈취한 것으로 추정하고 있다.[6)]

다만, 최근 북한의 사이버 공격 대상을 살펴보면 전통적인 금융기관 보다는 가상자산 거래소 및 관련 기업, 가상자산 투자자 등에 집중되는 모습을 보여주고 있다. 대표적인 블록체인 데이터 분석 기업인 체이널리시스의 보고서에 따르면, 전 세계적으로 발생하는 가상자산 관련 범죄에 가장 적극적인 단체는 북한의 해킹 그룹으로 파악되고 있으며, 이들이 탈취한 가상자산은 핵・미사일 개발의 재원으로 사용되는 것으로 추정되고 있다.

〈표 1〉 북한 사이버 공격의 시기별 주요 목적 및 특징

단계별 구분	주요 목적	대표사례	특징
초기 (2000~10)	- 시스템 교란 - 정보 수집	- 7・7 디도스 대란(2009)	- DDoS 공격 방법을 활용한 단순 공격
고도화・다양화 (2010~15)	- 인프라 파괴 - 정보 수집	- 농협 전산망 마비(2011) - 3・4 디도스 대란(2011) - 한수원, 소니픽쳐스 해킹(2014)	- APT, 스피어피싱 등 공격 방법의 고도화
수익 중심, 글로벌 확장 (2016~20)	- 외화 확보 - 금융시스템 교란 - 첨단 기술 탈취	- 방글라데시 중앙은행 해킹(2016) - 워너크라이 랜섬웨어 공격(2017) - 업비트 해킹(2018)	- 암호화폐 주요 표적 - 랜섬웨어 공격을 통한 공격 대상 확대
다차원적 공격 (2021~25)		- 로닌 브리지 해킹(2022) - 바이비트 해킹(2025) - 위장취업을 통한 정보 및 금전 탈취	- 보안시스템 강화 및 국제사회의 규제에 대응한 사회 공격 수법의 고도화

자료: 김성진, 「북한의 가상자산 탈취 및 자금세탁 방법 변화 양상에 대한 연구」, 『평화학연구』, 제26권 제2호, 2025, p.36.

6) Panel of Experts on the DPRK, "Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee," UN Doc., S/2019/691, New York: United Nations, 2019, p.26.

Ⅲ. 최근 북한 사이버 공격의 주요 특징

1. 랜섬웨어 공격을 통한 갈취

사이버 공격을 통한 수익을 추구하는 방법은 협박에 의한 갈취와 해킹을 통한 직접적 탈취로 구분할 수 있다. 북한 해킹 그룹이 사이버 공격을 시작한 초기에는 랜섬웨어 공격을 통한 갈취의 방법을 활용했다. 랜섬웨어(Ransomware)는 몸값(Ransome)과 소프트웨어(Software)의 합성어로 공격 대상자의 컴퓨터 및 네트워크에 악성코드를 설치하여 공격받은 컴퓨터를 장악한 뒤 일종의 몸값을 요구하는 방식으로 공격이 진행된다. 랜섬웨어는 공격 방식에 따라 여러 유형으로 존재하고 있으며, 대표적인 공격 유형은 스크린 로커(Screen Locker), 암호화 랜섬웨어(Encrypting Ransomeware), 독스웨어(Doxware), 서비스형 랜섬웨어(Rass) 등이 있다.

대중적으로 알려진 랜섬웨어 공격 방식은 스크린 로커와 암호화 랜섬웨어 방식으로 공격 대상에 침투한 악성코드는 피해자의 컴퓨터(혹은 네트워크) 접속 자체를 제한하거나 보유하고 있는 데이터를 암호화 시킨뒤 이를 복구해 주는 대가로 금전을 요구하는 방식이다. 대표적인 사례로 2017년 북한의 해킹 그룹 라자루스가 주도한 '워너크라이(WannaCry)' 랜섬웨어 공격이 있다. 해당 공격은 라자루스가 수익을 목적으로 불특정 다수를 대상으로 시행된 대규모 사이버 공격이었으며, 약 150개국 23만대의 PC 및 서버가 직접적 피해를 본 것으로 알려졌다.[7] 라자루스는 피해자들에게 공격당한 시스템을 정상화시켜주는 조건으로 가상자산을 요구했으나 대부분의 피해자가 몸값을 지불하지 않고 데이터 복구를 포기하는 선택을 했다. 그 결과, 라자루스가 몸값으로 획득한 수익은 원화 기준 1억원에 미치지 못하는 것으로 확인되고 있다.[8] 당시 북한뿐 아니라 많은 해커 집단들이 불특정 다수를 대상으로 랜섬웨어 공격을 시도하고 몸값을 요구했으나, 몸값을 지불하는 경우에도 암호화된 파일을 복구해 주지 않았기 때문에 몸값을 지불하는 대신 암호화된 자료를 포기하는 경우가 일반적이었다. 그 결과, 북한의 해킹 그룹들은 암호화 랜섬웨어 공격 대상을 선정할 때 다수의 일반인보다는 몸값 지불 가능성이 높은 중요한 정보를 취급하는 기업 및 관공서를 대상으로 공격을 시도하는 경향을 보이고 있다. 대표적으로 2022년 미국의 의료기관들을 대상을 실시한 암호화 랜섬웨어

---

7) 『중앙일보』, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 4. 2(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

8) 『지디넷코리아』, 「랜섬웨어 워너크라이 피해 현황은」, 2017. 5. 16(https://zdnet.co.kr/view/?no=20170516162743, 접속일: 2025. 4. 25). 일반적으로 랜섬웨어 공격을 받은 피해자들이 해커의 요구대로 금전을 지불하는 경우에도 암호화된 파일을 복구해 주지 않는 경우가 빈번하기 때문에 대부분의 피해자들은 해커의 요구에 불응하는 경향이 높다.

공격 사례가 있다. 당시 북한의 해커들은 미국의 병원과 의료기관의 서버를 대상으로 랜섬웨어 공격을 시도했으며, 환자들의 진료기록을 암호화하고 이를 복구해 주는 조건으로 가상자산을 요구했다. 당시 병원 운영진들은 응급환자의 진료를 위해 해커에게 가상자산을 입금하고 자료를 복구할 수밖에 없었다.[9)]

랜섬웨어 공격이 세계적으로 증가하면서 랜섬웨어 공격을 대비하여 자료를 별도로 백업하여 이중으로 보관하는 기관들이 증가했으며, 개인의 경우 암호화된 파일을 포기하고 시스템을 포맷하는 방법을 선택하는 경우가 증가했다. 그 결과, 금전적 이익을 목표로 랜섬웨어 공격을 시도하는 해커들은 새로운 랜섬웨어 공격인 독스웨어 공격을 선호하게 된다. 독스웨어는 개인정보를 온라인에 공개하는 것을 뜻하는 신조어 '독싱(Doxing)'의 개념을 활용하는 진화된 랜섬웨어 공격 방식으로 컴퓨터에서 민감한 개인정보 등을 획득한 후 이를 유포하겠다는 협박을 통해 몸값을 갈취한다. 민감한 개인정보, 기업의 영업 비밀 등 외부로 유출될 경우 피해자들에게 지속적인 피해가 발생할 수 있으며, 자료 백업 및 시스템 포맷으로 대응할 수 없다는 특징을 가지고 있다.

마지막으로 최근 가장 문제가 되고 있는 서비스형 랜섬웨어는, 랜섬웨어 개발자들이 자신들이 개발한 랜섬웨어 코드 및 멀웨어(Malware)[10)]를 다른 해커들에게 판매하고 해당 공격을 통해 발생 수익을 공유하는 개념이다. 이는 악성코드를 개발할 능력이 없는 해커들도 손쉽게 랜섬웨어 공격을 시도할 수 있기 때문에 랜섬웨어 범죄가 증가하는 데 결정적 요인을 한 것으로 분석된다. 초기 자체적으로 제작한 악성코드를 중심으로 랜섬웨어 공격을 진행하던 북한의 해킹 그룹은 최근 Rass 서비스 활용 및 다른 랜섬웨어 조직들이 사용한 수법을 분석하여 새로운 유형의 랜섬웨어 악성코드 및 공격 방법을 개발하면서 가상자산 탈취 및 사이버 스파이 활동을 하고 있는 것으로 파악된다. 2022년 미국의 마이크로소프트의 분석에 따르면 북한의 해킹 그룹인 '문스톤 슬릿(Moonstone Sleet)'이 러시아 기반 랜섬웨어 조직이 제공하는 서비스형 랜섬웨어인 '킬린(Killeen)'을 사용한 정황을 포착한 바 있다.[11)]

랜섬웨어 공격은 금전적 피해를 유발할 뿐 아니라 사회 기반 시설이 공격받을 경우 대규모 혼란을 초래할 수 있어 많은 국가가 정부 차원에서 랜섬웨어 공격을 대비할 수 있는 계획을 수립하고 있다. 미국정부는 해당 사건 외에도 대표적인 랜섬웨어 범죄 집단인 '하이브'의 시스템 해킹에 성공하여 탈취한 자금을 몰수하는 등 랜섬웨어 공격에 전면적으로 대응하고

9) 『VOA』, 「북한, 미 의료기관 겨냥 변종 랜섬웨어 공격… 법무부 50만달러 회수」, 2022. 7. 20(https://www.voakorea.com/a/6665412.html, 접속일: 2025. 4. 29).
10) 컴퓨터의 정상적인 기능을 방해하거나 데이터 탈취, 시스템 파괴, 시스템에 무단 접근 등을 목적으로 설계된 소프트웨어이며, 대표적으로 트로이 목마, 스파이웨어, 랜섬웨어 등이 있다.
11) 『VOA』, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 3. 12(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

있다.[12]

2. 해킹을 통한 탈취: 지능형 지속 위협(APT)를 중심으로

북한이 랜섬웨어 공격과 함께 가장 많이 활용하는 사이버 공격 방법은 해킹을 통해 현금, 가상자산 등을 직접 탈취하는 방법이다. 초기에는 은행 전산망, ATM 시스템을 해킹하여 달러 인출을 시도하는 일반 해킹 방법을 사용했으나, 최근에는 탐지 및 대응이 어려운 APT(Advanced Persistent Threat) 공격 방식을 적극적으로 활용하고 있다. APT 공격은 오랜 기간 동안 공격 대상을 관찰하면서 정밀하게 수립된 맞춤형 전략으로 진행되는 사이버 공격 방법을 총칭하는 표현이다. 해커들은 APT 공격 과정에서 스피어 피싱[13]을 통한 악성코드 유포 및 다양한 사회공학적 기법[14] 을 사용하고 있다.

2016년 발생한 방글라데시 중앙은행 해킹 사건은 북한이 1년 이상 준비한 전형적인 스피어 피싱을 활용한 APT 공격에 해당한다. 북한의 대표적인 해킹 그룹 '라자루스'는 방글라데시 중앙은행 직원들을 대상으로 스피어 피싱에 성공한 이후 약 1년 동안 은행 업무 과정을 관찰하면서 SWIFT 시스템을 이용한 달러 이체 업무 절차를 파악하고 이를 바탕으로 범행 계획을 수립했다. 또한, 탈취한 달러를 이체하고 인출하는 과정에서 정부나 금융기관들이 절차를 강제 중단 시킬 수 없도록 범행 일자와 인출 과정까지 계획 단계부터 치밀하게 준비된 공격이었다. 라자루스는 방글라데시 공휴일 전날인 2월 4일(목요일) 탈취한 은행 직원 계정을 통해 SWIFT 시스템에 접속한 후 뉴욕 연방준비은행에 총 35건(약 10억 달러 규모)의 달러 이체 요청과 함께 방글라데시 중앙은행이 보유한 프린터기 시스템의 작동을 강제 중단 시켰다. 해당 프린터 시스템은 SWIFT 시스템을 통한 자금 이체가 완료되면 송금 내역을 자동으로 출력하도록 설정되어 있었으나, 사건 당일 해커들이 작동을 강제 중단 시킴으로써 직원들이 송금 요청 사실을 즉시 인지하지 못했다. 또한, 2월 6일(토요일) 근무를 개시하고 프린터가 복원될 시점에는 FED(미국 연방준비제도)가 위치한 미국 현지 시각이 금요일 저녁으로 FED의 담당자들이 퇴근하여 신속한 대응이 불가능하다는 점도 계획에 반영했다. 북한은 탈취한 자금을 필리핀 은행을 통해 필리핀에 위치한 카지노의 계좌로 분산 입금을 시도했다.[15] 다만, 라자루스의 방글라데시 은행 해킹 사건은 현금화 단계에서 예상치 못한 변수와 해커들의

---

12) 『지디넷코리아』, 「미 FBI, 랜섬웨어 갱단 '하이브' 해킹해 사이트 압수」, 2023. 1. 29(https://zdnet.co.kr/view/?no=20230129120014, 접속일: 2025. 2. 17).
13) 공격 대상자에 대한 사전 조사를 바탕으로 설계된 맞춤형 피싱 공격을 의미한다.
14) 사이버 공격을 시도할 때 물리적, 기술적 보안 취약점을 이용하는 것이 아니라 사람 간 상호 관계를 바탕으로 공격 대상자의 신뢰 형성을 바탕으로 상대를 속여 정상적인 보안 절차를 무력화시키는 방법으로 인간관계의 취약성을 이용하는 공격 방법이다.
15) 김홍선, 『보이지 않는 위험』, 한빛미디어, 2023, pp.37~42.

단순 실수로 6,500만달러 정도만 탈취된 것으로 파악된다.[16]

북한의 APT 공격은 가상자산 분야에 대한 공격에도 적극적으로 활용되고 있다. 대표적인 사례로 2023년 에스토니아 가상자산 기업 '코인스페이드'의 가상자산을 탈취 사건이 있다. 북한의 해커들은 유령회사를 설립하고 온라인 구직 서비스인 '링크드인'에 코인스페이드 직원들의 관심을 유발할 수 있는 맞춤형 채용 조건 및 고액 연봉을 제시하는 공고를 통해 범행 대상을 물색하고 있었다. 이후, 채용 과정에 지원한 코인스페이드 직원들에게 화상 면접을 제안하면서 해당 직원들의 컴퓨터에 악성코드를 설치해 내부망 접근 권한을 획득했다. 내부망 침투에 성공한 북한의 해커들은 약 3,730만달러 규모의 가상자산을 탈취하는 데 성공했다. 이와 함께, 2025년 발생한 가상자산 거래소 '바이비트' 해킹 사건 역시 북한의 해킹 그룹이 범인으로 지목되고 있다. 해당 사건의 정확한 해킹 방법을 확인하지는 못했으나, 거래소 직원을 대상으로 스피어 피싱에 성공한 후 바이비트 거래소의 콜드월렛의 가상자산 이체 과정을 모니터링하면서 멀티시그 월렛의 취약점을 공략한 것으로 추정하고 있다.

3. 기타

현대 사회는 코로나19 팬데믹을 경험하면서 일상에서 많은 부분에 변화가 발생했다. 대표적으로 비대면 서비스가 증가했으며, IT 기업을 중심으로 채용 과정에서 온라인 화상 면접 증가 및 근로자들에게 출근할 필요 없이 원격 재택근무로 업무를 수행하는 것을 허용하고 있다.

북한의 해커들은 비대면 서비스가 일상화된 사회 변화를 활용해 제3국에 거주하면서 미국, 유럽에 위치한 IT 기업에 취업하거나, 직접 유령 회사를 설립하고 구직자들을 대상으로 화상 면접을 진행하는 과정에서 악성코드를 이용한 가상자산 탈취를 시도하고 있다. 2024년 미국 국무부의 발표에 따르면 북한의 해커들은 위장 취업을 통해 기업의 기밀 정보 및 약 8,800만달러에 달하는 자금을 탈취한 것으로 추정된다고 발표했다.[17]

같은 해 미국 법무부도 북한의 해커들이 IT기업에 위장 취업하여 기업의 기밀 정보를 탈취하거나 악성코드를 활용해 회사와 직원들이 보유하고 있는 가상자산을 탈취하는 행위를 적발했다고 발표했다. 법무부에 적발된 북한의 해커들은 미국에 거주하는 아이작 크누트가

16) 당시, 탈취한 자금을 이체하기 위해 개설한 필리핀 RCBC 은행 마닐라 지점의 주소 일부가 이란의 제재 대상 선박 이름과 일치하면서 일부만 이체가 완료됐으며, 이체에 성공한 자금 중 일부를 자금세탁을 위해 이체하던 중 수신자 영문명에 오타가 발생하여 수신인 불일치로 입금 절차가 중단됐다.

17) 『VOA』, 「FBI, 위장 취업 북한IT 노동자들 기업 데이터 훔친 뒤 금전 요구」, 2025. 1. 25(https://www.voakorea.com/a/7949475.html, 접속일: 2025. 2. 19).

제공하는 위장 신분증을 활용해 취업에 성공하면 기업들로부터 수령한 업무용 노트북을 동남아, 중국 등 제3국에 있는 자신의 거처에 설치했다. 이후, 해당 노트북에 원격제어 프로그램을 설치하여 미국에서 근무를 하는 것처럼 위장하는 방법을 사용했다.[18]

위장 취업과 함께 북한의 해커들은 직접 유령회사를 설립하여 구직자들을 대상으로 가상자산 탈취를 시도하고 있다. 북한의 해커들은 미국, 멕시코 등에 유령회사를 설립한 후 암호화폐 개발자들을 대상으로 가상자산 탈취를 시도했다. 구직자들에게 화상 면접을 제안하고, 면접을 구실로 악성코드가 포함된 화상회의 프로그램을 구직자들에게 배포한 뒤 구직자들의 컴퓨터에서 개인지갑 접속 권한 및 암호 문구를 탈취한 후 보유한 가상자산을 탈취하고 있다.

Ⅳ. 향후 전망 및 대응 방안

본고에서는 북한의 사이버 공격의 변화 과정과 함께 최근 북한 해킹 그룹들이 사용하는 공격 방법에 대해 살펴봤다. 북한 사이버 공격의 주요 특징을 살펴보면, 첫째, 포괄적 대북제재 시행을 기점으로 사이버 공격의 주목적은 수익성 추구로 변화하고 있다. 특히, 가상자산의 가치가 상승함에 따라 전통적인 금융기관들 보다 상대적으로 보안이 취약하고, 자금세탁이 수월한 가상자산에 집중하는 경향을 보이고 있다. 둘째, 사이버 공격의 주요 목적이 수익성 추구로 변화하면서 공격 대상이 불특정 다수로 변화하고 있다. 마지막으로, 북한의 사이버 공격 방식이 지속적으로 고도화되면서 각국 정부가 신속한 대응을 하기 어려워지고 있으며, 국가 간 협력을 통한 공동 대등이 필요한 상황으로 변하고 있다.

다만, 북한의 사이버 공격이 수익성 추구 경향이 높아지고 있지만, 동시에 수익 추구 목적과 무관한 정보 탈취를 위한 공격도 병행하고 있다. 올해 8월 미국의 비영리 단체 '디도시크릿츠(The DDosecrets)'는 해킹 관련 전문 매체인 '프랙(Phrack) 매거진'을 통해 'KIM'으로 통칭되는 해커의 서버를 해킹해 해당 해커가 보유한 자료를 검토하던 중 남한의 행안부, 외교부, 군, 검찰 등 주요 정부 부처 및 KT, LG 유플러스, 네이버, 카카오 등 국내 대기업들을 해킹한 자료를 확보한 사실을 공개했다. 'KIM'으로 통칭되는 해커의 서버에서 발견된 자료들을 분석한 결과 해커의 정체는 북한의 대표적인 해킹 그룹인 '김수키'가 유력한 것으로 추정하고 있다. 해당 발표 이후 정부는 자체 내부 점검을 통해 지난 3년간 해당 해커에게 정보를

18) 『TECHWORLD』, 「미국 기업에 위장 취업한 북한 IT 인력, 연간 3억 이상 수익 올려」, 2024. 8. 14(https://www.epnc.co.kr/news/articleView.html?idxno=305271, 접속일: 2025. 2. 19).

탈취 당한 사실은 인정했으나, 해커의 정체가 김수키라는 명확한 근거가 부족하기 때문에 확정 지을 수 없다는 입장을 보이고 있다.[19]

북한의 사이버 공격은 대북제재가 지속되는 환경에서 현재와 같이 외화 벌이를 목적으로 전 세계를 대상으로 지속될 뿐 아니라, 국제사회의 대응에 맞춰 새로운 방식으로 공격을 시도할 것으로 예상된다. 따라서, 북한 사이버 공격을 예방할 수 있도록 다차원적인 분석과 함께 현재 시점에서 공격에 취약한 지점에 대한 점검과 국제사회의 협력을 강화해야 한다. 특히, 북한이 집중적으로 공격하고 있는 가상자산 관련 산업(거래소, 가상자산 사업자, 개인 거래자 등)은 상시 감시체계 강화 및 정보보호 관련 교육 확대 등 내부 통제 시스템을 강화하고, 국제협력을 통한 글로벌 정보 공유 체계를 구축할 필요성이 있다. 가상자산 거래소의 경우 이상거래 패턴 감시 시스템 구축과 국제사회의 제재 대상 등 블랙리스트에 연관된 것으로 추정되는 가상자산 지갑에 대한 정보를 공유해야 한다. 이미 규모가 큰 가상자산 거래소는 자금세탁방지 준수를 위한 내부통제 시스템을 마련하고 있지만, 중소형 거래소 및 DEX, De-Fi 시스템 등 상대적으로 규모가 작은 기업들은 여전히 보안이 취약한 상태로 운영되고 있기 때문에 국제사회 차원에서 대비책 마련이 필요하다. 실시간 감시체계 및 국제협력의 중요성은 2025년 2월 발생한 바이비트 거래소 해킹 사건에서 확인할 수 있다. 바이비트 거래소의 경우 비정상 거래 발생 즉시 해킹 범죄를 인지하고 공유함으로써 도난당한 가상자산의 일정 부분에 대해서 현금화를 방지할 수 있었다. 당시, 바이비트의 신속한 정보 공유로 주요 가상자산 거래소들은 탈취된 이더리움이 입금된 지갑 주소에 '바이비트 해킹'이라는 태그를 달고 블랙리스트로 관리함으로써 해당 지갑을 동결할 수 있었다.

향후 북한 해킹 그룹의 가상자산 탈취 시도가 지속될 경우 다양한 블록체인 프로젝트에서 운영하고 있는 DAO[20] 생태계를 주의해야 할 것으로 보인다. 블록체인 프로젝트에서 많이 활용되는 DAO는 특정 가상자산의 메인넷에서 다양한 벤처 사업자들이 DApp을 등록하고 활동할 수 있는 플랫폼 성격을 가지고 있는 생태계이다. 이는 최근 IT 업계에서 주목하고 있는 차세대 인터넷 환경인 WEB3.0이 블록체인 기술을 통해 실현되고 있으며, WEB3.0을 가시화시키고 있는 결과물 중 하나가 DAO라는 점에서 활성화될 가능성이 높다. 대표적으로 솔라나(Solana), 비체인(Vechain)과 같은 주요 가상자산들은 자신들의 메인넷에 DAO 생태계를 구하여 DApp 사업자들의 참여를 유도하고 인센티브로 자신들의 가상자산을 부여하고 있다. 따라서, 북한의 해커들이 위장 회사를 창업하여 DAO 생태계에 참여한 뒤 사용자들에게

19) 『연합뉴스』, 「공무원 업무시스템 '온나라'·GPKI 인증 해킹 흔적」, 2025. 10. 17(https://www.yna.co.kr/view/AKR20251017062151530?input=1195m, 접속일: 2025. 10. 18).
20) Decentralized Autonomous Organization의 약자로, 탈중앙화 자율조직을 의미하며, 블록체인을 기반으로 한 공동 투자 조합의 성격이다.

높은 보상을 미끼로 고가의 NFT를 판매한 후 약속된 보상을 지급하지 않고 잠적하는 '러그풀(Rug pull)'[21]방식의 가상자산 탈취를 시도할 가능성이 높다.

또한 우리 정부의 경우 수익을 목적으로 하는 북한의 사이버 공격에 대한 대비와 함께 국가 주요 정보 탈취 및 주요 기반 시설 공격을 통한 사회 혼란 유발을 목적으로 하는 사이버 공격에 대한 철저한 사전 대비가 필요하다. 최근 북한은 남북 관계를 '적대적 두 국가' 관계로 규정하면서 통일을 부정하는 등 남한의 대화 요구에도 일절 호응하지 않으면서 한반도 긴장감을 지속적으로 높이고 있다. 특히, 북한은 자유민주주의 진영 국가들과 전체주의 진영 국가 간의 갈등이 심화되고 있는 국제 정세 속에서 중국, 러시아와 협력을 강화하고 있기 때문에 남북 간 대화가 단시간에 재개되기는 어려울 것으로 전망된다. 따라서, 현재와 같이 남북 관계 긴장이 지속될 경우 북한은 대내 체제 결속을 위해 남한 사회의 혼란을 유발하기 위한 대남 사이버 공격에 대한 대비도 필요할 것으로 보인다. 2022년 SK C&C 데이터센터[22] 및 2025년 국가정보자원관리원의 데이터센터 화재 사건은 북한의 사이버 공격과 무관한 사건이지만 남한 주민들의 일상의 많은 부분이 인터넷 환경에 기반하고 있으며, 주요 인터넷 인프라가 마비가 될 경우 사회적으로 큰 혼란과 경제적 손실이 발생할 수 있음을 보여준 사례다. 따라서, 남북 관계 갈등이 지속되고, 북한이 핵・미사일 발사가 아닌 사이버 공격을 통한 대남 도발을 감행할 경우 국민들에게 직접적인 피해가 발생하기 때문에 철저한 대비가 필요할 것으로 판단된다.

---

21) 러그풀은 가상자산과 De-Fi 분야에서 사용하는 용어로, 블록체인 프로젝트 개발자나 내부자가 가상자산의 사전 발행이나 NFT판매에 참여하는 사람들에게 막대한 보상을 지급할 것처럼 과대 광고를 한 후 획득한 가상자산을 가지고 잠적하는 사기행각을 의미한다.

22) 해당 화재로 인해 카카오톡 및 네비게이션, 모바일 결제 등 관련 주요 서비스가 약 10시간 동안 작동 불능 상태가 지속되면서 경제적 손실도 발생했다.

참고문헌

고명현, 「북한의 사이버 전력(戰力)과 금융범죄」, 『KDI 북한경제리뷰』, 10월호, 2021.

김성진, 「북한의 가상자산 탈취 및 자금세탁 방법 변화 양상에 대한 연구」,『평화학연구』, 제26권 제2호, 2025.

김홍선, 『보이지 않는 위험』, 한빛미디어, 2023.

『연합뉴스』, 「공무원 업무시스템 '온나라'·GPKI 인증 해킹 흔적」, 2025. 10. 17(https://www.yna.co.kr/view/AKR20251017062151530?input=1195m, 접속일: 2025. 10. 18).

『중앙일보』, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 4. 2(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

『지디넷코리아』, 「미 FBI, 랜섬웨어 갱단 '하이브' 해킹해 사이트 압수」, 2023. 1. 29(https://zdnet.co.kr/view/?no=20230129120014, 접속일: 2025. 2. 17).

_____, 「랜섬웨어 워너크라이 피해 현황은」, 2017. 5. 16(https://zdnet.co.kr/view/?no=20170516162743, 접속일: 2025. 4. 25).

『VOA』, 「FBI, 위장 취업 북한IT 노동자들 기업 데이터 훔친 뒤 금전 요구」, 2025. 1. 25(https://www.voakorea.com/a/7949475.html, 접속일: 2025. 2. 19).

_____, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 3. 12(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

_____, 「북한, 미 의료기관 겨냥 변종 랜섬웨어 공격... 법무부 50만 달러 회수」, 2022. 7. 20(https://www.voakorea.com/a/6665412.html, 접속일: 2025. 4. 29).

Montgomery Meigs, ed. US Army War College Editorial Board, "Unorthodox Thoughts about Asymmetric Warfare," *Parameters: Journal of the US Army War College,* 4-18. Carlisle, PA: US Army War College, 2003.

Panel of Experts on the DPRK, "Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee." UN Doc, S/2019/691, New York: United Nations, 2019.

『TECHWORLD』, 「미국 기업에 위장 취업한 북한 IT 인력, 연간 3억 이상 수익 올려」, 2024. 8. 14(https://www.epnc.co.kr/news/articleView.html?idxno=305271, 접속일: 2025. 2. 19).