북한의 사이버 전력(戰力)과 금융범죄

고명현 | 아산정책연구원 선임연구위원 | mhgo@asaninst.org

Ⅰ. 머리말

사이버 공간은 태생적으로 보안 위협에 취약하다. 사이버 공간의 물리적 바탕이라고 할 수 있는 인터넷은 초기부터 익명성과 개방성을 보장하는 방향으로 설계되었다. 인터넷은 네트워크를 구성하는 IP 주소가 간단한 숫자로 구성되어 있어 쉽게 위조가 가능하기 때문에 외부의 침투에 취약하다. 이러한 사이버 공간의 구조적 익명성은 공격자에게 유리한 환경을 조성하므로 사이버 공간에서 완벽한 보안은 실질적으로 불가능하다.

북한은 이러한 사이버 공간의 비대칭성을 활용하기 위해 사이버전(戰) 능력을 집중적으로 육성하였다. 국방부의 『2018 국방백서』에 따르면 북한의 사이버 전력은 6,800여 명에 달하며 1998년에 첫 사이버부대(121소)를 창설한 이후 꾸준히 조직과 인원이 확장되었다. 그러나 북한 정권 특유의 불투명성으로 인해 정확한 조직체계는 확실치 않다. 대표적으로 북한의 사이버전을 총괄하는 기관이 2012년에 창설된 것으로 알려진 '전략사이버사령부'인지, 아니면 일부의 주장대로 2017년에 '사이버전략사령부'가 신설되어 이전의 전략사이버사령부를 대체하였는지 불분명하다. 최근 한국과 미국의 정부기관이 밝힌 북한의 사이버 전력과 관련해 '전략사이버사령부' 또는 '사이버전략사령부'라는 기관 자체가 언급되지 않고 있다.

이렇게 베일에 싸여 있는 북한의 사이버 전력과 조직과는 달리 북한의 최근 사이버 활동의 추세는 뚜렷한 상승세를 보이고 있다. 특히 2017년 국제사회의 대북제재가 강화된 직후 북한이 배후인 것으로 의심되는 사이버 금융범죄의 빈도가 증가하였다. 북한은 악성코드인 랜섬웨어(ransomware), 방글라데시 중앙은행 사례에서 보여준 스페어 피싱(spear phishing)

범죄 그리고 비트코인 등 암호화폐 탈취 행위로 상당한 수익을 올린 것으로 추정된다. 이와 관련해 「2019 유엔 전문가 위원회 보고서」는 북한이 사이버범죄를 통해 최대 20억달러 가량의 수익을 올렸을 것으로 추정하기도 하였다.[1)]

북한이 사이버 금융범죄를 통해 국제사회의 대북제재 체제를 사실상 무력화할 수 있다는 점에서 북한의 사이버 전력은 한국뿐만 아니라 미국 등 주요 국가들의 큰 관심을 끌고 있다. 북한의 사이버 능력의 실체는 불투명하나, 빠르게 고도화되고 있다는 점만은 분명하다. 먼저 북한 사이버 전력의 구성 및 주요 행위자들에 대한 정보를 정리하고, 다음으로 북한 사이버 금융범죄의 최근 동향을 소개하는 본 연구자료를 통해 북한의 사이버 능력에 대한 이해를 돕고자 한다.

II. 북한의 사이버 전력

1. 북한의 사이버 전력 조직도

북한의 사이버 조직은 베일에 가려 있으나 지금까지 드러난 공개 출처 정보를 종합해 보면 크게 인민군과 정찰총국으로 나눠진다고 할 수 있다. 초창기 사이버 전력 양성을 주도한 것은 인민군이었다. 북한은 1986년에 '군 지휘자동화대학'(현 '김일 군사대학'), 일명 '미림대학'을 설립하여 100여 명의 컴퓨터 전문요원을 처음으로 양성하였다. 이후 1991년에 걸프전이 미국의 압도적 승리로 끝나자 북한은 전자전의 중요성을 통감하여 인민군 총참모부 직속으로 '지휘자동화국'을 창설하였다. 총참모부 산하 지휘자동화국은 현재도 해킹 프로그램을 개발하는 것으로 알려진 31소, 군 관련 프로그램을 개발하는 32소 그리고 지휘통신 프로그램을 개발하는 56소를 운영하고 있으며, 각각 50~60여 명의 장교로 구성되어 있는 것으로 알려져 있다.[2)] 또한 총참모부는 국군과 남한의 청소년, 일반인을 대상으로 사이버 심리전을 펼치는 204소를 휘하에 두고 있다. 이와는 별도로 인민무력부 정찰국은 1998년 사이버 관련 연구부서였던 121소 부대를 해킹과 사이버전을 전담하는 110호 연구소(별칭 기술정찰국)로 확대 개편하였다.[3)]

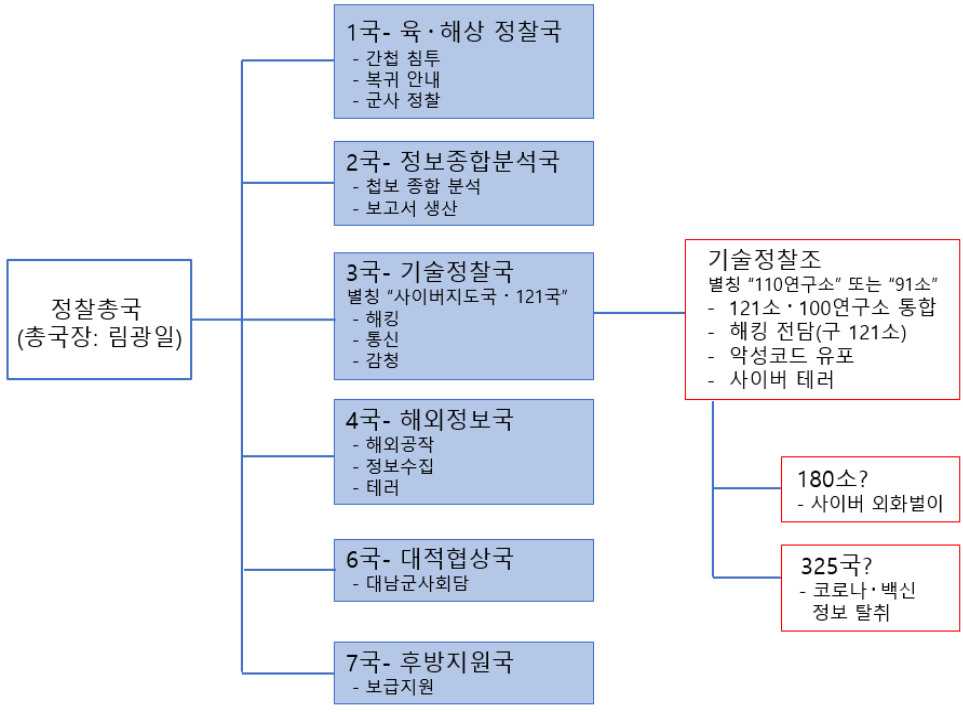
---

1) https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons- program-u-n-report-idUSKCN1UV1ZX
2) https://www.seoul.co.kr/news/newsView.php?id=20130411008007
3) https://www.yna.co.kr/view/AKR20090710197700043

이후 2009년 2월에 인민무력부 정찰국이 조선노동당 작전부, 조선노동당 대외정보조사부(일명 '35호실')와 통합되며 정찰총국이 출범하면서 노동당 작전부는 1국, 대외정보조사는 4국 그리고 110호 연구소/기술정찰국은 정찰총국 3국으로 각각 편입되게 된다. 〈표 1〉은 북한의 사이버 활동을 총괄하는 정찰총국의 현 조직도이다.[4] 2012년과 2017년에 보도된 북한의 전략사이버사령부와 사이버전략사령부는 아직까지 실체가 밝혀지지 않고 있다는 점에서 실제로는 존재하지 않을 가능성이 높다. 국군의 사이버작전사령부는 해킹을 전담하는 정찰총국 인원을 1,700명, 외곽 지원 인원을 5,100여 명으로 추정하였다.[5]

보통 3국 기술정찰국이 주도하는 것으로 알려진 사이버 활동은 기술정찰국 산하 기술정찰조가 담당한다. 별칭으로 '110연구소'라고 불리는 기술정찰조는 해킹을 담당했던 '121소'와

[그림 1] 정찰총국 조직도



자료: 김일기·김호흥(2020) 및 언론보도를 바탕으로 저자 작성.

4) 하지만 정찰총국의 실제 구성은 확실치 않다. 일부 연구와 언론 보도는 정찰총국이 1국 작전국, 2국 정찰국, 3국 해외정보국, 5국 대화조정국, 6국 기술국 또는 기술정찰국으로 구성되었다고 본다. 본 연구는 2019년 미 법무부 공소장과 2020년 국가안보전략연구원에서 발간한 북한 정보기구 관련 보고서에 기초하여 정찰총국 3국을 해킹을 전담하는 기술정찰국으로 지칭한다.

5) https://www.donga.com/news/Politics/article/all/20181122/92972617/1

‘100연구소’가 통합된 부서로서, 2009년 7.7 DDoS 사태의 배후로 지목되었다. 또한 북한의 해킹 그룹으로 알려진 라자루스(Lazarus)・안다리엘(Andariel)・김수키(Kimsuky)・블루노로프(Bluenoroff) 등이 기술정찰조에 속해 있는 것으로 여겨진다. 3국의 별칭 중 하나가 ‘121국’이라는 점은 이 부서가 북한 첫 사이버 부대였던 ‘121소’ 중심으로 만들어졌음을 시사한다.

비교적 조직 변화가 없는 정찰총국의 타 부서들과는 달리 3국/기술정찰국은 지속적으로 확대 개편되는 것으로 보인다. 북한의 사이버 활동이 증가하고 기술 능력이 고도화되면서 기술정찰국 산하 부대들 또한 세분화되고 있는 것으로 추정된다. 당장 사이버 금융범죄를 통한 외화벌이에 특화된 ‘180소’[6] 및 코로나19 관련된 정보와 백신 기술을 탈취하는 것이 목표인 ‘325국’이 창설되었다는 보도[7]는 북한 정권이 당면한 제재와 코로나19의 대유행이라는 위기를 타파하기 위해 사이버 전력에 크게 의존하고 있음을 시사한다.

2. 북한의 해킹 집단

북한의 해킹 집단으로 흔히 라자루스, 안다리엘, 블루노로프, 김수키 등이 언급된다. 하지만 이들은 사이버 보안업체들이 임의로 정한 명칭[8]들이며, 모두 정찰총국 소속일 것으로 추정되지만 당연히 정찰총국이 사용하는 정식명칭이 아니다. 북한 해킹 집단의 명칭들이 다양한 이유는 사이버 보안업체들과 연구자들이 각자 명명법에 따라 명칭을 정하기 때문이다. 예를 들어 미 정부 사이버 및 인프라 보안국(CISA)은 소니 픽처스를 공격한 라자루스(Lazarus)[9]를 히든 코브라(Hidden Cobra)라고 부른다.[10] 다른 예로는 저명한 사이버 보안업체인 Mandiant가 식별한 북한의 해킹 집단인 APT37와 APT38에 대해 기타 보안업체 및 기관들은 각각을 리퍼 (Reaper)와 블루노로프(Bluenoroff)라는 다른 명칭을 부여한 것이 있다.

더 자세한 분류법은 이들이 사용하는 기법, 전술 및 절차(Techniques, Tactics, and Procedures: TTP)에 기반한다. TTP는 각 해킹 집단이 선호하는 악성코드 등 해킹 도구와 가짜 이메일 사용 같은 침투전략을 종합한 것으로, 한 해킹 집단만의 노하우가 고스란히 녹아 있어 조사자 입장에서는 지문과 같은 식별력을 가지게 된다. 물론 타 해킹 집단의 TTP를 모방하여 자신의 정체를 감추는 것도 가능하다. 일반적으로 TTP는 한 해킹 집단의

---

6) http://news.kmib.co.kr/article/view.asp?arcid=0923850772
7) 『데일리NK』, 「코로나 정보 전문 탈취 정찰총국 325국, 김정은 직접 챙긴다.」, 2021. 2. 4.
8) 예를 들어 김수키(Kimsuky)의 경우 2013년 피싱 공격에 사용된 이메일 주소가 ‘kimsukyang’이라는 이름으로 등록되었던 점에 착안해 명칭이 정해졌다.
9) 러시아 사이버 보안업체인 카퍼스키(Kapersky)가 지정한 명칭이다.
10) https://us-cert.cisa.gov/ncas/alerts/TA17-164A

기술 수준과 위험성을 추정하고 해킹 피해 발생 시 공격자를 특정하는 데 도움을 준다.

사이버 보안 전문가들은 이러한 TTP 정보를 기반으로 북한의 해킹 집단을 '지능적・지속적 위협', 즉 APT(Advanced Persistent Threat)인 것으로 판단한다. APT는 영리목적을 띠는 개인이나 범죄집단의 공격과는 달리 정보 취득 및 유무형의 자산 파괴가 목적인 경우가 많다(Verizon, 2020). 또한 APT는 보안이 허술한 개인이나 일반기업들보다는 탄탄한 보안을 갖춘 공공・금융 기관과 방산 및 하이테크 기업들을 공격한다는 특징을 가진다. 그만큼 공략하는데 많은 시간과 노력 그리고 고도의 기술을 요하기 때문에 시간과 효율을 중요시하는 일반 범죄형 해킹과는 다른 공격패턴을 보인다. 북한의 한수원・방글라데시 중앙은행・소니 픽쳐스 해킹 사례들은 짧게는 수개월에서 길게는 일년 넘게 사전 작업이 있었고 고도의 해킹 능력을 보여 주었다는 점에서 APT 공격 범주에 들어간다.

〈표 1〉 북한의 해킹집단

해킹 집단	공격 대상	목적	기타 명칭
라자루스 (Lazarus)	- 전 세계 금융기관 - 공공기관, 군, 기업	정보 탈취 범죄수익 사이버 테러	히든 코브라x(Hidden Cobra) - 안다리엘* (Andariel)
APT37	- 한국+ - 공공기관 및 개인	정보 탈취	리퍼(Reaper) 스카크러프트(Scarcruft)
APT38	- 전 세계 금융기관 - 카지노	범죄수익	블루노로프(Bluenoroff) 템프 허밋(TEMP.Hermit) 비글보이즈x(BeagleBoyz)
김수키 (Kimsuky)	- 한국+ - 공공기관 및 개인 (한국수력원자력 등)	정보 탈취 사이버 테러	벨벳 천리마(Velvet Chollima) 탈륨(Thallium)

주: 1) + 한국 및 미국, 일본, 중국 등 주요 국가
2) x 미 정부가 사용하는 명칭
3) * 라자루스 하위그룹
자료: MITRE ATT@CK DB와 언론보도를 바탕으로 저자 작성.

북한의 해킹 집단은 공격 대상과 목적에 따라 분류할 수 있다(표 1). 라자루스와 APT38이 사이버범죄 수익에 집중한다면 APT37과 김수키는 정보 탈취에 특화된 전형적인 국가 지원 APT 행태를 보인다. APT37과 김수키는 주로 한국, 일본, 미국 등 주요 국가들의 공공기관, 군 및 방산업체와 개인들을 표적으로 삼고 정보 탈취에 방점을 둔다. 반대로 라자루스와 APT38은 IT 보안이 상대적으로 취약한 중남미, 아프리카, 서남아시아로까지 활동 영역을 넓히고 있다.

북한을 대표하는 APT라고 할 수 있는 라자루스는 초창기에는 정보 탈취・사이버 테러에

중점을 두었으나 현재는 금융기관과 암호화폐 거래소 등을 공략해 범죄수익을 올리는 사이버 범죄 집단으로 변화하였다. 라자루스의 변화는 국가가 지원하는 APT 해킹 집단이 고도화된 기술과 전술을 금융범죄 목적에 활용할 경우 엄청난 경제적 피해를 줄 수 있다는 것을 잘 보여 준다. 금융범죄를 목적으로 하는 국가 차원의 해킹 집단은 북한의 라자루스와 APT 38 둘뿐인 것으로 사료된다.

Ⅲ. 북한의 사이버 금융범죄 유형

북한의 사이버 금융범죄는 크게 1) 은행 내부의 SWIFT 및 ATM 단말 해킹을 통한 불법 인출, 2) 랜섬웨어를 활용한 '몸값' 갈취, 3) 암호화폐 탈취 등 3개 유형으로 나눌 수 있다. 특히 북한은 암호화폐를 단순히 수익을 위해 노리는 것을 넘어 암호화폐의 돈세탁 용이성을 활용해 랜섬웨어 같은 다른 사이버 금융범죄에도 활용하는 행태를 보인다. 북한의 금융범죄를 담당하는 해킹 집단으로는 라자루스와 APT38이 언급되며, 피해 사례를 들여다 보았을 때 이 두 집단의 TTP가 상당 부분 겹친다는 점을 근거로 미 정부는 금융기관을 공격하는 북한의 해킹 집단을 지칭할 때 비글보이즈(BeagleBoyz)라는 단일 명칭을 사용한다.

1) SWIFT 및 ATM망 해킹을 통한 불법인출

북한은 은행 간 송금을 위한 국제 통신망인 SWIFT(Society of Worldwide Interbank Financial Telecommunication)망과 현금 자동 입출금기(Automated Teller Machine: ATM) 망에 연결되는 은행 내부 단말기를 해킹하는 수법으로 상당한 수익을 올린 것으로 추정된다. 북한은 내부 관리자급으로 추정되는 직원들의 메일 계정으로 악성코드가 담긴 피싱 이메일을 보내 SWIFT와 ATM망 계좌와 연결되는 내부 컴퓨터를 장악하는 수법을 주로 사용한다. 즉, 북한 해커들은 SWIFT망을 해킹하는 것이 아니라 은행 내부의 SWIFT망 단말기를 해킹하는 것이다. ATM망 또한 유사한 방식으로 해킹한다.

북한 해커들의 SWIFT와 ATM 단말 해킹을 통한 불법인출 시도들은 미 법무부가 라자루스 소속 해커인 전창혁, 김일, 박진혁을 기소한 공소장에 자세히 나와 있다.[11] 2015년 이후부터 북한 해커들이 2016년 방글라데시 중앙은행에서 9억 5,100만달러를 불법 인출하려다 8,100만

11) https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

달러를 빼돌리는 데 성공한 사례가 가장 잘 알려져 있다. 하지만 이외에도 북한의 해커들은 2015년 베트남과 필리핀 현지 은행들을 공격하여 베트남 티엔퐁(TienPhong) 상업은행에서 약 미화 700만달러가량을 탈취하였다. 이후 북한은 2016년 아프리카 지역 은행에서 1억 4백만달러를 탈취하였고, 2017년에는 대만의 원동국제상업은행(Far Eastern International Bank)에서 6천만달러, 2018년에는 멕시코 방코멕스트(Bancomext)에서 1억1,000만달러를 탈취하였다. 방코멕스트의 경우 도난당한 돈이 한국으로 송금되어 논란이 되기도 하였다.[12] 가장 최근 알려진 북한의 불법 인출 사례는 2019년 말타의 뱅크 오브 발레타(Bank of Valleta)가 약 1,300만유로를 도난당한 것이다.

미 법무부 기소장에 포함된 사례들 외에도 2015년 에콰도르의 방코 델 아우스트로(Banco del Austro) 은행이 입은 1,200만달러[13] 불법 인출 피해, 2017년에 있었던 인도의 유니언 뱅크 오브 인디아(Union Bank of India)의 1억 7,100만달러 불법 인출 시도, 2018년 칠레의 방코 데 칠레(Banco de Chile)에서 1천만달러가 불법 인출된 사건도 북한이 배후인 것으로 의심되는 해킹 사례들이다.

ATM망 해킹의 경우 자동현금입출금기의 현금 인출 한도 때문에 상대적으로 소액을 여러 번 인출해야 한다는 한계가 있다. 북한은 현지 범죄 조직과 곁탁하여 이 문제를 해결한 것으로 보인다. 북한은 2018년 파키스탄의 뱅크이슬라미(BankIslami)를 해킹해 ATM망을 통해 약 6천만달러를 탈취하였다. 북한은 또한 같은 해 인도의 코스모스 은행(Cosmos Bank)의 SWIFT망과 ATM망이 각각 겪은 1,150만달러와 200만달러 도난 사건의 배후로도 지목되었다.[14] 코스모스 은행의 경우 5시간 동안 28개 국가에 있는 14,000여 개의 ATM 기기에서 현금이 인출되었다.

미 정부는 북한이 2015년부터 2020년까지 최소 30여 개국 금융기관의 SWIFT망과 ATM망 해킹을 통해 약 20억달러가량을 탈취하려 했다고 추정하였다.[15] 그러나 이 중 상당액은 북한의 손에 완전히 들어가기 전에 각국의 금융 당국에 의해 차단된 것으로 보인다. 대표적으로 방코멕스트의 경우 전액이 한국 등 각국 금융 당국에 의해 회수되었으며, 유니언 뱅크 오브 인디아의 경우도 불법 인출이 발생한 지 3일 내로 피해액 전액을 회수하는 데 성공하였다.[16] 발레타 은행의 경우에도 피해금액 중 일부만 회수가 되지 않은 것으로 보고되었다.

북한이 SWIFT망 해킹을 통해 불법 인출하려 시도한 총액은 크지만, 실제로는 상당 부분이

12) https://www.chosun.com/international/us/2021/02/19/LAVTQSFQWZAM5BZMNM47VJT2DE/
13) http://www.inews24.com/view/1129745
14) https://www.zdnet.com/article/how-hackers-managed-to-steal-13-5-million-in-cosmos-bank-heist/
15) https://www.cisa.gov/news/2020/08/26/cisa-treasury-fbi-and-uscybercom-release-cyber-alert-latest-north-korea-bank
16) https://www.livemint.com/Industry/xuBJNapRGBrtl05iEAvsYO/How-Union-Bank-was-hacked-and-got-its-money-back.html

바로 회수되었다. ATM망 해킹의 경우 현지 범죄조직과 수익을 나눠야 한다는 점과 현금 인출이 가진 물리적 한계 때문에 북한에 아주 매력적이지는 않을 것으로 보인다. 최근 북한의 해킹 집단이 국가 간 이전이 쉽고 돈세탁이 용이한 암호화폐에 관심을 갖게 된 계기에는 은행망 해킹을 통한 불법인출 성공률이 상대적으로 낮은 점도 작용할 것으로 사료된다.

2) 랜섬웨어 '워너크라이 (WannaCry)'

2017년 5월 라자루스는 미국 국방안보국(NSA)에서 유출된 EternalBlue라는 해킹툴을 이용하는 워너크라이 랜섬웨어를 제조・배포하였다. 랜섬웨어(ransomware)는 감염된 컴퓨터의 데이터를 암호화하여 피해자가 '몸값'을 지불해야지만 해독을 해주는 유형의 악성코드이다. 워너크라이의 첫 피해자는 영국의 국가의료서비스(National Health Service)로, 약 19,000건의 진료 예약이 취소되고 약 1주일간 진료시스템이 오작동하는 피해를 입었다.[17] 워너크라이는 최종적으로 150여 개국 230,000여 대의 컴퓨터를 감염시켜 40억달러의 재산 피해를 낸 것으로 추정된다.[18]

하지만 라자루스가 랜섬웨어를 통해 노린 것은 핵심인프라 마비가 아니라 범죄 수익이었다. 3명의 북한 해커들에 대한 미 법무부 공소장에 따르면 라자루스는 중미의 온라인 카지노 두 곳에서 각각 데이터 해독 몸값으로 230만달러와 36만달러 상당의 암호화폐를 받았다. 북한의 해킹 집단이 개인 피해자들에게는 데이터 해독을 위해 300~700달러 사이의 몸값을 요구했다는 점을 감안할 때 개인들에게서도 상당한 수익을 올렸을 것으로 추정된다.

3) 암호화폐 탈취

금융자산으로서 암호화폐가 각광을 받게 되면서 북한의 해킹 집단은 암호화폐로 눈길을 돌리게 된다. 북한의 해커들은 은행 내부망을 해킹하는 것과 동일한 방식, 즉 악성코드를 담은 이메일을 내부 직원이 열어 보도록 유도하여 내부망을 장악한 후 거래소의 암호화폐를 빼돌리는 방식으로 암호화폐 거래소를 공격하고 있다. 미 법무부 공소장에 따르면 북한의 해커들은 암호화폐 거래 프로그램을 가장한 악성코드도 살포하고 있다.

암호화폐 관련 악성코드 살포 외에도 북한은 2017년 슬로베니아의 한 거래소에서 7,500만달

17) https://www.nationalhealthexecutive.com/News/wannacry-cyber-attack-cost-the-nhs-92m-after-19000-appointments-were-cancelled
18) https://symantec-enterprise-blogs.security.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later

러 상당의 암호화폐를 탈취한 것을 시작으로 2018년 인도네시아의 한 거래소에서 2,500만달러, 2020년에는 뉴욕의 한 금융기관에서 1,200만달러 상당의 암호화폐를 훔쳤다.

이 외에도 유엔 대북제재위원회 전문가패널의 2019년 보고서에 따르면 북한은 2019년 한국의 암호화폐 거래소인 업비트를 공격해 암호화폐의 일종인 이더리움(Ethereum)을 570억 원가량 탈취하였다. 빗썸은 2017년에 있었던 두 번의 공격에서 각각 7백만달러, 2018년과 2019년에 각각 3,100만달러 및 2,000만달러 상당의 암호화폐를 도난당했다.[19] 유빗(Youbit)의 경우 북한 해커들에게 170여억원 상당의 암호화폐를 도난당한 후 2017년 파산하였다. 가장 최근에는 2020년 라자루스가 KuCoin 암호화폐 거래소에서 2억5,000천만달러 상당의 암호화폐를 훔친 것으로 보고되었다.[20]

암호화폐 분석업체인 체인널리시스(Chainalysis)의 추정에 따르면 북한 해커들이 2017~20년 사이에 훔친 암호화폐의 총액은 17억 5,000만달러에 육박하며,[21] 이는 북한이 불법 인출을 시도한 액수인 20억달러와 맞먹는다. 그러나 은행 내부망의 SWIFT 단말 해킹과는 달리 북한이 훔친 대부분의 암호화폐는 회수가 되지 않고 있다.

Ⅳ. 평가 및 전망: 암호화폐와 북한의 사이버 금융범죄

북한에 있어 암호화폐는 사이버 금융범죄의 성공률을 높이는 매우 유용한 수단이다. 강력한 대북제재 아래 놓여 있는 북한이 암호화폐를 선호하는 배경에는 암호화폐가 주는 돈세탁의 용이함과 여기서 파생되는 제재 우회 효과가 있다. 불법 인출의 경우, 실제 훔친 자금을 인출하는데는 상당한 시간이 소요되며 실제 현금으로 인출되기 전까지는 추적도 용이하다. 이는 불법 인출된 자금의 상당 부분이 회수되는 것에서도 알 수 있다. 이와는 달리 탈중앙화를 추구하는 암호화폐는 중앙관리자가 없으므로 거래자의 익명성이 보장된다. 이는 해킹을 통해 암호화폐를 탈취했을 때에도 똑같이 유효하여 랜섬웨어 등 각종 사이버 금융범죄를 용이케 하는 측면이 있다.

주력 암호화폐인 비트코인의 경우 거래장부인 블록체인(Blockchain)이 공개되어 있어 암호화폐의 이동 경로를 쉽게 파악할 수 있을 것으로 흔히들 생각한다. 하지만 실제로는 암호화폐의 이동 경로를 감출 수 있는 방법들이 존재한다. 대표적으로는 '믹서(Mixer)',

19) https://www.joongang.co.kr/article/23551061#home
20) https://www.technologyreview.com/2020/09/10/1008282/north-korea-hackers-money-laundering-cryptocurrency-bitcoin/
21) https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack

즉 비트코인을 쪼개어 다수의 다른 출처의 비트코인과 섞는 방식으로 훔친 비트코인의 출처를 감추는 것이다. 여기에 최종적으로 거래장부를 공개하지 않는 '알트코인(Altcoin)', 즉 비트코인을 대체하는 암호화폐들로 교환하는 방식으로 자금 추적을 회피하는 방법도 있다. 여기에 동원되는 암호화폐로는 모네로(Monero)와 지캐시(ZCash)가 있다.

북한 해커들이 당면한 최종 문제는 훔친 암호화폐의 현금화이다. 2020년 미 국무부는 북한 해커들이 탈취한 암호화폐로 애플(Apple)사의 아이튠스(iTunes) 상품권을 구매하는 방식으로 1억달러 상당의 암호화폐를 현금화해 준 중국의 암호화폐 브로커 2명을 기소하기도 하였다.[22] 북한 당국의 딜레마는 대량의 암호화폐를 현금화하려면 거래소를 반드시 거쳐야 한다는 점이다. 현재 암호화폐를 현금화할 수 있는 거래소는 전 세계 500여 개 정도로 알려져 있으나[23] 이 중에서 충분한 유동성을 갖춘 곳은 많지 않은데에다 주요 국가들은 암호화폐 거래소에 대한 자금세탁방지(AML) 규제를 강화하였다. 특히 고객확인제도(Know Your Customer: KYC) 규정이 강화되면서 거래소를 통한 암호화폐 거래의 익명성은 더 이상 보장받지 못하는 상황이다. 만약 북한이 당장 암호화폐를 현금화한다면 소량만 가능할 것이다. 당장 시급한 외화 확보 측면에서 암호화폐는 크게 도움이 되지 않는다.

그러나 북한 해커들이 암호화폐 거래소들을 본격적으로 해킹하기 시작한 2017년도부터 지금까지 비트코인 가격은 60배 이상 상승하였다는 점을 감안하면 북한은 탈취한 암호화폐를 장기투자의 관점에서 바라보는지도 모른다. 북한에게 암호화폐는 제재 회피 용도뿐만 아니라 강력한 경제제재 아래서 획득 가능한 유일한 금융자산이 된 셈이다.

---

22) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack
23) https://www.cryptimi.com/guides/how-many-cryptocurrency-exchanges-are-there

참고문헌

『국민일보』, 「"北, 사이버전략사령부 창설 추진" 김흥광 NK지식인연대 대표 주장」, 2017. 11. 16.

『동아닷컴』, 「北, 판문점선언 이후에도 사이버 공격… '모든 공간서 적대행위 중지' 합의 어겨」, 2018. 11. 22.

『서울신문』, 「['3・20 사이버테러' 북한 소행] 대남공작・사이버전 총괄 핵심기구… 정예 해커만 3000여명 보유 추정」, 2013. 4. 11.

『아이뉴스』, 「세계 금융기관 노린 APT38, 배후에는 北 정권」, 2018. 10. 4.

『연합뉴스』, 「北사이버전 전담부대 '110호연구소'는」, 2009. 7. 10.

『조선일보』, 「멕시코서 1200억 턴 北해커, 한국 계좌로 송금...누구에게?」, 2021. 2. 19.

『중앙일보』, 「"한국만 北에 암호화폐 10번 털렸다…빗썸 6500만 달러 피해"」, 2019. 8. 13.

BROADCOM, "WannaCry: Lessons Learned 1 Year Later," 16 May 2018.

CRYPTIMI, "How Many Cryptocurrency Exchanges are there?," 27 June 2021.

MINT, "How Union Bank was hacked and got its money back," 18 April 2017.

MIT Technology Review, 「North Korean hackers steal billions in cryptocurrency. How do they turn it into real cash?」, 2020. 9. 10.

National Health Executive, "WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled," 12 October 2018.

Reuters, "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report," 6 August, 2019.

United Nations, 「Report of the Panel of Experts established pursuant to resolution 1874(2009)」, S/2019/691. 2019.

Verizon, 「Data Breach Investigations Report」, 2020.

ZD Net, "How hackers managed to steal $13.5 million in Cosmos bank heist," 27 August 2018.

〈웹사이트〉

Cybersecurity & Infrastructure security agency, HIDDEN COBRA – North Korea's

DDoS Botnet Infrastructure, https://us-cert.cisa.gov/ncas/alerts/TA17-164A, 접속일: 2021. 10. 26.

Insights, Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack, 접속일: 2021. 10. 26.

The United States Department of Justice, Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack, 접속일: 2021. 10. 26.

The United States Department of Justice, Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and, 접속일: 2021. 10. 26.