북한 사이버 위협 주의보

발행: **2020 년 4 월 15 일**

제목: **북한 사이버 위협에 대한 지침**

국무부, 재무부, 국토안보부 그리고 연방수사국은 국제 사회와 네트워크 보호자와 대중을 위해 북한의 사이버 위협에 대한 종합적인 자료로 이 주의보를 발행합니다. 이 주의보는 공식적으로 조선민주주의인민공화국이라고 알려진 북한이 제기하는 사이버 위협을 강조하고 그 위협을 완화하는 단계를 권장합니다. 구체적으로 부록 1을 보면 북한 사이버 위협에 관련된 미국 정부의 자원 목록이 나와 있으며 부록 2에는 유엔 안전보장이사회 1718 (대북)제재위원화 전문가 패널 보고서에 대한 링크가 들어 있습니다.

북한의 악의적인 사이버 활동은 미국과 더 넓은 국제사회를 위협하며 특히 국제 재정 체계의 온전성과 안정성에 심각하게 위협하고 있습니다. 미국과 UN의 강력한 제재 압력으로 대량 학살 무기와 탄도 미사일 프로그램에 대한 자금을 만들기 위해 북한은 사이버 범죄를 포함한 불법 행위에 점점 의존해 왔습니다. 특히 미국 정부가 "히든 코브라"(HIDDEN COBRA)라고 지칭하는 북한의 악의적인 사이버 활동에 대해 미국은 상당히 우려하고 있습니다. 북한은 미국 핵심 사회기반시설을 방해하거나 파괴하는 사이버 활동을 할 수 있는 능력을 갖추고 있습니다. 또한, 북한은 사이버 능력을 이용해 금융 기관을 대상으로 절도 행위를 해왔으며, 사이버 공간에서 책임 있는 국가 행위가 무엇인가에 대해 국제 사회가 점점 동의하는 바와 전혀 일치하지 않는 방해적 파괴적 사이버 활동 양식을 보여왔습니다.

미국은 비슷한 생각을 하는 국가와 긴밀히 협조해 사이버 공간에서 북한이 하는 방해 및 파괴 행위 혹은 다른 식으로 안정을 무너뜨리는 행위에 집중하고 그것을 규탄하고자 합니다. 예를 들어, 2017년 12월 호주, 캐나다, 뉴질랜드, 미국 그리고 영국은 "워너크라이 2.0"(WannaCry 2.0) 랜섬웨어 공격이 북한의 행위로 공식 발표했으며, 북한의 해롭고 무책임한 사이버 활동을 규탄했습니다. 덴마크와 일본은 2017년 5월 전 세계 수십 만 대의 컴퓨터에 피해를 준 "워너크라이 2.0" 랜섬웨어 공격을 공동 규탄하는 지지 성명을 발표했습니다.

국제 사회와 네트워크 보호자 그리고 대중이 경계를 늦추지 않고 협력해 북한이 제기하는 사이버 위협을 완화하는 것이 중요합니다.

금융 부문을 겨냥한 북한의 악의적인 사이버 활동

많은 북한의 사이버 행위자는 정찰총국과 같은 유엔과 미국이 지정한 기관에 속해 있습니다. 북한 정부의 지원을 받는 사이버 행위자는 주로 첩보 활동, 금융 기관과 디지털 화폐를 겨냥한 사이버 기반 절도 그리고 외국 언론사에 반하는 정치적 동기를 가지고 활동을 하는 해커, 암호학자 그리고 소프트웨어 개발자입니다. 이들은 이런 활동을 가능케 하는 폭넓은 악성 프로그램 도구를 전세계에 개발·보급하며 그 활동이 점점 정교해지고 있습니다. 북한이 지원하는 사이버 행위자가 불법 수익을 올리기 위해 흔히 쓰는 수법에는 다음과 같은 것에 국한되지 않지만 이것을 포함합니다.

사이버 기반 금융 절도 및 돈 세탁. 유엔 안보리 1718 위원회 전문가 패널의 2019년 중간 보도(2019 전문가 패널 중간 보고서)에 따르면 국제연합 안보리의 제재에도 불구하고 악의적인 사이버 활동을 통해 점점 정교한 도구와 수법으로 금융 기관을 대상으로 절도를 해 수익을 올리는 북한의 능력이 향상되고 있습니다. 어떤 경우에는 이런 악의적인 사이버 활동이 여러 관할지에 걸쳐 자금을 세탁하는 데까지 이르렀다고 2019 전문가 패널 중간 보고서는 지적하고 있습니다. 2019 전문가 패널 중간 보고서는 북한에 의한 사이버 기반 강도로 의심되는 수십 건의 사건을 조사 중이며, 2019년 후반 현재 북한이 이런 불법 사이버 활동을 통해 20억 달러나 되는 돈을 훔치려고

시도했다고 언급하고 있습니다. 2020년 3월 사법부 몰수 소장에 제기된 혐의가 전문가 패널의 일부 조사 결과와 일치합니다. 몰수 소장은 어떻게 북한의 사이버 행위자가 디지털 화폐 거래소를 해킹한 뒤 수억 달러에 해당하는 디지털 화폐를 훔쳤으며 자금 세탁을 위한 음모를 진척시키기 위해 북한의 사회기반시설을 이용했는지 기술하고 있습니다.

강요 작전. 북한 사이버 행위자는 또한 조직의 네트워크를 약화하고 조직이 몸값을 지불하지 않으면 폐쇄하겠다고 위협하는 식으로 제 삼국 조직에 대해 강요 작전을 써왔습니다. 어떤 경우 북한 사이버 행위자는 거짓으로 그런 악의적인 사이버 활동이 미래에 발생하는 것을 막기 위한 장기 유료 자문 서비스를 제공한다며 피해자에게 돈을 요구했습니다. 또한, 북한 사이버 행위자는 제삼자 의뢰인을 위해 돈을 받고 웹사이트를 해킹하고 해킹 대상자로부터 돈을 강요했습니다.

크립토재킹. 2019 전문가 패널 중간 보고서는 또한 북한이 피해자의 기기를 약화하고 디지털 화폐를 채굴하는 컴퓨팅 리소스를 훔쳐 가는 계략인 "크립토재킹"을 사용하는 것에 대해 전문가 패널이 수사를 하고 있다고 밝혔습니다. 전문가 패널은 크립토재킹 악성 프로그램에 감염된 컴퓨터가 채굴된 자산-대부분이 익명성이 강화된 디지털 화폐(때로는 "프라이버시 코인"이라고도 불림)-을 평양의 김일성 대학을 포함해 북한 소재 서버에 보낸 사례 몇 건을 발견했습니다.

이런 활동은 제재 영향을 완화하면서 수익을 창출하기 위해 북한이 사이버 기반 수단을 이용하고 있으며 어느 나라나 북한에 노출되어 이용당할 수 있다는 사실을 분명히 보여줍니다. 2019 전문가 패널 중간 보고서에 따르면, 전문가 패널은 또한 유엔 안보리의 대북 제재에 대한 위반 시도 같은 행위를 조사하고 있습니다.

미국 정부, 사이버 운영이 북한의 행위라고 공식 발표

북한은 데이터를 훔치고, 파괴적이면서 방해를 주는 사이버 활동을 하기 위해 미국과 다른 정부 및 군사망 그리고 민간 조직과 중요한 사회기반시설에 관련된 네트워크를

계속 겨냥해 왔습니다. 지금까지 미국 정부는 아래의 사이버 사고가 북한 정부의 지원을 받는 사이버 행위자와 그 공모자에 의한 것으로 공식적으로 밝혔습니다.

- ***소니 영화사***. 2014년 11월 북한 정부의 지원을 받는 사이버 행위자가 2014년 영화 "인터뷰"에 대한 보복으로 소니 픽처스 엔터테인먼트(SPE)에 사이버 공격을 가한 것으로 보입니다. 북한 사이버 행위자는 기밀 데이터를 훔치기 위해 SPE 네트워크를 해킹했고 SPE 임직원을 위협했으며 수천 대의 컴퓨터를 손상했습니다.

    - 소니 사건 조사에 대한 FBI의 최신 자료(2014년 12월 19일) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - 북한 정권의 지지를 받는 프로그래머에 대한 사법부의 형사 소장(2018년 9월 6일) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***방글라데시 은행 강도 사건***. 2016년 2월 북한의 지원을 받은 사이버 행위자는 전 세계 금융 기관에서 10억 달러를 훔치려고 시도한 혐의와 국제 은행 간 통신 협회(SWIFT) 네트워크 상에서 무허가 거래를 통해 방글라데시 은행으로부터 8천백만 달러를 훔친 혐의를 받고 있습니다. 그 소장에 따르면 북한의 사이버 행위자는 은행 직원을 대상으로 한 스피어 피싱 이메일을 이용해 컴퓨터 네트워크에 침입한 후 SWIFT 네트워크와 연결된 방글라데시 은행의 컴퓨터 단말기에 접속했습니다. 그리고서 북한의 사이버 행위자는 방글라데시 은행에서 자금을 인출해 음모자가 통제하는 계정으로 이체하라는 내용을 거짓 인증된 SWIFT 메시지로 보냈습니다.

    - 북한 정권의 지원을 받는 프로그래머에 대한 사법부의 형사 소장(2018년 9월 6일) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***워너크라이 2.0***. 북한이 지원하는 사이버 행위자가 워너크라이 2.0이라고 알려진 랜섬웨어와 함께 그 랜섬웨어의 이전 버전 두 개를 개발했습니다. 2017년 5월 워너크라이 2.0 랜섬웨어가 150개국이 넘는 나라의 병원, 학교, 사업체 그리고 가정에 있는 수십만 대의 컴퓨터를 감염시켰습니다. 워너크라이 2.0 랜섬웨어는 감염된 컴퓨터의 데이터를 암호화해서 사이버 행위자가 비트코인 디지털 화폐로 몸값의 지급을 요구할 수 있게 합니다. 재무부는 워너크라이 2.0 음모에 참여하고 소니 영화사 사이버 공격 그리고 방글라데시 은행 강도 사건에 역할을 한 이유로 북한 컴퓨터 프로그래머 한 사람을 지명했으며, 그가 일한 조직도 추가로 지명했습니다.

    - CISA의 기술 주의보: 워너크라이 랜섬웨어와 연관된 지표 (2017년 5월 12일) https://www.us-cert.gov/ncas/alerts/TA17-132A
    - 워너크라이 랜섬웨어에 대한 백악관의 기자단 브리핑 (2017년 12월 19일) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
    - 북한 정권을 배후에 둔 프로그래머에 대한 사법부의 형사 소장 (2018년 9월 6일) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
    - 여러 차례 사이버 공격에 대한 재무부의 대북 제재 (2018 년 9 월 6 일) https://home.treasury.gov/news/press-releases/sm473

- ***패스트캐시(FASTCash) 작전.*** 2016년 말부터 북한 정권의 지원을 받는 사이버 행위자가 아시아와 아프리카에 있는 ATM에서 수천만 달러의 돈을 훔치기 위해 "패스트캐시"라고 알려진 거짓 ATM 현금 인출 책략을 써왔습니다. 패스트캐시 책략이란 거짓 거래를 도와주는 지불 스위치 애플리케이션 서버에 원격으로 침입하는 것을 말합니다. 2017년 한 사건에서 북한의 사이버 행위자는 30국이 넘는 여러 나라에 있는 ATM에서 동시에 현금을 인출할 수 있었습니다. 2018년에 일어났던 다른 사건에서는 북한의 사이버 행위자가 23개 국에 있는 ATM에서 동시에 현금을 인출할 수 있었습니다.

- CISA의 패스트캐시 작전 주의보 (2018년 10월 2일) https://www.us-cert.gov/ncas/alerts/TA18-275A
- CISA의 악성 프로그램 분석 보고: 패스트캐시 관련 악성 프로그램 (2018년 10월 2일) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***디지털 화폐 교환 해킹.*** 2018년 4월 사법부의 대물 몰수 소장에 자세히 기술된 것처럼 북한의 지원을 받는 사이버 행위자가 디지털 화폐 거래소를 해킹해 2억 5천만 달러에 해당하는 디지털 화폐를 훔쳐 갔습니다. 그 소장에는 또한 경찰의 자산 행로 추적을 막으려는 시도로 자금의 출처를 애매하게 하려고 수백 건의 자동 디지털 화폐 거래를 통해 어떻게 훔친 자산을 세탁했는지 기술되어 있습니다. 기소장에 따르면 중국 국적의 두 사람이 북한이 관리하는 계정에서 인출된 약 9천 백만 달러와 함께 다른 거래소를 해킹해 훔친 950만 달러를 추가로 받은 뒤 북한 해커 집단을 대신해 자산을 세탁한 혐의를 받고 있습니다. 2020년 3월 재무부는 사이버 및 대북 제재 권위 아래 두 사람을 지명했는데, 이것은 그 두 사람이 돈 세탁과 무허가 자금 이체로 기소되었으며 113개의 화폐 계정을 몰수한다는 사법부의 발표와 시기를 같이 했습니다.

  - 라자루스 그룹을 위해 암호 화폐 세탁을 한 자에 대한 재무부의 제재 (2020년 3월 2일) https://home.treasury.gov/news/press-releases/sm924
  - 거래소 해킹 후 암호 화폐를 세탁한 혐의로 사법부가 기소한 두 중국인과 민사 몰수 소장 (2020년 3월 2일) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

북한의 사이버 위협 대응 조치

북한은 대량 학살 무기 프로그램을 포함해 정권이 우선시하는 임무를 하는 데 필요한 자금을 만들기 위해 전 세계에 걸쳐 사이버 기반 사회기반시설을 겨냥합니다. 정부,

기업, 시민 사회와 개인이 북한의 사이버 위협에서 자신을 보호하고 거기에 대항하기 위해 아래와 같은 관련된 모든 행동을 취할 것을 우리는 강력히 권합니다.

- **북한의 사이버 위협에 대한 인식을 높이십시오.** 북한의 악의적인 사이버 활동의 심각성, 범위 그리고 다양함을 강조하는 것이 공공 및 민간 부문 전체에서 위협에 대한 인식을 높이며 적절한 예방 및 위험 완화 조치를 채택하고 실시하는 데 도움이 됩니다.

- **북한의 사이버 위협에 대한 기술 정보를 공유하십시오.** 북한의 사이버 위협을 탐지하고 막아 내기 위한 정보를 국내 및 국제 수준에서 공유함으로써 네트워크와 시스템의 사이버 보안을 강화할 수 있습니다. 모범 사례를 정부 및 민간 부문과 공유해야 합니다. 2015 년 사이버 보안 정보 공유법 (6 U.S.C. §§ 1501–1510) 규정에 따라 비연방 단체도 히든 코브라에 관련된 사이버 위협 지표와 방어 조치를 연방 단체 및 비연방 단체와 공유할 수 있습니다.

- **사이버 보안 모범 사례 실시 및 장려**. 사이버 보안을 강화하기 위해 기술과 행동 양면에서 조치를 취하면 미국과 국제 사이버 사회기반시설이 더욱 안전하고 탄력적으로 될 것입니다. 화폐 서비스 사업자를 포함한 금융 기관은 북한의 악의적인 사이버 활동으로부터 자사를 보호하기 위한 독립된 조치를 해야 합니다. 그러한 조치는 정부 그리고/또는 기업 통로를 통한 위협 정보 공유, 위험의 최소화를 위한 네트워크 분할, 정기적 데이터 백업 사본 관리, 흔한 사회 공학 수법에 대한 의식 교육, 정보 공유와 네트워크 접속에 대한 정책 도입 그리고 사이버 사고 대응 계획을 만들기에 국한되지 않지만 그것을 포함합니다. 에너지국의 "사이버 보안 역량 성숙도 모델"과 국립표준기술연구소의 "사이버 보안 프레임워크"는 강력한 사이버 보안 사례를 개발하고 실시하는 것에 관한 지침이 됩니다. 부록 I 에 소개된 것처럼, 사이버 보안 및 사회기반시설 보안청(CISA)은 네트워크 보호자가 악의적인 사이버 활동을 파악하고 그것에 노출되는 것을 줄일 수 있도록 기술 주의보와 악성 프로그램 분석 보고를 포함한 폭넓은 자료를 제공합니다.

- **법 집행 당국에 알리십시오**. 북한에서 비롯되는 것이든 그렇지 않든 귀하 조직이 악의적인 사이버 활동의 피해자로 의심되면 적절한 시간 내에 법 집행 당국에 알리는 것이 중요합니다. 이것은 신속한 조사를 하게 할 뿐만 아니라 금융 범죄 사건이 발생했을 때 도난당한 자산을 되찾을 수 있는 확률을 높입니다.

  미국 법 집행 당국은 북한이 사이버 행위로 훔친 수백만 달러 가치의 디지털 화폐를 압수했습니다. 화폐 서비스 사업자를 포함해 모든 유형의 금융 기관은 전방에서는 이런 사이버 위협에 대한 미국 법 집행 당국의 정보 요청에 응하고, 후방에서는 미 법 집행 당국의 요청이나 미 법원 명령을 받았을 때는 몰수 가능한 자산을 파악하거나 그런 자산의 압수를 도와주는 식으로 미국 법 집행 당국에 협조해줄 것을 권합니다.

- **돈세탁 방지(AML)/테러 자금 조달 방지/확산 금융 대응(CPF) 준수 강화**. 모든 나라는 국제자금세탁방지기구(FATF)의 AML/CFT/CPF 기준을 신속하고 효과적으로 적용해야 합니다. 여기에는 금융 기관과 다른 해당 조직이 위험 FATF 기준과 FATF 공개 성명서 및 지침과 일치하는 위험 완화 조치를 반드시 실행해야 하는 것이 포함됩니다. 구체적으로 FATF 는 북한이 일으키는 계속된 돈 세탁, 테러 자금 그리고 금융 확산의 위험에서 국제 금융 기관을 보호하는 대응 조치를 할 것을 요청했습니다.[1] 그 예로 FATT 는 모든 금융 기관과 다른 해당 조직에 북한의 회사, 금융 기관 그리고 이들을 대신해서 행위를 하는 사람을 포함해 북한과의 사업 관계와 거래에 특히 주의할 것을 권고했습니다. 유엔 안보리 결의안 2270 호 본문 33 항의 내용처럼 모든 회원국은 자국 영토 내 기존 북한 은행 지점, 자회사 그리고 대표 사무실을 닫고 북한 은행과의 환거래 관계를 단절해야 합니다.

  또한, 2019 년 6 월 FATF 는 모든 국가가 디지털 화폐 거래를 할 때는 디지털 화폐 거래소를 포함한 디지털 자산 서비스 공급자를 규제 및 감독하고,

[1] *FATF 의 북한에 대한 조치 요구서 전체 내용이 여기에 나와 있습니다:* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

위험을 완화해야 하는 것으로 그 기준을 수정했습니다. 디지털 자산 서비스 공급자는 자신의 회사가 돈 세탁, 테러 자금 혹은 금융 확장을 도모하는 데 이용될 수 있으므로 고객의 활동에 변동이 있는지 항상 주의해야 합니다. 미국은 무엇보다도 거래 감시, 의심스러운 활동 보고 그리고 고객 실사가 없는 상태에서 무기명 지불이나 계정 서비스 기능을 제공하는 플랫폼에 대해 특히 우려하고 있습니다.

사업 전체나 상당 부분을 미국에서 하는 해외 소재 디지털 자산 서비스 공급자를 포함해 미국 금융 기관과 다른 해당 사업체와 개인은 "은행 기밀법"[재무부의 31 CFR 10 장 내 금융 범죄 단속 네트워크(FinCEN) 규정에 따라 도입]에 따라 반드시 규제 의무를 준수해야 합니다. 금융 기관의 입장에서 이런 의무는 화폐 서비스 사업자가 돈 세탁과 테러 활동 자금을 도모하는 데 이용되는 것을 막도록 적절하게 설계된 효과적인 돈 세탁 방지 프로그램을 개발·유지하는 것뿐만 아니라 의심되는 활동을 FinCE 에 보고하는 데 있어 디지털 자산이 연루된 사이버 사건이나 불법 자금에 의해 이루어지거나 영향을 받거나 지원을 받은 거래를 포함해 의심되는 거래를 파악하고 보고하는 것이 포함됩니다.

국제 사회의 협력. 북한의 악의적인 사이버 활동에 대응하기 위해 미국은 북한의 사이버 위협에 대한 인식을 높이기 위해 전 세계 국가와 정기적으로 교류하며 외교, 군사, 법 집행 및 사법, 네트워크 보호 그리고 다른 경로를 통해 정보과 증거를 공유합니다. 사이버 공간을 통해 자금을 훔치려는 북한의 시도를 방해하고 북한의 악의적인 사이버 활동을 막기 위해 미국 정부는 다른 나라가 해당 국제법과 일치하는 방식으로 네트워크 보호를 강화하고 제 삼국에서의 북한 합작 투자를 중단하며 외국에 있는 북한의 정보 기술(IT) 근로자를 추방할 것을 강력히 권합니다. 2017년 유엔 안보리 결의안은 IT 근로자를 포함해 외국에서 수입을 올리는 북한 국적 근로자를 2019년 12월 22일까지 본국으로 송환해야 한다고 규정하고 있습니다. 미국은 또한 외국 정부와 민간 부문이 북한의 사이버 위협을 이해하고 파악하며 방어하고 조사하며 처벌하고, 거기에 대응하는 능력을 증강하고, 사이버 공간의 안정을 확보하는 국제적인 노력에 동참하고자 합니다.

금지되거나 제재를 받을 수 있는 행동을 했을 때 따르는 결과

관련 금융 거래를 처리하는 것을 포함해 북한의 사이버 관련 활동에 참여하거나 그것을 지원하는 개인이나 조직은 금지되거나 제재를 받을 수 있는 행동을 했을 때 따르는 결과를 잘 알고 있어야 합니다.

재무부의 해외재산관리국(OFAC)은 그 무엇보다도 다음과 같은 행위를 한 것으로 생각되는 모든 사람에게 제재를 가할 수 있는 권한을 가지고 있습니다.

- 북한 정부나 조선로동당을 위해 사이버 보안을 취약하게 만드는 주요 활동에 참여
- 북한에서 정보 기술(IT) 산업에 근무
- 다른 특정 악의적인 사이버 기반 활동에 참여
- 어떤 물품이나 서비스 혹은 기술을 중요한 목적으로 북한에서 적어도 한 차례 수입하거나 북한에 수출

또한, 재무장관이 국무장관과 협의해 외국 금융 기관이 북한과 주요 거래를 알면서 했거나 그 거래를 도와주었거나 북한 관련 행정명령 혹은 행정명령 13382 호에 의해 지정된 사람(대량파괴 무기 확산자와 그 지지자)을 위해 주요 거래를 알면서 했거나 그 거래를 도와준 경우, 그 기관은 가능한 제재 중 미국에서 환거래 혹은 대리지불 계좌를 유지하는 능력을 상실할 수 있습니다.

OFAC 는 경제 제재 집행 지침, 31 C.F.R. 501 부분, 부록 A 에 요약된 것처럼 제재 규정을 위반한 것으로 보이는 경우를 조사하며 집행권을 행사합니다. 대북 제재 규정, 31 C.F.R. 501 부분을 위반하는 사람은 법에서 허용된 최고 벌금과 원래 거래액의 두 배 액수 중 더 큰 액수를 최고 벌금으로 하는 민사 벌금형을 받게 됩니다.

2019 전문가 패널 중간 보고서는 북한이 은행과 디지털 거래소에서 자금을 훔치기 위해 사이버 기반 수단을 사용하거나 사용을 시도하는 행위가 유엔 안보리 결의안(UNSCR)(즉, UNSCR 1718 본항(OP) 8(d), UNSCR 2094, 본항 8 그리고 11 그리고

UNSCR 2270, 본항 32)을 위반하는 것이 될 수 있다고 지적합니다. 북한 관련 UNSCR 은 또한 유엔이 가한 북한 관련 제재의 준수를 도와주기 위한 다양한 기제도 제공합니다. 예를 들어 유엔 안보리 1718 위원회가 유엔이 지정한 조직과 사업상 거래를 하거나 제재를 회피하는 개인이나 조직을 대상으로 제재(즉, 자산 동결 및 개인의 경우 여행 금지)를 가할 수 있습니다. .

사법부는 국제비상경제권법, 50 U.S.C. §§ 1701 이하 참조와 같은 해당 제재법을 고의로 위반한 경우 형사 처벌을 합니다. 그런 법을 고의로 위반하는 사람은 최대 20 년의 감옥형, 백만 달러와 전체 수익의 두 배 액수 중 더 많은 액수를 최고 액수로 하는 벌금형 그리고 그런 거래에 연루된 모든 자산의 몰수라는 처벌을 받을 수 있습니다. 사법부는 또한 금융 기관이 그 무엇 보다 효과적인 돈 세탁 방지 프로그램을 유지하고 FinCEN 에 일부 보고서를 제출하도록 의무화하고 있는 은행 기밀법(BSA), 31 U.S.C. §§ 5318 그리고 5322 를 고의로 위반한 경우 형사 처벌을 합니다. BSA 를 위반하는 사람은 최대 5 년의 감옥형과 최대 25 만 달러의 벌금 그리고 위반 사건에 연루된 부동산을 몰수당할 수 있습니다. 사법부는 또한 필요한 경우 이런 법규를 어기는 회사와 다른 조직을 형사 처벌합니다. 사법부는 또한 외국 정부와 양국 간 형사 수사와 처벌을 뒷받침하는 증거를 공유하기 위해 협력할 것입니다.

연방법전 타이틀 31 § 5318(k)에 따라 재무장관과 법무장관이 미국에 환거래 은행 계정을 가지고 있는 외국 금융 기관을 외국에 저장해 둔 기록을 이유로 법원에 소환할 수 있습니다. 재무장관이나 법무장관이 외국 금융 기관이 그런 소환장에 불응했다는 내용의 통지서를 미국 금융 기관에 보내는 경우, 그 미국 금융 기관은 영업 일 기준 10 일 이내에 환거래 금융 관계를 단절해야 합니다. 그렇게 하지 않으면 그 미국 금융 기관은 매일 민사 벌금형을 받을 수 있습니다.

대북 정의 보상 제도

과거나 현재 진행 중인 사이버 공간 내 북한의 불법 활동에 대해 정보를 가지고 있어 그 정보를 국무부 정의 보상 제도 프로그램을 통해 제공하는 경우, 최대 5 백만 달러의 포상금을 받을 수 있습니다. 더 상세한 내용은 www.rewardsforjustice.net 에 나와 있습니다.

부록 I : 북한의 사이버 위협에 대한 USG 정보와 대응 방안

국가 정보장실 미국 정보 공동체 연례 세계 위협 평가. 2019년 미국 정보 공동체는 북한이 금융 기관에 심각한 사이버 위협을 주며, 사이버 첩보 위협을 계속 제기하고, 방해 사이버 공격을 할 수 있는 능력을 갖추고 있다고 판단했습니다. 북한은 계속 사이버 역량을 이용해 수익을 창출하기 위한 목적으로 금융 기관으로부터 자금을 훔치고 있습니다. 평양의 사이버 범죄 활동에는 방글라데시 은행에서 8천 1백 달러로 추정되는 돈을 성공적으로 빼낸 사이버 강도 행위를 포함해 전 세계 금융 기관에서 약 11억 달러가 넘는 돈을 훔치려는 시도가 포함되어 있습니다. 그 보고서는 다음 웹사이트에서 볼 수 있습니다: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

사이버 보안 및 사회기반시설 보안청(CISA) 기술 보고서. 미국 정부는 북한의 악의적인 사이버 활동을 히든 코브라로 지칭합니다. 히든 코브라 보고는 북한의 사이버 행위자들이 사용하는 도구와 사회기반시설에 대한 기술적인 상세 내용을 제공합니다. 이 보고는 네트워크 보호자가 북한의 악의적인 사이버 활동을 파악하고 거기에 노출되는 것을 줄이도록 도와줍니다. CISA 웹사이트에 이런 지속적인 위협에 대한 최신 정보가 나와 있습니다: https://www.us-cert.gov/northkorea.

또한, CISA는 사이버 보안과 사회기반 시설에 대한 폭넓은 지식과 실무를 이해관계자에게 제공하며, 더 나은 위험 관리를 위해 그 지식을 공유하고 국가의 필수 기능을 보호하기 위해 그것을 실천합니다. CISA 자료에 대한 링크가 아래 나와 있습니다.

- 핵심 사회기반시설 보호: https://www.cisa.gov/protecting-critical-infrastructure
- 사이버 안전: https://www.cisa.gov/cyber-safety
- 탐지 및 예방: https://www.cisa.gov/detection-and-prevention
- 정보 공유: https://www.cisa.gov/information-sharing-and-awareness
- CISA 통찰력: https://www.cisa.gov/insights
- 사이버 범죄 척결: https://www.cisa.gov/combating-cyber-crime
- 사이버 보안 필수 제도: https://www.cisa.gov/cyber-essentials

- 조언: https://www.us-cert.gov/ncas/tips
- 국가 사이버 인지 시스템: https://www.us-cert.gov/ncas
- 기업 규제 체계 주의보: https://www.us-cert.gov/ics
- 사건, 피싱, 악성 프로그램 그리고 취약성 보고: https://www.us-cert.gov/report

FBI PIN 및 FLASH 보고. FBI 민간 기업 부문 통지(PIN)는 사이버 위협 가능성에 대한 민간 부문의 인식을 높이는 최신 정보를 제공합니다. FBI 연락 경고 시스템(FLASH) 보고에는 특정 민간 부문 파트너가 사용할 수 있도록 FBI가 수집한 중요 정보를 포함되어 있습니다. 이 보고는 사이버 보안 전문가와 시스템 관리자가 끈질긴 사이버 범죄자의 악의적인 행위를 막을 수 있도록 도와주는 실천가능한 정보를 수취인에게 제공하는 것이 그 목적입니다. 귀하의 회사에서 의심되는 활동을 발견하거나 관련 정보가 있으면 즉시 FBI CYWATCH에 연락하십시오. 북한 관련 사이버 위협 PIN 혹은 FLASH 보고에 대해 궁금한 점이 있으면 cywatch@fbi.gov.에 연락하십시오.

- FBI 사이버 부서: https://www.fbi.gov/investigate/cyber
- FBI 국내 지부 프로그램: FBI 국내 지부의 핵심 임무는 지정된 외국 국가에 주요 법 집행 당국과 보안청과 관계를 맺고 유지하는 것입니다. https://www.fbi.gov/contact-us/legal-attache-offices

미국 사이버 사령부 악성 프로그램 정보. 국방부의 사이버 인력은 금융 기관을 이용하고, 계속적으로 첩보 활동을 하며, 미국과 협력 국가를 대상으로 악의적인 사이버 활동을 가능케 하는 북한의 악성 프로그램을 포함해 북한의 악의적인 사이버 활동을 적극적으로 찾아내고 있습니다. 미국 사이버 사령부는 정기적으로 악성 프로그램 정보를 발표해 기업과 정부가 북한의 불법 활동으로부터 사회 기반 시설과 네트워크를 보호할 수 있도록 취약점을 찾아냅니다. 사이버 보안을 강화하는 데 필요한 악성 프로그램 정보는 다음 트위터 계정에 나와 있습니다: @US_CYBERCOM 그리고 @CNMF_VirusAlert.

미 재무부의 제재 정보 및 불법 금융 주의보. ***해외재산관리국***(OFAC)의 온라인 자료 센터는 북한과 사이버 관련 제재에 관한 제재 주의보, 관련 법규, 행정 명령, 규칙 그리고 규정을 포함해 대북 제재와 악의적인 사이버 기반 활동에 관련된 제재에 관한 상세한 정보를 제공합니다. OFAC는 또한 대북 제재, 사이버 관련 제재 그리고 디지털

화폐에 대한 몇 가지 자주 하는 질문(FAQ)을 게재했습니다. OFAC 제재 규정과 요건에 관련된 질문이나 우려되는 점이 있으면 OFAC 준수 핫라인으로 연락하십시오(전화: 1-800-540-6322, 이메일: OFAC_Feedback@treasury.gov).

- 대북 제재
    - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
    - 자주 하는 질문 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- 악의적인 사이버 활동 제재
    - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
    - 자주 하는 질문 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
    - 가상 화폐에 대해 자주 하는 질문 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

금융 범죄 단속 네트워크(FinCEN)는 북한의 국제 금융 체계 이용에 대한 주의보를 발행했습니다(https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008). FinCEN은 또한 의심 활동을 보고할 의무가 있는 금융 기관에 사이버 범죄 그리고/또는 디지털 화폐 관련 범죄 행위를 언제 그리고 어떻게 보고해야 하는지에 대한 지침을 전달했습니다.

- 사이버 범죄
    - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- 불법 디지털 화폐 활동
    - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- 회사 이메일 해킹
    - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005

- https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

연방 금융 기관 검사 협의회(FFIEC)는 금융 기관이 위험을 찾아내고 사이버 보안 대비 정도를 평가하는 데 도움이 되는 사이버 보안 평가 도구를 개발했습니다. 평가 도구는 https://www.ffiec.gov/cyberassessmenttool.htm 에 나와 있습니다.

부록 II: 북한의 사이버 위협에 대한 유엔 전문가 패널 보고서

유엔 1718 제재 위원회(DPRK) 전문가 패널 보고서. 유엔 안보리 1718 대북 제재 위원회는 유엔 회원국, 관련 유엔 단체 그리고 다른 단체로부터 유엔 안보리 대북 결의안에 요약된 조치의 시행에 대한 "정보를 수집·검사·분석하는" 전문가 패널의 지원을 받습니다. 또한, 이 패널은 1718 위원회에 중간 및 최종 보고서를 제출해 어떻게 더 제재를 잘 할 수 있는지에 대해 권고를 합니다. 이들 보고서는 https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports에 나와 있습니다.