국가전략연구위원회 이슈브리핑 17호 (발간일: 2023.12.13.)

# 북한의 사이버 공격의 진화와 현황: 암호화폐 공격과 랜섬웨어 공격을 중심으로[1)]

김보미 (국가안보전략연구원)

## Ⅰ. 금전을 노린 전방위적 사이버 공격: 암호화폐 해킹과 랜섬웨어 공격

2010년대 이후 북한발 사이버 공격의 가장 큰 특징은 재정적 목적의 공격에 집중되고 있다는 것이다. 무기 수출, 불법 마약, 위조지폐 밀매 등이 북한의 불법적인 외화확보 수단이었다. 그러나 2010년대 이후로는 사이버 공간에서 금융 공격, 특히 암호화폐 해킹이 주요 외화 수익원으로 자리매김하였다.

북한의 암호화폐 공격능력은 2010년대 중반부터 본격적으로 주목받기 시작했다. 2000년대 후반 이후 북한은 한국의 정부 기관이나 웹사이트, 국방 인프라에 대한 파괴적인 사이버 공격을 개시하였다. 그러나 북한은 세계 금융시스템의 추세를 날카롭게 인식하면서 2016년 이후 부과된 강력한 경제제재에 대한 회피 방안으로 암호화폐에 대한 관심을 키워나갔다. 북한은 비트코인을 비롯한 암호화폐 가격의 상승과 맞물려 미국·UN 대북제재가 확대되면서 은행과 암호화폐거래소 등 금융기관 쪽으로 사이버 공격의 방향을 전환하였다.[2)] 이러

1) 이 글은 2023년 12월 7일 제6차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.
2) Jason Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program," The Diplomat, July 18, 2022,

한 북한의 금융권 공격은 일부 정치적 동기부여에 따르기도 했으나 대부분은 재정적 이유의 사이버 공격이었다. 북한은 암호화폐 해킹이 특별한 비용이 들지 않는 데 비해 수익성이 높고 공격 출처를 추적하기 어려워 적은 위험으로 더 많은 돈을 탈취할 수 있다는 점에 매력을 느끼고 암호화폐 탈취에 집중하는 것으로 보인다.

북한은 또한 랜섬웨어(ransomware) 공격을 암호화폐 거래소 및 지갑 해킹과 함께 주요 외화확보 수단으로 활용하고 있다. 랜섬웨어는 몸값과 소프트웨어의 합성어로 피해자의 컴퓨터 시스템을 감염시켜 접근을 제한한 뒤 이를 해제하는 대가로 일종의 몸값을 요구하는 악성 해킹 수법을 의미한다.[3] 랜섬웨어 공격은 북한이 2016년 이후 외화확보를 위한 암호화폐 해킹에 주력하면서 다소 소강상태에 있었다. 그러나 2022년을 기점으로 북한에 의한 랜섬웨어 피해 규모는 급증하였으며 미국에서만 지방 정부, 학교, 병원 등 200개 이상의 기관이 피해를 입은 것으로 드러났다. 랜섬웨어 공격의 이유는 여러 가지로 나뉠 수 있지만 북한 같은 경우는 재정적 목적의 랜섬웨어 공격이 주를 이룬다고 할 수 있다.[4] 2017년 5월, 전 세계적으로 커다란 피해를 입힌 워너크라이 2.0 랜섬웨어 공격 당시 북한은 랜섬머니로 300달러어치의 비트코인을 요구한 바 있다. 미국 NSC 사이버·신기술 담당 부보좌관인 앤 뉴버거(Anne Neuberger)는 북한의 사이버 활동은 다른 국가들의 사이버 프로그램이 지정학적 목적을 위한 스파이 활동을 벌이는 것과는 달리 제재를 우회하기 위한 경화 절도에 집중한다는 점에서 차별성을 보인다고 지적했다.[5] 랜섬웨어 공격 시 해커들은 추적을 회피하기 위해 암호화폐로 대가를 지불받게 되는데 이 때문에 북한의 암호화폐에 대한 선호도가 더욱 높아졌을 것으로 판단된다.

## Ⅱ. 암호화폐 가격 하락이 가져온 변화

문제는 2021년을 기점으로 암호화폐가 급격한 가격 하락을 맞이하였다는 점이다. 이에 따라 2022년 북한이 사이버 해킹을 통해 벌어들인 암호화폐 규모는 역대 최고 액수를 기록

https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/.

3) 랜섬웨어는 크게 시스템의 바탕화면이나 드라이브의 일부를 잠그는 락커(Locker)와 파일 또는 데이터를 직접 암호화하는 크립토(Crypto)로 분류된다. 랜섬웨어에 감염되면 파일 암호화, PC 또는 스마트폰 화면이 잠금처리 되거나 PC 재부팅이 불가능해지는 등 피해가 발생한다.

4) 반면 중국이나 러시아는 첩보와 선전 선동 등 정치적 목적이 강한 랜섬웨어 공격을 선호한다. 국가행위자가 스파이 활동이나 기만, 평판 훼손, 기금 마련을 포함한 다양한 목적을 가지고 감행하기도 한다.

5) 뉴버거 부보좌관은 이에 덧붙여 북한이 암호화폐 해킹을 통해 미사일 개발에 필요한 자금의 절반을 충당하는 것으로 추정했다. 2022년 7월, 북한 미사일 개발비용의 1/3에 달하는 금액이 암호화폐 해킹을 통해 마련되었다고 발언한 것을 상향 조정한 것으로 보인다. 노정연, "미 NSC 부보좌관 "북한, 사이버 활동으로 미사일 재원 3분의 1 충당"," 『경향신문』, 2022년 7월 29일, https://www.khan.co.kr/politics/north-korea/article/202207290825001.

한 것으로 나타났으나 실질적으로 벌어들인 외화수입은 이보다 훨씬 더 적을 것으로 추정된다. 미국의 블록체인 분석업체인 체이널리시스(Chainalysis) 북한이 현금화하지 못한 암호화폐가 2021년 말 1억 7,000만 달러어치였으나 암호화폐 가치 하락으로 6,500만 달러 수준으로 급감하였을 것으로 분석하였다.

북한의 경우 암호화폐 공격을 통한 거액의 탈취에도 불구하고, 추적을 피해 암호화폐를 안정적인 자금원으로 현금화하는데 어려움을 겪고 있었다. 더군다나 대량의 암호화폐를 현금화할 수 있는 거래소가 많지 않은 데다 해킹 피해 방지를 위해 주요 국가들이 감시와 제재를 강화하면서 자금세탁 방지 규정을 강화하면서 암호화폐를 현금화하기가 쉽지 않았을 것으로 보인다. 더군다나 북한은 훔친 암호화폐를 법정화폐로 바꿔줄 수 있는 브로커를 찾으면서 훔친 통화 가치의 3분의 1만 받는 것으로 알려졌다.[6)]

2023년에도 북한은 암호화폐 공격을 꾸준히 시도하였으나 벌어들인 총액은 2022년에 비해 크게 줄어들었다. 올해 2분기 전세계 암호화폐 공격 건수는 전년 동기 대비 65.3%가 증가한 81건(지난해 49건)을 기록하였다. 그럼에도 불구하고 2023년 북한의 암호화폐 해킹 금액은 3분기까지 약 3억 4천만 달러로 지난해와 비교하여 다소 줄어들었다. 암호화폐 탈취 시도는 늘어났지만 탈취한 총액은 줄어든 것이다. 암호화폐의 특징인 높은 가격 변동성과 현금화 문제, 그리고 주요 국가들의 감시와 제재 강화로 인해 북한이 탈취한 암호화폐 해킹 금액이 줄어든 것으로 추정된다.

암호화폐 해킹을 통한 수입 총액은 줄어든 반면 암호화폐에 기반하는 범죄인 랜섬웨어 공격은 증가하고 있다. 이유는 해커들이 랜섬웨어를 통해 대규모 자금력을 갖춘 기관을 집중적으로 노리고 있기 때문이다. 북한은 대기업이 주요 데이터와 시스템에 대한 권한을 회복하고 몸값을 지불할 능력도 갖추고 있다는 점에 착안하여 집중 타켓으로 삼아 최대한의 몸값을 받아내려는 것으로 보인다. 특히 병원이나 보건기관은 이러한 공격의 대상이 되기 쉽다. 북한이 개발한 마우이(Maui) 랜섬웨어는 생명을 다루는 의료 및 공중보건 기관들의 특성상 서비스의 중단을 피하기 위해서라도 돈을 지불할 용의가 크다는 사실을 간파하고 2021년 5월부터 이듬해까지 미국 전역의 의료기관을 타겟으로 삼아 전방위적인 공격을 감행하였다.

최근 북한은 랜섬웨어 유포로 대기업과 같은 고가치 표적뿐만 아니라 보안 수준이 낮은 영세기업이나 개인으로부터 소액 탈취까지 시도하고 있다. 대표적인 사례가 홀리고스트(HOlyGhOst) 랜섬웨어이다. 2022년 6월 최초 등장한 홀리고스트 랜섬웨어는 데이터를 암호화한 뒤, 랜섬머니를 지불하지 않으면 유출한 정보를 가지고 다른 조직이나 기관에 이를 공개하겠다고 협박하는 이중협박 전략을 사용하여 소액을 탈취하였다. 홀리고스트 랜섬웨어의 주체는 북한의 해킹조직 안다리엘(Andariel)로 추정되는데, 이들은 주로 소규모 사업체를 겨

6) John Smith, "Insight: Crypto crash threatens North Korea's stolen funds as it ramps up weapons tests," Reuters, June 29, 2022, https://www.reuters.com/technology/crypto-crash-threatens-north-koreas-stolen-funds-it-ramps-up-weapons-tests-2022-06-28/.

냥하여 시스템에 손상을 입히고 암호해제를 조건으로 소액의 비트코인을 요구한 것으로 알려졌다. 특히 해커들은 피해자들이 협상에 잘 응할 경우 제시한 금액의 1/3까지 랜섬머니를 낮춰주기도 해 북한 해커들이 개인의 금전적 이익을 위해 공격을 시도한 것으로 추정된다.

북한 해커들이 민간인을 표적으로 주머니털이에 나선 사례는 홀리고스트 랜섬웨어뿐만이 아니다. 2023년 10월 27일, 국내의 한 데이터 복구업체는 북한의 해킹조직인 라자루스 그룹(Lazarus Group)과 협력하여 랜섬웨어의 해결수법을 전달받아 피해자에게 랜섬머니를 지불하도록 하는 한편 거액의 복구 비용을 챙긴 것으로 확인되었다. 해당 사건은 북한이 국내업체와도 협력해 우리 사회 내부를 파고들어 랜섬웨어를 퍼뜨리고 금전적 이익을 취했다는 점에서 기존의 랜섬웨어 공격과 차별화된다고 할 수 있다. 북한의 사이버 공격은 주로 국가가 배후에 있으며 거액 탈취를 목표로 하고 있는 것으로 알려졌지만 최근에는 해커 개인의 금전적 이익을 목표로 소액 탈취도 시도되고 있어 피해 규모가 더 커질 가능성이 우려된다.

## Ⅲ. 러시아와의 협력 가능성

북러간 무기거래와 군사협력 확대 가능성에 대한 우려가 커지는 가운데 북한은 가상세계에서도 러시아와 협력하여 현금화 문제의 돌파구를 찾고 있는 것으로 확인되고 있다. 체이널리시스는 2023년 9월 19일 발표한 보고서에서 북한이 2021년부터 암호화폐 자금세탁을 위해 여러 러시아 암호화폐 환전거래 서비스를 이용해왔으며 2022년 탈취한 암호화폐 중 2,190만 달러의 암호화폐가 러시아의 거래소로 이체되었다고 밝혔다.[7] 향후 북한에 대한 직접적 재정 지원이나 물자 지원이 어려운 러시아가 자국의 암호화폐거래소를 통해 낮은 비용으로 자금세탁을 도와줄 가능성이 우려된다. 특히 러-우전쟁 발발 이후 첩보전에 집중해온 러시아 해커들이 외화수입의 확충을 원한다면 북한의 암호화폐를 적극적으로 도와줄 가능성을 배제하기 어렵다. 북한은 러시아의 암호화폐 거래소를 통해 우호 가격에 대량의 암호화폐를 안정적으로 세탁할 수 있게 되고 러시아 또한 브로커 비용을 챙겨 외화수입을 올림으로써 일석이조의 효과를 기대할 수 있을 것이다.

북한과 러시아의 협력이 훔친 암호화폐의 자금세탁에만 그치지 않고 랜섬웨어 기술 이전, IT 인력 송출 등으로 확대될 가능성도 배제하기 어렵다. 러시아는 북한과 함께 미국의 사이버 제재를 적용받는 국가로서 양국이 적극적으로 협력할 여지가 있다. UN안보리 상임이사국인 러시아가 대북제재 결의를 정면으로 위반하기는 어렵겠지만 국제사회의 감시망을

7) Chainalysis Team, "Russian and North Korean Cyberattack Infrastructure Converge: New Hacking Data Raises National Security Concerns," Chainalysis, September 14, 2023, https://www.chainalysis.com/blog/north-korea-russia-crypto-money-laundering/ (accessed: October 20, 2023).

피해 국적 및 신분을 위장한 북한 IT 노동자를 수용할 수도 있을 것이다. 한미 양국은 2023년 10월 19일, 국내외 기업 및 개인들이 국적과 신분을 위장한 북한 IT 인력을 고용하거나 이들의 활동을 돕지 않도록 주의를 요구하는 IT 인력주의보를 공동으로 발표하였다. 그러나 가상세계에서 국가간 협력 정황은 포착과 증명이 쉽지 않아 대북제재 위반 루트로써 활용될 여지가 있다. 북한 IT 인력이 러시아의 첩보전을 보조함으로써 외화를 습득하거나 첩보능력을 획득하여 한국에 활용하게 된다면 매우 심각한 피해를 양산할 수 있다.

## Ⅳ. 우리의 대응방안

올해 북한의 사이버 공격에 의한 암호화폐 시장의 피해 규모는 2022년에 비해 줄어들었지만, 외화확보를 위한 북한의 암호화폐 공격행위 역시 계속되고 있어 피해 사례는 누적될 것으로 예상된다. 랜섬웨어에 의한 공격은 전 세계적으로 증가추세에 있으며 피해액 역시 매년 늘어나 올해는 열대 두 번째로 많은 피해액을 기록할 것으로 전망된다.

한국 정부는 점증하는 북한의 사이버 위협에 대응방안들을 마련해오고 있지만 일부 한계점을 노출하고 있다. 사이버 공격에 대해 북한의 소행이라는 명백하고 확실한 직접적인 증거의 제시가 어려운 데다 가해 당사자로 의심되는 북한이 이를 적극 부인하면서 사이버 공격의 책임을 부담하기 곤란한 현실적인 어려움 때문이다. 그럼에도 불구하고 국가적 차원에서 사이버 피해를 최소화하기 위한 법령 제정, 사이버안보 보험 개발, 카운터해킹(counterhacking), 국제협조 체계 강화와 새로운 대북제재의 적용 등의 노력을 기울여야 할 것이다.

우선 정부와 국회는 관련 기업과 개인이 해킹 피해에 대한 신고를 의무화하는 법령을 제정할 필요가 있다. 해킹 피해에 대한 의무 신고를 실행한다면 사고의 원인을 분석하고 피해 확산을 방지하며 회복력 강화 및 재발 방지 대책을 마련하는 체계를 가동할 수 있게 된다.[8] 랜섬웨어 공격에 대해서는 이를 사이버범죄로 분류하는 미국의 사이버 침해사고 보고 관련 법제를 참고하여 랜섬웨어 공격에 특화된 법제를 제정하는 것을 고려해 볼 수 있다. 가칭 "사이버보안법"을 제정하여 랜섬웨어에 의한 피해를 입었을 경우 72시간 내에 국가정보원을 포함한 관계기관에 신고하도록 하고 랜섬머니를 지급하였을 경우 복구지원을 실행하도록 법적 기반을 마련토록 하는 것이다.

또한 금융기관으로 하여금 보다 현실에 적합한 사이버안보 보험을 개발하여 시장에서 채택될 수 있도록 독려하고, 기업과 지방자치 단체에 사이버안보 보험에 가입하도록 적극적으로 유도할 필요가 있다. 다만 사이버안보 보험 가입으로 기업들의 랜섬웨어에 대한 경각심이 축소되지 않도록 유의하여야 한다. 미국의 사례와 우리의 간첩신고 보상제 등을 참고

8) 다만 사이버 위협 확산을 막겠다는 목표 아래 해킹 피해의 책임을 오로지 기업에 대한 처벌 강화를 통해 해결하려 해서는 안 될 것이며 정부의 복구 지원 및 교육이 병행되어야 할 것이다.

하여 랜섬웨어 신고자 또는 결정적 제보자 등에 대한 포상금을 지급하는 방안을 검토할 필요가 있다.[9)]

무엇보다 한국 정부는 자체적으로 기업에 대한 보안 관리와 관련 법령을 정비하는 일뿐만 아니라 실질적 대응방식인 카운터해킹 등을 통해 탈취된 자금을 회수하기 위해 적극적으로 노력해야 할 것이다. 2021년 5월 28일, 경찰청 국가수사본부는 최초로 해외거래소로부터 해킹당한 45억 원 상당의 암호화폐를 환수하는 등 피해자 보호를 위해 적극적으로 대응하였다.[10)] 올해 4월에는 국정원이 미국 민간조사단과 합동작전을 벌여 북한으로부터 해킹당한 암호화폐 100만 달러를 회수했다는 언론 보도도 있었다.[11)]

이밖에 다른 미비점들은 미국을 비롯한 국제사회 주요국들 및 기관들과 국제협력을 통해 보완해 나갈 필요가 있다. 북한의 사이버 위협에 대응한 국제공조는 협력 의지 표명뿐만 아니라 구체적 실현방안이 필요하며 효과적이고 장기적인 사이버 안보전략을 수립하는 데 초점을 맞추어야 할 것이다. 구체적으로 북한의 사이버 위협과 관련하여 보고서를 주요 협력국과 합의하여 백서형태로 1년 또는 2년 주기로 발간하여 암호화폐 공격 기법 공개, 성공적 대응 사례 소개, 기술적 대응방안을 공유할 필요가 있다. 북한을 비롯한 국가 연계 사이버 행위자의 위협과 위험성을 설명한 사이버 공동주의보 발표 또한 한미 사이버 실무그룹의 역할이 될 수 있을 것이다.

나아가 북한 사이버 분야에 대해서도 제재를 가하는 것을 고려해 볼 필요가 있다. UN 안보리는 아직 사이버 대북제재를 부과하지 않고 있다. 따라서 향후 러북 협력 가능성을 약화하기 위해 우리 정부 주도로 UN에서의 추가 대북제재를 건의해볼 수 있을 것이다.

이러한 자체적인 노력과 국제적 협력을 통해 북한의 암호화폐 공격으로 인한 손실을 최소화하고 북한이 훔친 자금을 핵·미사일 프로그램에 투자하지 않도록 저지하여야 할 것이다.



9) 오일석·김보미, "북한 사이버위협의 특징과 대응방안: 김정은 시대를 중심으로," INSS 연구보고서 2022-03 (서울: 국가안보전략연구원, 2022), p. 68.
10) 박홍용, "경찰, 국내 최초 해외거래소에서 해킹 암호화폐 환수…"45억원 상당,"" 『서울경제』, 2021년 6월 7일, https://www.sedaily.com/NewsView/22NJM0NZ82/.
11) 김종훈, "국정원-美 판교 모여 협동 작전, 北 훔친 암호화폐 회수했다," 『머니투데이』, 2023년 4월 10일, https://news.mt.co.kr/mtview.php?no=2023041014085027920.