INSS
전략보고
November 2022. No.191

www.inss.re.kr
INSTITUTE FOR NATIONAL SECURITY STRATEGY

북한의 암호화폐 공격과 미국의 대응

김보미 부연구위원
bomi@inss.re.kr

Ⅰ. 문제 제기

Ⅱ. 북한의 암호화폐 공격: 사례와 특징

Ⅲ. 북한의 암호화폐 공격에 대한 미국의 대응

Ⅳ. 결론: 한국에 주는 시사점

국가안보전략연구원

국문 초록

2010년대 중반 이후, 사이버공간에서 금융 공격, 특히 암호화폐 해킹이 김정은 정권의 주요 외화 수익원으로 자리매김하고 있다. 북한은 2000년대 후반 이후 사이버공격의 방향을 은행과 암호화폐거래소 등 금융기관 쪽으로 전환하였으며 이러한 금융권 공격은 대부분 정치적 동기보다는 재정적 이유에서 출발하였다. 북한은 2016년 이후로 랜섬웨어, 은행 드롭(bank drops), 분산 서비스 거부(DDos), 공급망 공격과 같은 악성코드가 얽힌 스피어피싱 등 다양한 사이버 침입과 암호화폐 해킹 전술을 금융기관을 상대로 시행했다. 그 결과 북한의 암호화폐 공격과 피해 규모가 해마다 증가하였으며 2022년 3월, 북한이 게임업체 '액시 인피니티'를 상대로 감행한 해킹은 역대 최대규모의 손실을 낸 사건으로 기록되었다. 미국은 북한이 제재망을 회피하여 핵·미사일 프로그램을 발전시킬 수 있었던 이유로 암호화폐 해킹을 꼽고 적극적으로 대응하고 있다. 미 정부는 대북 경제제재는 물론 사이버범죄 담당 전문부서의 신설, 북한의 사이버공격에 대비한 사전 경보발령 및 보고서 발간, 북한이 훔친 암호화폐를 다시 해킹으로 회수하는 카운터해킹과 해킹 피해 신고자에 대한 포상을 실행하고 있다. 또한 미국 정부는 양자 및 다자협의를 통해 랜섬웨어 위협에 대한 공동대응의 필요성을 강조하고 전 세계가 돈세탁 방지 규칙에 대한 사이버보안 조처를 이행할 것을 요청하는 등 사이버 위협에 대응하기 위해 국제협력을 강화해 나가고 있다. 우리의 경우 미국을 비롯한 국제사회 주요국들 및 기관들과 국제협력을 통해 미비점을 보완해 나갈 필요가 있을 것이다.

핵심어: 북한, 암호화폐, 해킹, 카운터해킹, 헌트 포워드

목차

Ⅰ. 문제 제기

Ⅱ. 북한의 암호화폐 공격: 사례와 특징

1. 암호화폐에 대한 사이버공격

2. 북한의 대표적인 암호화폐 공격 사례

3. 북한의 암호화폐 공격 양상과 특징

Ⅲ. 북한의 암호화폐 공격에 대한 미국의 대응

1. 경제제재와 카운터해킹, 포상 프로그램의 실행

2. 국제협력 강화

Ⅳ. 결론: 한국에 주는 시사점

Ⅰ. 문제 제기

• 2020년 코로나19의 발생으로 북한은 '3중고(감염병·대북제재·수해)'로 대표되는 심각한 경제적 위기에 직면하였음에도 핵·미사일 프로그램을 지속적으로 확장
  - 북한은 2022년에만 30여 차례에 걸쳐 무력도발을 감행하였으며 7차 핵실험 또한 준비 중인 것으로 알려짐
  - 김정은 지도부는 각종 담화·성명·연설 등을 통해 국제사회의 대북 적대시 정책이 계속되는 한 핵무력을 질량적으로 끊임없이 강화할 계획임을 선언
    ※ 2022년 9월 8일, 최고인민회의 제14기 제7차 회의에서 김정은은 북한이 불가역적 핵보유국이 되었음을 선언하였으며 회의에서 새롭게 채택된 "조선민주주의인민공화국 핵무력정책에 대하여"의 9조는 북한이 국제안보 상황에 맞추어 핵능력을 지속 증강할 것임을 명시[1)]

• 미국을 비롯한 국제사회는 북한이 경제위기 속에서도 지속적으로 핵·미사일 프로그램을 발전시킬 수 있었던 이유로 사이버 기술을 활용한 암호화폐 공격을 꼽고 이에 대한 국제적 대응의 필요성을 강조
  - 2022년 3월, UN안보리 대북제재위원회 보고서는 북한이 암호화폐 거래소 해킹을 통해 핵·미사일 개발에 필요한 자금을 조달해왔다고 적시[2)]
  - 2022년 7월, 미 NSC 사이버·신기술 담당 부보좌관인 앤 뉴버거(Anne Neuberger)는 북한 미사일 개발비용의 1/3에 달하는 금액이 암호화폐 해킹을 통해 마련되었다고 발언[3)]
  - 미국은 북한의 악의적 사이버 활동이 세계금융시스템의 안정성을 해치고 제재망을 빠져나가고 있다고 지적하면서 북한의 사이버 위협에 대응하여 국제공조의 필요성을 강조하고 있음

1) 『노동신문』, 2022년 9월 9일.
2) United Nations Security Council, S/2022/132, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf (검색일: 2022.10.6.).
3) 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 (검색일: 2022.10.1.).

- 무기 수출, 불법 마약, 위조지폐 밀매 등이 북한의 불법적 외화 확보 수단이었으나, 2010년대 이후로는 사이버공간에서 금융 공격, 특히 암호화폐 해킹이 주요 외화 수익원으로 자리매김하고 있는 상황
  - 암호화폐는 거래내용을 암호화하여 실제 소유주를 확인하기가 쉽지 않아 도난이나 분실의 경우 익명성으로 인해 범인을 잡기 어려워 거래소와 투자자 모두 해커의 표적이 될 수 있음[4)]
  - 북한은 암호화폐 해킹에 특별한 비용이 들지 않는 데 비해 수익성이 높고 공격출처를 추적하기 어려워 적은 위험으로 더 많은 돈을 탈취할 수 있다는 점에 매력을 느낄 것으로 추정

- 최근 암호화폐 가격의 하락에도 불구하고 김정은 정권은 재정적 어려움을 극복하기 위해 지속적으로 암호화폐 관련 사이버공격을 전개해 나갈 것으로 예상

- 이에 따라 본 전략보고는 김정은 시대 날로 심각성을 더해가는 북한의 암호화폐 공격 양상·특징·사례에 대해 간략히 소개하고 한국의 바람직한 대응방향은 무엇인지 제시하는 것을 목표로 함[5)]
  - 2장에서 북한의 암호화폐 해킹 양상과 사례를 설명하고 3장에서는 가상세계에서 북한의 불법적 활동에 대해 가장 적극적 대응을 펼치고 있는 미국의 대응을 분석한 후 4장 결론에서 한국의 대응방향을 제시
    ※ 미국은 북한이 암호화폐 공격으로 핵·미사일 개발 자금을 마련하고 대북제재를 회피함으로써 비확산 레짐을 무력화하고 동북아 안정을 해친다고 판단하고 다양한 방법을 활용하여 북한 사이버위협에 대응하고 있다는 점에서 비중있게 다루어질 필요가 있음
    ※ 특히 북한의 사이버위협이 우리의 안보와 국익에 미치는 심각성을 고려할 때 효과적이고 다양한 대응방안 수립을 위해서라도 미국의 사례는 반드시 참고할 필요
  - 본 연구는 논의의 초점을 북한 암호화폐 공격의 심각성에 초점을 맞추고 기술적 내용보다는 사이버공격 현황과 해외의 대응을 중심으로 서술

4) 김문환, "가상화폐 해킹에 대한 사례 연구," 『한국산업보안연구』 제9권 제2호 (2019), pp. 23-54.
5) 미국은 북한의 암호화폐 공격에 대한 심각성을 제고하고 관련 보고서 발간, 제재를 포함한 처벌, 고발자 등에 대한 보상, 해킹 피해 금액을 회수(counter-hacking)하는 방법 등 다양한 방법을 활용하여 적극 대처.

Ⅱ. 북한의 암호화폐 공격: 사례와 특징

1. 암호화폐에 대한 사이버공격

- 암호화폐는 중개기관이 존재하지 않는 탈중앙화(deceontralization)가 특징으로 2008년 세계 금융위기 이후 기존 금융제도에 대한 불신과 반감이 배경이 되어 탄생
  - 기존통화는 중앙은행이 발행하여 통화량을 조절하는 반면 암호화폐는 화폐에 대한 모든 권리를 제어하는 중앙이 존재하지 않아 발행주체에 따른 가치 조작 문제에 대한 우려 불필요
  - 2009년 첫 암호화폐인 비트코인(Bitcoin)을 시작으로 2022년 현재는 수천여개의 암호화폐가 존재하며 암호화폐 시장은 1조 달러의 가치를 지닌 것으로 평가

- 암호화폐는 거래내용을 암호화하여 실제 소유주를 확인하기 쉽지 않고 도난·분실시 익명성으로 인해 범인을 잡기 어려워 거래소와 투자자 모두 해커의 표적이 되고 있음[6]

- 암호화폐와 관련된 해킹은 암호화폐거래소와 블록체인 정보 지갑(info wallet)에 대한 공격이 가장 일반적
  - 해킹 피해로 인해 피해자는 정보 및 자산 손실, 컴퓨터의 성능 장애, 문제해결을 위한 시스템 교체 등의 피해를 입게 됨
  - 최초의 암호화폐 해킹사례는 2011년 6월, 비트코인 포럼 이용자 '올인베인(Allinvain)'이 당시 50만 달러 상당의 2만 5천개의 비트코인을 도난당한 것

- 암호화폐거래소에 대한 사이버 공격은 주로 아시아 국가에 집중되는 경향
  - 2014년 2월, 일본의 가상화폐거래소 마운트곡스(Mt. Gox)는 85만 개의 비트코인을 도난(역대 최대금액)당한 후 파산
  - 국내 가상화폐거래소 빗썸(Bithumb)은 최근 5년간 무려 3번의 해킹을 당한 것으로 확인

6) 김문환, "가상화폐 해킹에 대한 사례 연구," pp. 23-54.

- 암호화폐 시장은 계속 확장세에 있는 데다 해킹 수법이 점차 진화함에 따라 피해 규모 역시 증가할 것으로 예상
  - 암호화폐 해킹에 따른 총 피해 금액은 2018년 17억 달러, 2019년 45억 달러, 2020년 19억 달러, 2021년 140억 달러로 추정[7]
  - 해킹 기법은 브라우저 기반(browser-based) 해킹 기법이 가장 빠르게 증가하는 범죄 유형이었으나 최근 몇 년 사이 수익성이 더 높은 랜섬웨어(ransomware)쪽으로 점차 증가하는 상황[8]
  - 다만 심각한 가격변동이 발생하는 암호화폐의 특성상 해킹을 통해 얻을 수 있는 수익에 편차가 있을 수밖에 없으며 최근에는 암호화폐 가격이 하락함에 따라 해킹 피해 금액의 총액 또한 줄어들 것으로 전망

2. 북한의 대표적인 암호화폐 공격 사례[9]

- 북한은 2017년 2월 국내 암호화폐거래소인 2위 업체인 빗썸에 대한 700만 달러 해킹의 배후로 지목되면서 자금 마련 목적의 해킹에 본격적으로 착수한 것으로 알려짐
  - 2017년 6월에는 빗썸이 2차 공격을 당하면서 자금 탈취뿐만 아니라 직원 PC 해킹에 따른 회원 3만여 명의 개인정보 유출 사고까지 발생[10]

- 2018년 1월, 암호화폐를 채굴하고 본국으로 송금토록 하는 북한의 악성 프로그램이 발견되면서 대북 경제제재를 상쇄할 외화벌이 수단으로 암호화폐에 대한 북한의 관심이 재확인됨
  - 비트코인 채굴경쟁이 심해지자 북한 출신 해커들은 암호화폐 모네로(Monero)를 채굴하여 김일성종합대학의 서버로 자금을 송금

7) 암호화폐 가격 상승에 따라 2021년 해킹 금액 역시 사상 최대로 증가하였다. Smiljanic Stasha, “Cryptocurrency Hacking Statistics: Facts on Crypto,” Policy Advice, February 13, 2022, http://policyadvice.net/money/insights/cryptocurrency-hacking-statistics/ (검색일: 2022.9.7.); MacKenzie Sigalos, “Crypto Scammers Took a Record $14 Billion in 2021,” NBC News, January 7, 2022, https://www.nbcnews.com/tech/security/crypto-scammers-took-record-14-billion-2021-rc-na11192 (검색일: 2022.9.7.).

8) 그러나 가장 많이 발생하는 암호화폐 해킹 기법은 1년마다 달라질 수 있다.

9) 북한의 암호화폐 해킹사례는 월렛, 거래소, 랜섬웨어 공격 등으로 나누어 볼 수 있으나 기술적 분류에 대한 논란의 여지가 있어 본 보고서에서는 이와 같은 분류는 생략한다.

10) 2017년 발생한 빗썸 암호화폐거래소 해킹은 북한 해킹 조직인 라자루스 그룹(the Lazarus Group)의 소행으로 추정되었다.

• 북한의 해킹조직들은 빗썸뿐만 아니라 코인이즈(Coinis), 업비트(Upbit)와 유빗(Youbit) 등 국내 암호화폐거래소에 대한 공격을 자주 벌인 것으로 확인
  - 북한은 2017년 4월 야피존(유빗 전신), 2017년 9월 코인이즈, 2017년 12월 유빗 등에 대한 암호화폐 도난 사건이 발생하였으며 해킹에 쓰인 악성코드를 바탕으로 북한 해킹조직 라자루스 그룹(the Lazarus Group)이 배후로 추정되었음[11)]
  - 빗썸은 북한으로부터 해킹 피해를 가장 자주 받은 국내거래소로 UN안보리 대북제재위원회 패널보고서에 따르면 북한은 무려 네 차례의 공격을 감행하면서 2017년 2월 700만 달러, 2017년 6월 최소 700만 달러, 2018년 3,100만 달러, 2019년 2,000만 달러를 탈취[12)]
  - 이밖에 북한은 2019년 11월 업비트를 공격해 이더리움(Ethereum)을 탈취하였으며 4,900만 달러의 손실을 준 것으로 확인

• 2020년 9월, 북한의 해킹 조직인 라자루스 그룹이 슬로바키아의 소규모 암호화폐거래소에 침입하여 약 540만 달러의 암호화폐를 강탈하는 등 한국뿐만 아니라 다른 해외국가들을 표적으로 삼고 공격을 지속[13)]
  - 북한은 세계최대 암호화폐거래소인 바이낸스(Binance)에서 최소 20개의 익명 계정을 개설하여 훔친 자금을 전환하고 자금 추적을 어렵게 만들었으며 미 정부는 이 사건을 북한의 핵프로그램에 자금 지원을 목표한 사이버 강탈 중 하나로 평가[14)]

• 2022년 3월, 라자루스 그룹이 블록체인 기반 게임업체인 '액시 인피니티(Axie Infinity)'를 상대로 감행한 해킹은 6억 1,500만 달러라는 역대 최대 규모의 손실을 낸 사건으로 기록
  - 라자루스 그룹은 게임에 활용되는 네트워크 시스템 '로닌(Ronin)'을 해킹한 후 훔친 암호화폐를 숨기기 위한 목적으로 1만 2천여 개의 가상계좌 활용
  - 이에 미국 FBI는 북한 해커들이 탈취한 암호화폐를 법정화폐로 만들려는 시도를 추적하면서 암호화폐 관련 업체들이 해당 자금을 동결하도록 함으로써 일부 금액을 회수하는 데 성공

11) 유빗은 해당 사건으로 인한 피해로 파산하였다.
12) 김진욱, "유엔 안보리 "북, 가상화폐 초점으로 사이버 해킹 강화...남한도 뚫려"," 『한국일보』, 2019년 9월 6일, https://www.hankookilbo.com/News/Read/201909060864067555 (검색일: 2022.10.9.).
13) 라자루스 그룹은 정찰총국 소속으로 2014년 소니 픽처스(Sony Pictures) 해킹 사건과 워너크라이(WannaCry) 2.0의 배후로 알려져 있다.
14) Angus Berwick and Tom Wilson, "How Crypto Giant Binance Became a Hub for Hackers, Fraudsters and Drug Traffickers," Reuters, June 6, 2022, https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirty-money/ (검색일: 2022.9.7.).

• 한편 북한은 암호화폐 해킹을 포함하여 코로나19 백신 관련 제약회사 해킹 시도 등 다양한 사이버공격 사건의 배후로 지목되는데 대해 일관되게 혐의를 부정하는 한편 미국에 비난의 화살을 돌리는 상황
  - 북한 외무성은 2022년 2월 8일 미국의 북한에 대한 사이버테러 혐의 제기는 북한에 대한 체질적 거부감이 고안해 낸 창작품이라고 부인하면서 에드워드 스노든 사례나 미국의 유럽 정치인에 대한 도청 의혹을 거론하며 반발[15]
  - 외무성은 2022년 4월 13일에도 홈페이지에 미국을 "지구상에서 없어져야 할 해커왕국"으로 지칭하며 맹비난하고 모든 해킹 혐의를 부인
    ※ 북한은 미국이 우크라이나 사태가 터지자 반러시아 사이버 전쟁에 공포와 불안을 야기하는 온갖 허위자료를 유포하고 있다고 주장[16]

3. 북한의 암호화폐 공격 양상과 특징

(1) 북한의 암호화폐 공격 양상

• 북한의 암호화폐 공격의 심각성은 2010년대 중반부터 부각되기 시작
  - 2000년대 후반 이후 북한은 본래 한국의 정부 기관, 웹사이트, 국방 인프라에 대한 파괴적인 사이버 공격을 개시하였으나 세계 금융시스템의 추세를 날카롭게 인식하면서 제재 회피 방안을 모색
  - 비트코인을 비롯한 암호화폐 가격 상승과 맞물려 미국·UN 대북제재가 확대되면서 북한은 은행과 암호화폐거래소 등 금융기관 쪽으로 사이버공격의 방향을 전환[17]
    ※ 북한의 금융권 공격은 일부 정치적 동기부여에 따르기도 했으나 대부분은 재정적 이유의 사이버 공격이었던 것으로 확인

15) 북한 외무성, "도청제국, 해킹왕초, 비밀절취국으로 악명높은 미국," 2022년 2월 8일.
16) 북한 외무성, "지구상에서 없어져야 할 해커왕국," 2022년 4월 13일.
17) Jason Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program," The Diplomat, July 18, 2022, https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/ (검색일: 2022.10.6.).

- 2016년부터 북한은 랜섬웨어, 은행 드롭(bank drops), 분산 서비스 거부(DDos), 공급망 공격과 같은 악성코드가 얽힌 스피어피싱 등 다양한 사이버 침입과 암호화폐 해킹 전술을 금융기관을 상대로 시행
  - 북한은 주로 피싱 공격을 통해 해외의 암호화폐 지갑에 침입하거나 가짜 링크드인(LinkedIn) 페이지에서 채용공고를 활용하여 피해자들을 유입하거나 암호화폐거래소를 직접 공격
  - 이후 북한은 탈취한 암호화폐를 쪼개 누가 전송했는지 출처를 불분명하게 만드는 믹싱(mixing) 기술을 활용하여 암호화폐의 이동 추적을 어렵게 만듦

  ※ 북한은 비트코인을 기반으로 하는 블렌더(Blender.io)와 이더리움을 기반으로 하는 토네이도 캐시(Tornado Cash)를 통해 믹싱 서비스를 받았으며 그 결과 2천만 달러가 넘는 비트코인과 5천만 달러 상당의 이더리움을 세탁한 것으로 추정[18]
  - 자금세탁 과정이 끝나면 해커들은 암호화폐를 아시아 기반 거래소로 이동시켜 중국의 인민폐와 같은 법정 통화로 교환하여 현금 확보[19]

(2) 북한의 암호화폐 해킹 규모

- 분석기관마다 일부 차이는 존재하지만, 공통적으로 북한의 암호화폐 공격과 피해 규모가 해마다 증가하고 있는 것으로 분석
  - 2011년부터 2022년 사이 발생한 암호화폐 해킹 사건 중 북한은 가장 많은 15건의 암호화폐 해킹을 시도한 것으로 알려짐[20]
  - 아일랜드 암호화폐 분석업체 코인컵(Coingcub)은 북한이 2017년부터 2021년까지 탈취한 암호화폐의 가치가 총 16억 달러에 달할 것으로 평가[21]

18) 고명현, ""Winter Is Coming," 북 암호화폐 해킹 꼼짝 마!," 『신동아』, 2022년 10월 6일, https://https://n.news.naver.com/mnews/article/262/0000015934?sid=104 (검색일: 2022.10.8.).

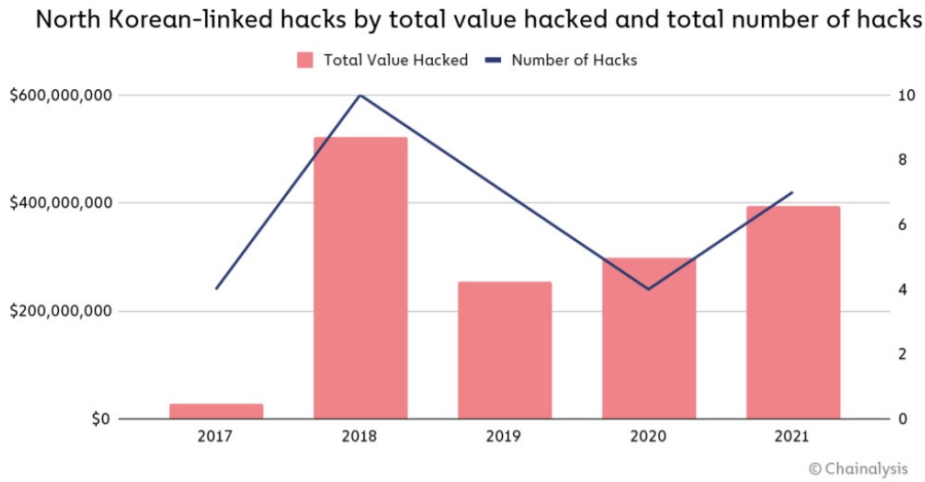
19) 위의 내용은 Chainalysis Team, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," Chainalysis, January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/ (검색일: 2022.9.30.).

20) 임재섭, "암호화폐 해킹 시도, 북이 가장 많아...아일랜드 암호화폐 분석업체 설명," 『디지털타임스』, 2022년 6월 30일, http://www.dt.co.kr/contents.html?article_no=2022063002109958050002 (검색: 2022.9.8.). 다만 UN대북제재위원회에 의해 파악된 암호화폐 해킹사례 건수일뿐 실제로는 더 많을 것으로 추정되었다.

21) 강영진, "북한 암호화폐 탈취 해킹 전세계에서 가장 활발," 『뉴시스』, 2022년 6월 30일, https://newsis.com/view/?id=NISX20220630_0001925595&cID=10101&pID=10100 (검색일: 2022.9.8.).

- 블록체인 분석업체인 체이널리시스(Chainalysis)에 따르면 북한과 연계된 해킹조직이 2022년까지 훔친 암호화폐의 가치는 10억 달러에 달할 것으로 평가([그림 1] 참조)[22]

[그림 1] 2017-2021년 북한이 해킹을 통해 벌어들인 총액



*출처: 체이널리시스[23]

- 다만 암호화폐 공격을 통한 거액의 탈취에도 불구하고, 북한은 추적을 피해 암호화폐를 안정적인 자금원으로 현금화하는데 어려움을 겪고 있는 것으로 확인
  - 북한은 책임을 회피하기 위해 훔친 자금을 오랜 시간에 걸쳐 소량씩 현금으로 전환하고 자금 추적을 모호하게 만들려 노력하는 것으로 알려져 있음
  - 그러나 대량의 암호화폐를 현금화할 수 있는 거래소가 많지 않은 데다 해킹 피해 방지를 위해 주요 국가들이 감시와 제재를 강화하면서 자금세탁 방지 규정을 강화하고 있는 상황[24]

22) Sidhartha Shukla, "Crypto Hacks Soar as North Korea Targets Defi," Bloomberg, August 16, 2022, https://https://www.bloomberg.com/news/articles/2022-08-16/crypto-hacks-soar-as-north-korea-targets-defi-chainalysis-says (검색일: 2022.10.6.).

23) Chainalysis Team, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," Chainalysis, January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/ (검색일: 2022.9.30.).

24) 고명현, ""Winter Is Coming," 북 암호화폐 해킹 꼼짝 마!," 『신동아』, 2022년 10월 6일, https://https://n.news.naver.com/mnews/article/262/0000015934?sid=104 (검색일: 2022.10.8.).

- 미처 현금화하지 못한 암호화폐들이 있는 상태에서 암호화폐가 급격한 가격 하락을 맞이하면서 북한이 벌어들일 수 있는 불법적 외화수입 역시 감소할 것으로 분석
  ※ 블록체인 분석업체인 체이널리시스(Chainalysis)는 북한이 현금화하지 못한 암호화폐가 2021년 말 1억 7,000만 달러어치였으나 암호화폐 가치 하락으로 6,500만 달러 수준으로 급감하였을 것으로 분석[25]

• 흥미로운 점은 최근 암호화폐 가격 하락과 현금화 문제에도 불구하고 북한이 암호화폐거래소에 대한 공격을 계속하고 있다는 사실
  - 저비용, 익명성, 높은 수익성 등 암호화폐 공격을 통해 얻을 수 있는 장점이 확실한 반면 고강도 제재에 놓인 상태에서 외화확보를 위한 별다른 방법이 없는 북한으로서는 가치 하락에도 불구하고 암호화폐 해킹에 주력할 수밖에 없는 것으로 판단[26]

(3) 북한의 암호화폐의 다목적 활용 고려

• 북한은 대북제재의 돌파구로 암호화폐와 블록체인 등 첨단기술에 관심을 두고 '평양 블록체인·가상화폐 콘퍼런스'를 개최하여 관련 기술의 국제적인 네트워크 구축의 기회로 활용하려 시도
  - 북한은 해외의 기술전문가들을 초청하여 북한 IT·과학기술계 인사와 교류하고 암호화폐 기술을 이용하여 제재를 우회하는 방법을 확보하려 했던 것으로 확인[27]
  - 2019년 4월, 1회 회의에서 강연했던 버질 그리피스(Virgil Griffith)와 크리스토퍼 엠스(Christopher Emms)는 북한에 제재를 회피할 수 있는 암호화폐 거래방식을 제안하고 북한이 암호화폐 기술을 활용하여 글로벌 금융 시스템에서 독립 가능할 수 있을지 논의[28]
    ※ 북한은 이듬해인 2020년 2월, 제2차 "'평양 블록체인·가상화폐 콘퍼런스'"를 개최하려고 하였으나 UN안보리 경고, 북한행 항공편 중단, 미국의 그리피스와 엠스 기소, 코로나19 발생 등의 문제로 인하여 행사 취소

25) Choe Sang-Hun and David Yaffe-Bellany, "How North Korea Used Crypto to Hack Its Way Through the Pandemic," *The New York Times*, July 1, 2022, https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html (검색일: 2022.9.8.).

26) 암호화폐 가치 하락으로 최근에는 북한이 다시 금융권 공격에 관심을 두고 있다는 분석도 있다. 조상진, "북한 해킹조직, 암호화폐 폭락으로 전통적 금융권 공략 조짐," VOA, 2022년 6월 18일, https://www.voakorea.com/a/6622206.html (검색일: 2022.10.1.).

27) 대북 기술유출 차단조치를 우회하기 위해 기술협력 제한이 없는 EU 전문가와의 네트워크 구축 기회로 활용하려 했던 것으로 보인다. 김민관, ""평양 암호화폐 국제콘퍼런스" 개최 가능성 점검," Weekly KDB Report, 2020년 2월 10일, p. 9.

28) 버질 그리피스는 이더리움(Ethereum) 재단의 공동 창시자이며 크리스토퍼 엠스는 암호화폐 컨설팅업체 토큰키(Token-Key)의 대표이다.

- 북한이 경제제재와 미국 중심의 글로벌 금융 시스템에 대처하기 위해 자신들만의 암호화폐를 개발 중이며 중국과 협력할 가능성도 있는 것으로 확인
  - 2019년 9월 외신보도에 따르면 북한은 암호화폐, 채굴, 교환 해킹, 크립토재킹(암호화폐 채굴) 등에 많은 관심을 갖고 있으며 자체 암호화폐 개발 및 도입에 필요한 전문지식은 이미 갖춘 것으로 보임[29)]
  - 비록 초기단계이긴 하지만 북한 정부는 일부 외국 기업들과 교육, 의료, 금융 등의 분야에서 블록체인 시스템 개발을 위한 협약까지 체결한 것으로 보도[30)]

Ⅲ. 북한의 암호화폐 공격에 대한 미국의 대응

1. 경제제재와 카운터해킹, 포상 프로그램의 실행

(1) 사이버 범죄 담당 전문 부서 신설

- 미국 바이든 정부는 사이버공간에서의 위협을 정책 우선순위로 상정하고 해킹 공격 또는 암호화폐 탈취 등 각종 사이버 범죄를 전문적으로 다루는 부서들을 잇따라 신설
  - 2021년 10월, 미 법무부는 암호화폐 관련 불법 활동을 수사하기 위해 전담 부서로 '국가 암호화폐단속국(National Cryptocurrency Enforcement Team, NCET)'을 신설
  - 2022년 4월 4일, 미 국무부는 사이버 공간 내 규정을 논의하고 랜섬웨어 확산 및 인터넷 문제 해결을 위해 '사이버공간 및 디지털 정책국(Bureau of Cyber Space and Digital Policy, CDP)'을 출범

29) David Gilbert, "North Korea Is Building Its Own Bitcoin," Vice, September 19, 2019, https://www.vice.com/en/article/9ke3ae/north-korea-is-building-its-own-bitcoin. (검색일: 2022.9.8.).
30) Ibid.

(2) 사이버공격 사전 경보발령 및 보고서 발간

- 미국의 사이버안보 관련 기관들은 북한에 특화된 대응책 마련을 위해 사이버공격에 대한 경보발령과 함께 북한 사이버공격의 특징을 정리한 보고서들을 발표하여 경각심 제고[31]
  - 2020년 8월 26일, 연방수사국(FBI)과 CISA는 북한 해커들의 불법송금과 현금자동입출금기(ATM)를 통한 불법인출 시도에 대한 경보 발령[32]
  - 2020년 4월, CISA, 재무부, 국토안보부, FBI는 암호화폐 공격을 포함한 북한의 악의적인 사이버 활동 관련 경보발령 보고서 발표[33]
  - CISA, 사이버사령부, FBI는 2020년 5월 12일, 북한 해커들이 사용하는 악성코드 3개에 대한 개요와 대응 권장사항, 피해 경감대책 등이 정리된 분석보고서를 작성하여 발간[34]

(3) 제재와 처벌

- 미국 재무부와 법무부는 암호화폐 탈취 관련 대북제재 조치를 내리는 한편 일부 해커들을 기소
  - 재무부는 2019년 9월, 라자루스 그룹·블루노로프(BlueNorOff)·안다리엘(Andariel) 등 북한의 대표적인 사이버 범죄 조직들을 제재 리스트에 올렸으며 2021년 12월에는 미 법무부가 박진혁, 김일, 전창혁 등 북한의 악명 높은 해커들 3명을 기소
    ※ 박진혁의 경우 이미 수년 전 북한으로 되돌아간 것으로 알려져 사실상 미국이 실제로 그를 체포하거나 법원에 출석시킬 방법은 없으나 기소와 사진·실명 공개를 통해 북한 사이버 범죄 근절에 대한 미 정부의 강력한 의지를 보여준 것으로 평가

- 미국 정부는 북한 해킹그룹과 해커들에 대한 직접적인 제재뿐만 아니라 북한의 자금세탁을 도운 인물과 기업들에 대한 처벌도 강화하는 상황
  - 법무부는 자금세탁을 도운 갈렙 알라우마리(Ghaleb Alaumary)에게 11년 형을 선고하는 한편 재무부는 2022년 5월, '액시 인피니티(Axie Infinity)'에서 해킹한 6억 1500만 달러 중 일부 세탁에 가담한 혐의를 갖는 믹서 기업 '블렌더(Blender)'에 대한 제재 부과

31) 김보미·오일석, "김정은 시대 북한의 사이버 위협과 주요국 대응," 『INSS 전략보고』, 147호, p. 15.
32) Cyber Security and Infrastructure Security Agency, "Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," August 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a (검색일: 2022.10.9).
33) Cyber Security and Infrastructure Security Agency, "Alert (AA20-106A): Gudiance on DPRK Cyber Threat Advisory," April 15, 2020, https://www.cisa.gov/uscert/ncas/alerts/aa20-106a (검색일: 2022.11.20.).
34) Cyber Security and Infrastructure Security Agency, "North Korean Malicious Cyber Activity," May 12, 2020, https://www.us-cert.gov/ncas/current-activity/2020/05/12/north-korean-malicious-cyber-activity (검색일: 2022.10.9.).

- 또한 미 재무부는 2022년 8월, 믹서 기업 '토네이도 캐시(Tornado Cash)'를 통해 라자루스 그룹이 4억 5,500만 달러의 암호화폐를 세탁했다고 발표하고 해당 기업의 미국내 자산을 동결시키고 미국인과의 거래를 금지[35]
- 2022년 4월, 미 사법당국은 허가없이 2019년 평양에서 열린 암호화폐 회의('평양 블록체인·암호화폐 콘퍼런스')에 참가하고 북한 주민들에게 암호화폐와 기술에 대해 교육한 미국인 암호화폐 전문가 버질 그리피스를 63개월의 징역형에 처함[36]

• 다른 한편으로 미국 정부는 사이버공격 제보에 현상금을 인상하는 등 처벌과 포상을 모두 활용
- 미 국무부가 운영하는 테러정보신고보상 프로그램인 "정의를 위한 보상(Rewards for Justice)"의 공식 트위터는 북한의 사이버공격 신고시 현상금을 500만 달러에서 1,000만 달러로 2배 인상을 선언

(5) 카운터해킹(counter-hacking)[37]

• 미국은 또한 북한이 해킹한 불법자금을 다시 회수하는 방식으로 대응함으로써 북한의 돈줄을 차단하는 등 북한의 진화하는 사이버 공격에 맞서 적극적이고 전방위적으로 대응
- 2022년 9월, 미 FBI가 라자루스 그룹이 액시 인피니티에서 훔친 암호화폐를 현금화하려는 시도를 파악하고 거래를 동결하여 3천만 달러 이상을 회수하였다는 발표
- 2022년 7월, 미 법무부와 FBI가 캔자스주의 한 병원이 랜섬웨어 공격을 당해 라자루스 그룹에 몸값으로 지불한 암호화폐 50만 달러어치를 회수한 사실 공개

• 미국의 카운터해킹은 북한의 해킹 능력이 날로 진화하고 있는 만큼, 미국의 대응방법 또한 다양화되고 있으며 대응방향 또한 적극적으로 변모하고 있다는 사실을 반증한다고 볼 수 있음

35) U.S. Department of The Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," August 8, 2022, https://home.treasury.gov/news/press-releases/jy0916. (검색일: 2022.9.8.).
36) 혐의는 국제비상경제권법(the International Emergency Economic Powers Act), 대북제재 행정명령 위반이었으며 그리피스는 '블록체인과 평화(Blockchain and Peace)'라는 제목으로 프레젠테이션을 한 것으로 알려졌다.
37) 해킹으로 탈취당한 자금을 다시 회수하는 방법.

2. 국제협력 강화

(1) 양자 및 다자협력 합의

- 현재 사이버위협에 공동으로 대응할 수 있는 플랫폼은 부재하지만 바이든 집권 이후 미국 정부는 다양한 국제회의, 정상회담 등을 통해 사이버위협에 대응한 국제협력의 필요성을 더욱 강력히 주장하는 상황
  - 2021년 10월, 미국은 유럽, 중동, 아프리카, 아시아 등 주요국 30개국을 초대하여 랜섬웨어 대책 회의를 개최하고 공동 대응을 위한 외교적 협력의 내용을 담은 공동성명 발표[38]
  - 2022년 5월, 한미정상회담에서 윤석열 대통령과 바이든 미 대통령은 한미가 북한 핵 프로그램뿐만 아니라 사이버안보와 관련하여서도 협력을 강화하기로 합의

- 특히 북한의 암호화폐 해킹과 관련하여 미국 정부는 전 세계가 돈세탁 방지 규칙에 대한 사이버보안 조처를 이행할 것을 강조
  - 미 국무부는 북한에 초점을 맞추어 국가 지원을 받는 해커들에 의한 위협에 대응하여 국제사회의 공동 대응의 필요성을 강조하고 있으며 CDP를 설립함으로써 다른 나라와 협력을 조율할 것으로 예상

(2) 사이버 방어훈련 및 군사작전 실행

- 미국은 군사적 차원에서 2011년부터 매년 사이버사령부(U.S. Cyber Command) 주관하에 다국적 사이버 방어훈련인 '사이버 플래그(Cyber Flag)'를 개최
  - 동맹, 우방국과의 연합 사이버 준비태세 및 파트너십을 강화하기 위한 사이버 방어훈련으로 참여국간 위협 정보를 공유하고 효과적인 대응방법을 도출하여 방어작전의 효과를 검증
  - 한국은 2022년 10월 24일부터 28일까지 개최하는 사이버 플래그에 최초로 참여하여 영국, 캐나다, 호주 등 20여개국과 함께 국방 사이버 대응역량을 한층 강화할 것으로 기대[39]

38) U.S. Department of State, "Update on the International Counter-Ransomware Initiative," October 15, 2021, https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative (검색일: 2022.10.9.).

39) 김지헌, "한국, 미 '사이버 플래그' 훈련에 첫 참가...다국적 사이버방어," 연합뉴스, 2022년 10월 24일, https://yna.co.kr/view/AKR20221024028100504?input=1195m (검색일: 2022.10.24.).

• 나아가 미국은 '헌트 포워드(Hunt Forward)' 사이버 작전을 실시하고 있으며 북한의 악의적 사이버 활동에 대응하기 위해 한국과의 협력 또한 예고
  - 정보(intelligence) 기반 및 파트너 요청에 의한 방어적 사이버 작전으로 악의적인 사이버 위협 활동을 관찰 및 식별하여 국토방위를 강화하고 사이버 위협에 대한 중요 네트워크의 복원력을 높이는 것을 목표로 설정[40)]
    ※ 미 사이버사령부 사이버국가임무부대(Cyber National Mission Force)는 2018년부터 에스토니아, 리투아니아, 크로아티아, 몬테네그로, 북마케도니아, 우크라이나 등 18개국에서 35건의 작전 수행[41)]
  - 2022년 9월 16일, 미 사이버사령부를 방문한 신범철 국방부 차관과 티모시 호(Timothy D. Haugh) 부사령관은 암호화폐 해킹 등 북한 사이버 위협에 대해 헌트 포워드 연합을 비롯한 작전공동 대응의 필요성에 공감한 것으로 확인[42)]

Ⅳ. 결론: 한국에 주는 시사점

• 김정은 집권 이후 북한의 사이버 공격은 더욱 대담하게 전개되고 있으며 특히 경제제재를 우회하고 핵·미사일 개발을 지탱하기 위해 북한은 암호화폐 공격을 통한 외화확보 노력을 계속
  - 2022년 9월 28일 미 하버드대 벨퍼센터(Belfer Center)가 발표한 '국가 사이버 역량 지표 2022(National Cyber Power Index 2022)'에 따르면 북한의 종합순위는 전 세계 14위지만 암호화폐 해킹 등의 사이버 공격 역량에 힘입어 사이버 금융 분야에서 1위를 기록[43)]

40) U.S. Cyber Command, Public Affairs, "U.S. Conducts First Hunt Forward Operation in Lithuania," May 4, 2022, https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/ (검색일: 2022.10.9.).

41) Ibid.

42) 우리의 경우 평시에는 국가정보원이 전시에는 사이버사령부가 주가 되어 사이버안보활동을 수행하고 있으나 미국의 경우 평시에도 사이버사령부가 불법적 사이버활동 차단 활동을 수행한다는 차이점이 있다.

43) Julia Voo, Irfan Hemani, Daniel Cassidy, National Cyber Power Index 2022, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2022, p. 11.

- 우리 정부는 북한에 의한 사이버위협에 대응하기 위해 법령제정, 기업 보안 위반시 제재, 사이버위협 관련 정보 공유, 국제공조를 강화해 나가고 있는 상황
  - 우리 정부는 2022년 5월 한미정상회담을 개최하여 사이버 안보 전반에 걸쳐 미국과의 공동대응에 합의하고 2022년 5월 NATO의 사이버방위센터 회원 가입을 통해 양자 및 다자협력 강화에 합의
  - 국가정보원(이하 국정원)의 경우 국내 대형 암호화폐거래소인 업비트, 빗썸, 코빗(Korbit), 코인원(Coinone) 등 4곳에 국내·외 주요 사이버위협정보를 제공하는 등 정보 공유 서비스를 확대하는 중
  - 방송통신위원회는 2017년 12월, 개인정보 파일을 암호화하지 않고 백신 소프트웨어 업데이트를 하지 않는 등 보안조치 소홀을 이유로 빗썸에 과징금과 과태료를 부과하였으며 이는 암호화폐거래소에 대한 첫 제재조치 사례로 기록됨

- 그러나 우리의 경우 북한으로부터의 사이버공격의 피해규모에 비해 미국보다 적극적 대응을 펼치지 못하고 있으며 미국을 비롯한 국제사회 주요국들 및 기관들과 국제협력을 통해 미비점을 보완해 나갈 필요가 있음

- 자체적으로는 암호화폐 추적이나 환수에 있어서 해외기업 및 정부의 기술력에 의존하는 측면이 크기 때문에 우리 정부와 기업들의 암호화폐 추적 기술역량 고도화 필요

- 북한의 사이버위협에 대응한 국제공조는 협력 의지 표명뿐만 아니라 구체적 실현방안이 필요하며 효과적이고 장기적인 사이버 안보전략을 수립하는 데 초점을 맞추어야 할 것
  - 북한의 사이버 위협과 관련하여 보고서를 주요 협력국과 합의하여 백서형태로 1년 또는 2년 주기로 발간하고 암호화폐 공격 기법 공개, 성공적 대응 사례 소개, 기술적 대응방안 공유
  - 제재에 대한 실효성과는 별개의 문제로 독자제재나 북한 사이버 공격으로 피해를 입은 국가들과 함께 공동제재에 참여하는 방식을 취할 수도 있음
  - 북한을 비롯한 국가 연계 사이버 행위자의 위협과 위험성을 설명한 사이버 공동주의보 발표 또한 한미 사이버 실무그룹의 출발점이 될 수 있을 것으로 기대

- 자체적으로는 기업에 대한 보안 관리뿐만 아니라 관련 법령을 정비하는 한편 미국과 마찬가지로 실질적 대응방식으로서 카운터해킹을 통해 탈취된 자금 회수하기 위한 적극적 노력 필요
  - 관련 기업들이 해킹 피해에 대한 신고를 의무화하는 법령 제정 필요
  - 2021년 5월 28일, 경찰청 국가수사본부는 최초로 해외거래소로부터 해킹당한 45억원 상당의 암호화폐를 환수하는 등 피해자 보호를 위해 적극적으로 대응[44)]

- 이와 같은 자체적인 노력과 국제적 협력을 통해 북한의 암호화폐 공격으로 인한 손실을 최소화하고 북한이 훔친 자금을 핵·미사일 프로그램에 투자하지 않도록 저지하여야 할 것

44) 박홍용, "경찰, 국내 최초 해외거래소에서 해킹 암호화폐 환수…"45억원 상당,"" 『서울경제』, 2021년 6월 7일, https://www.sedaily.com/NewsView/22NJM0NZ82/ (검색일: 2022.10.1.).

참고문헌

국내문헌

강영진. “북한 암호화폐 탈취 해킹 전세계에서 가장 활발.”『뉴시스』. 2022년 6월 30일, https://newsis.com/view/?id=NISX20220630_0001925595&cID=10101&pID=10100 (검색일: 2022.9.8.).

고명현. ““Winter Is Coming,” 북 암호화폐 해킹 꼼짝 마!.”『신동아』. 2022년 10월 6일, https://https://n.news.naver.com/mnews/article/262/0000015934?sid=104 (검색일: 2022.10.8.).

김문환. “가상화폐 해킹에 대한 사례 연구,”『한국산업보안연구』. 제9권 제2호 (2019), pp. 23-54.

김민관. ““평양 암호화폐 국제콘퍼런스” 개최 가능성 점검,” Weekly KDB Report, 2020년 2월 10일, pp. 8-10.

김보미·오일석. “김정은 시대 북한의 사이버 위협과 주요국 대응,”『INSS 전략보고』. 147호.

김지헌. “한국, 미 ‘사이버 플래그’ 훈련에 첫 참가...다국적 사이버방어.” 연합뉴스. 2022년 10월 24일, https://yna.co.kr/view/AKR20221024028100504?input=1195m (검색일: 2022.10.24.).

김진욱. “유엔 안보리 “북, 가상화폐 초점으로 사이버 해킹 강화...남한도 뚫려”.”『한국일보』. 2019년 9월 6일, https://www.hankookilbo.com/News/Read/201909060864067555 (검색일: 2022.10.9.).

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 (검색일: 2022.10.1.).

박홍용. “경찰, 국내 최초 해외거래소에서 해킹 암호화폐 환수…“45억원 상당”.”『서울경제』. 2021년 6월 7일, https://www.sedaily.com/NewsView/22NJM0NZ82/ (검색일: 2022.10.1.).

임재섭. “암호화폐 해킹 시도, 북이 가장 많아...아일랜드 암호화폐 분석업체 설명.”『디지털타임스』. 2022년 6월 30일, http://www.dt.co.kr/contents.html?article_no=2022063002109958050002 (검색: 2022.9.8.).

조상진. “북한 해킹조직, 암호화폐 폭락으로 전통적 금융권 공략 조짐.” VOA. 2022년 6월 18일, https://www.voakorea.com/a/6622206.html (검색일: 2022.10.1.).

북한문헌

『노동신문』. 2022년 9월 9일.
북한 외무성. "도청제국, 해킹왕초, 비밀절취국으로 악명높은 미국." 2022년 2월 8일.
북한 외무성. "지구상에서 없어져야 할 해커왕국." 2022년 4월 13일.

영미문헌

Bartlett, Jason. "Mapping Major Milestones in the Evolution of North Korea's Cyber Program." The Diplomat. July 18, 2022, https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/ (검색일: 2022.10.6.).

Berwick, Angus and Tom Wilson. "How Crypto Giant Binance Became a Hub for Hackers, Fraudsters and Drug Traffickers." Reuters. June 6, 2022, https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/ (검색일: 2022.9.7.).

Chainalysis Team. "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High." Chainalysis. January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/ (검색일: 2022.9.30.).

Choe Sang-Hun and David Yaffe-Bellany. "How North Korea Used Crypto to Hack Its Way Through the Pandemic." *The New York Times*. July 1, 2022, https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html (검색일: 2022.9.8.).

Cyber Security and Infrastructure Security Agency, "Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks." August 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a (검색일: 2022.10.9.).

Cyber Security and Infrastructure Security Agency. "Alert (AA20-106A): Gudiance on DPRK Cyber Threat Advisory." April 15, 2020, https://www.cisa.gov/uscert/ncas/alerts/aa20-106a (검색일: 2022.11.20.).

Cyber Security and Infrastructure Security Agency, "North Korean Malicious Cyber Activity," May 12, 2020, https://www.us-cert.gov/ncas/current-activity/2020/05/12/north-korean-malicious-cyber-activity (검색일: 2022.10.9.).

Gilbert, David. "North Korea Is Building Its Own Bitcoin." Vice. September 19, 2019, https://www.vice.com/en/article/9ke3ae/north-korea-is-building-its-own-bitcoin. (검색일: 2022.9.8.).

Shukla, Sidhartha. "Crypto Hacks Soar as North Korea Targets Defi." Bloomberg. August 16, 2022, https://https://www.bloomberg.com/news/articles/2022-08-16/crypto-hacks-soar-as-north-korea-targets-defi-chainalysis-says (검색일: 2022.10.6.).

Sigalos, MacKenzie. "Crypto Scammers Took a Record $14 Billion in 2021." NBC News. January 7, 2022, https://www.nbcnews.com/tech/security/crypto-scammers-took-record-14-billion-2021-rcna11192 (검색일: 2022.9.7.).

Stasha, Smiljanic. "Cryptocurrency Hacking Statistics: Facts on Crypto." Policy Advice. February 13, 2022, http://policyadvice.net/money/insights/cryptocurrency-hacking-statistics/ (검색일: 2022.9.7.).

United Nations Security Council. S/2022/132, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf (검색일: 2022.10.6.).

U.S. Cyber Command, Public Affairs. "U.S. Conducts First Hunt Forward Operation in Lithuania." May 4, 2022, https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/ (검색일: 2022.10.9.).

U.S. Department of State, "Update on the International Counter-Ransomware Initiative," October 15, 2021, https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative (검색일: 2022.10.9.).

U.S. Department of The Treasury. "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash." August 8, 2022, https://home.treasury.gov/news/press-releases/jy0916. (검색일: 2022.9.8.).

Voo, Julia, Irfan Hemani, Daniel Cassidy, National Cyber Power Index 2022, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2022.

Abstract

North Korea's Cryptocurrency Hacks and U.S. Countermeasures

Bomi Kim
(Institute for National Security Strategy)

Since the mid-2010s, financial attacks in cyberspace, especially cryptocurrency hacking, have become a major source of foreign currency revenue for the Kim Jong Un regime. Since the late 2000s, North Korea has shifted the direction of cyber attacks toward financial institutions such as banks and cryptocurrency exchanges, and most of these attacks in the financial sector started for financial reasons rather than political motives. Since 2016, North Korea has implemented various cyber intrusion and cryptocurrency hacking tactics particularly against financial institutions, including ransomware, bank drops, DDos, and spear phishing involving malicious codes such as supply chain attacks. As a result, the number of North Korea's cryptocurrency attacks and the dimension of the damage that North Korean hackers caused increased every year, and in March 2022, the hacking conducted by North Koreans against the game company Axie Infinity was recorded as the largest loss in history. The U.S. is actively responding to cryptocurrency hacking as the reason why North Korea was able to develop its nuclear and missile programs by evading sanctions. In addition to economic sanctions against North Korea, the U.S. government has established a department

Abstract

in charge of cybercrime, issued preliminary alerts and published reports in preparation for cyber attacks from North Korea, and issued counter-hacking and compensation for victims of hacking. The U.S. government is also strengthening international cooperation to counter cyber threats, emphasizing the need for joint response to ransomware threats through bilateral and multilateral consultations and asking the world to implement cybersecurity measures against anti-money laundering rules. In our case, it will be necessary to supplement the deficiencies through international cooperation with major international countries and institutions, including the United States.

Keywords: North Korea, Cryptocurrency, hacking, counter-hacking, Hunt Forward

INSS 전략보고

November 2022. No.191

※ 본지에 실린 내용은 집필자 개인의 견해이며, 국가안보전략연구원의 공식입장이 아닙니다.

국가안보전략연구원

06295 서울시 강남구 언주로 120 인스토피아 빌딩
02-6191-1000 02-6191-1111 www.inss.re.kr