ISSUE BRIEF

이슈브리프 472호
(2023.11. 1)

진화하는 북한의 사이버 공격 현황과 대응

제472호

김보미 통일미래연구실

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

올해 2분기까지 전 세계적으로 암호화폐 공격 건수는 전년 동기대비 크게 증가하였고 이중 북한이 차지하는 규모는 약 30%에 육박하는 것으로 알려졌다. 그러나 2023년 3분기까지 북한이 사이버 해킹을 통해 벌어들인 암호화폐 규모는 약 3억 4천만 달러로, 역대 최고 액수를 기록한 2022년에 비해 줄어든 것으로 집계되고 있다. 북한의 암호화폐 해킹을 통한 수입감소는 암호화폐 가격의 급락, 각국의 모니터링과 제재 강화, 탈취한 자금세탁의 어려움에 따른 것으로 추정된다. 그러나 북한은 이 같은 어려움에도 불구하고 다양한 방법을 통해 위기에 대응하는 모습을 보이고 있는데 첫째, 암호화폐에 대한 직접적 공격 외에 랜섬웨어 공격까지 감행하여 자금출처를 다양화하고 둘째, 러시아의 암호화폐거래소를 통해 훔친 자금을 세탁하며 셋째, 기존의 해킹 그룹간 협력을 강화하여 추적을 따돌리려 노력한다. 이처럼 북한의 진화하는 사이버 공격에 대응하여 한국 정부는 법령제정, 국내기업 보안 위반시 제재, 사이버 분야 대북 독자제재, 사이버 위협 관련 정보 공유 등의 다양한 방안을 실행하고 있다. 그러나 다른 무엇보다 자금세탁을 방지하고 해킹을 통해 빼앗긴 자산을 다시 회수하는 카운터해킹 능력을 향상하여 북한의 불법적 외화자금 확보를 근본적으로 차단하고 악의적인 사이버 활동을 위축시키는 것이 가장 중요하다.

핵심어 : 북한, 암호화폐, 라자루스, 사이버 해킹, 러북 협력

2010년대 중반부터 본격화된 북한의 암호화폐 해킹은 현재진행형이다. 미국의 블록체인 분석업체인 체이널리시스(Chainalysis)는 2023년 3분기까지의 전체 암호화폐 피해액에서 북한의 탈취 규모가 29.6%를 차지한다고 밝혔으며 최근 3개월 동안에만 총 2억 4천만 달러의 암호화폐를 탈취한 것으로 확인되었다. 김정은 정권은 사이버 공격을 중요한 외화벌이 수단으로 간주하고 있으며 훔친 암호화폐로 핵미사일 프로그램 발전에 필요한 자금을 충당하고 있는 것으로 알려졌다. 미국 NSC 사이버·신기술 담당 부보좌관인 앤 뉴버거(Anne Neuberger)는 북한이 암호화폐 공격을 통해 미사일 프로그램 자금의 절반을 충당하고 있다고 밝히기도 했다. 북한의 암호화폐 해킹 금액은 2022년 최고점을 찍은 뒤 올해는 다소 하락세를 나타내고 있다. 이 글은 북한의 암호화폐 해킹 금액이 최근 감소하게 된 배경과 이에 대한 북한의 우회전략을 분석하고 우리의 대응방안을 점검 및 제시한다.

2023년 사이버 해킹 피해 규모

북한이 사이버 해킹을 통해 벌어들인 암호화폐는 2022년 역대 최고액수를 기록하였다. 유엔안보리 대북제재위원회 전문가 패널은 2023년 8월 발표한 보고서에서 북한 해커들이 2022년 한 해 동안 사이버 공격을 통해 역대 최고액인 17억 달러를 훔쳤다고 밝혔다. 2023년에도 암호화폐 공격은 꾸준히 시도되었다. 2분기 전 세계 암호화폐 공격 건수는 전년 동기 대비 65.3%가 증가한 81건(지난해 49건)을 기록하였다. 그러나 늘어난 해킹 공격 횟수에 비해 실제 탈취된 자금 총액은 감소하였다. 2023년 3분기까지 북한의 암호화폐 해킹이 차지하는 비중은 29.6%에 달함에도 불구하고 탈취 금액은 약 3억 4천만 달러로 지난해와 비교할 때 다소 줄어든 것으로 집계되고 있다. 그렇다면 2023년 북한의 암호화폐 탈취 금액은 왜 줄어들었을까?

올해 암호화폐 탈취 금액이 감소한 데에는 암호화폐의 특징인

높은 가격 변동성과 현금화 문제, 그리고 주요 국가들의 감시와 제재 강화를 이유로 꼽을 수 있다. 북한은 암호화폐를 탈취한 뒤 추적을 피하기 위해 오랜 시간에 걸쳐 소량씩 현금으로 전환해 왔다. 미처 현금화하지 못한 암호화폐들이 남아있는 상태에서 2021년과 2022년에 암호화폐가 미국의 금리 인상, 테라-루나 폭락, FTX 파산 등 여러 악재로 급격한 가격 하락을 맞이하면서 북한의 불법적 외화수입은 더욱 감소하였다. 체이널리시스는 북한이 현금화하지 못한 암호화폐가 2021년 말 1억 7,000만 달러어치였으나 암호화폐 가치 하락으로 6,500만 달러 수준으로 급감하였을 것으로 분석하였다.

또한 대량의 암호화폐를 현금화할 수 있는 거래소가 많지 않은 데다가 북한은 훔친 암호화폐를 법정화폐로 바꿔줄 수 있는 브로커를 찾아 훔친 통화 가치의 3분의 1만 받는 것으로 알려져 수입은 더더욱 감소하였을 것으로 추정된다. 뿐만 아니라 2022년 역대 최고 손실액을 보인 '액시 인피니티(Axie Infinity)' 해킹 사태가 반면교사의 계기가 되어 주요 국가들이 감시와 제재를 강화하면서 2023년 북한이 취득할 수 있는 암호화폐의 총액이 줄어든 것으로 판단된다.

진화하는 북한의 우회전략

그러나 북한이 전 세계 암호화폐 해킹에서 차지하는 비중은 여전히 절대적이고 사이버공간에서 외화확보를 위한 노력도 중단되지 않고 있다. 그동안 북한이 암호화폐 관련하여 직면한 문제로 탈취한 암호화폐의 현금화와 암호화폐 가격 하락 및 각국의 제재 강화로 인한 수입 감소를 꼽을 수 있었다. 그러나 북한은 위기를 기회로 삼으면서 공격방법과 대상의 다양화, 러시아와의 협력, 해킹 그룹 쇄신 등 다양한 방법을 통해 위기에 대응하고 있다.

첫째, 암호화폐 가치의 불안정성으로 인해 북한은 다시 금융권

공격에 관심을 두기 시작했으며 지난해부터는 랜섬웨어 공격을 증가시키고 있다. 정찰총국 산하 해킹 조직인 라자루스 그룹(Lazarus Group)은 최근 몇 년간 암호화폐 탈취에 집중해왔으나 2022년을 기점으로 랜섬웨어 공격을 다시 늘리고 있다. 랜섬웨어의 경우에는 사이버 보안 체계를 악용하여 피해자의 네트워크를 장악한 뒤 금액을 갈취하고 이를 세탁하기 위해 암호화폐에 의존하게 되어 역시나 북한의 불법적 외화수입 확보와도 깊은 관련이 있다.

둘째, 북한은 러시아로부터 환전 거래 서비스를 받음으로써 현금화 문제의 돌파구를 찾고 있는 것으로 보인다. 북한은 암호화폐 거래소를 직접 공격해오던 패턴을 벗어나 추적을 따돌리기 위해 믹서 및 교차 체인 스왑 기술 등 복잡한 다단계 자금세탁 과정을 거치기 시작했다. 이 과정에서 러시아의 암호화폐 거래소가 북한의 피난처가 되어주고 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. 제재를 정면으로 위반하기 어려운 러시아가 북한의 암호화폐를 낮은 수수료를 받고 세탁하여 간접적인 재정지원을 해 줄 가능성도 배제할 수 없다.

셋째, 북한은 국제사회의 제재에 적극적으로 대응하기 위해 해킹 그룹의 조직 쇄신을 시도하고 있다. 글로벌 사이버 보안 기업인 맨디언트(Mandiant)가 10월 10일 발표한 '2023년 북한 사이버 구조와 조직 평가' 보고서에 따르면 정체를 드러내지 않기 위해 서로 소통하지 않았던 라자루스 그룹(APT38), 안다리엘(Andariel), 템프 허밋(TEMP. Hermit) 등 북한의 해킹조직들이 해킹에 필요한 도구들과 악성코드를 공유함으로써 협업을 강화하기 시작했다고 밝혔다. 특히 북한 내 해커들이 같은 위치에 있거나 심지어 워크스테이션(workstation)을 공유하여 기존 추적을 방해하거나 잘못 오도하는 결과를 낳을 수도 있다고 보았다.

우리의 대응

북한의 진화하는 사이버 공격에 한국 정부는 법령제정, 국내기업 보안 위반시 제재, 사이버 분야 대북 독자제재, 사이버위협 관련 정보 공유, 국제공조 강화 등의 다양한 대응방안을 실행하고 있다. 지난해 11월, 대통령 소속 국가사이버안보위원회를 설치하는 내용을 담은 국가사이버안보기본법 제정안이 입법예고 되었다. 또한 한국 정부는 사이버 산업 발전과 역량 강화를 위해 사이버 10만 인재 양성 프로젝트를 가동할 예정임을 밝혔다. 국방부는 전시 북한의 사이버 공격에 대비하여 사이버 예비군 창설을 추진하기로 했으며 내년 1월에는 한미간 최초의 사이버훈련 역시 추진 중에 있다.

그러나 자체적으로 기업에 대한 보안 관리와 관련 법령을 정비하는 일 뿐만 아니라 자금세탁을 방지하고 해킹을 통해 빼앗긴 자산을 다시 회수할 수 있는 능력을 향상하는 것이 가장 중요하다. 한국 정부는 훔친 자금을 다시 해킹으로 찾아오는 방법인 카운터해킹(counter-hacking)을 시도하여 북한이 훔친 일부 금액을 회수하는 데 노력을 기울이고 있다. 2022년 8월 설립한 한미 실무그룹을 중심으로 북한이 탈취한 가상 자산 100만 달러의 현금화 시도를 포착하여 동결 및 압수하는 성과를 거둔 바 있다.

이밖에 다른 미비점들은 미국을 비롯한 국제사회 주요국들 및 기관들과 국제협력을 통해 보완해 나갈 필요가 있다. 주요 협력국과 합의하여 북한의 암호화폐 공격 기법 공개, 성공적 대응 사례 소개, 기술적 대응방안에 대한 보고서를 백서형태로 발간하여 공유하고 사이버 공동주의보를 발표할 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.

//끝//