2022 년 05 월 16 일

조선 민주주의 인민 공화국 정보 기술 근로자에 대한 지침

미국 국무부(Department of State), 미국 재무부(Department of the Treasury), 연방수사국(Federal Bureau of Investigation, FBI)은 본 권고를 발행하여 국제 사회, 민간 부문, 대중에게 북한 국적이 아닌 것처럼 가장하면서 취직하려는 조선민주주의인민공화국(DPRK, 일명 북한) 정보 기술(IT) 근로자의 시도를 경고하려고 한다. 북한 IT 근로자 관련 활동에 참여 또는 지원하거나 관련 금융 거래를 처리하는 개인 및 단체의 경우, 평판 리스크와 더불어 미국 및 국제 연합(유엔) 당국이 부과한 거래 제재를 포함한 법적 결과를 초래할 가능성이 있다.

북한은 미국과 유엔의 제재를 위반하고 대량 살상 무기(WMD) 및 탄도 미사일 프로그램에 이용할 수익을 창출하기 위해 전 세계에 고도로 숙련된 IT 근로자를 파견하고 있다. 이러한 IT 근로자는 소프트웨어 및 모바일 애플리케이션 개발 등 특정 IT 기술에 대한 기존의 수요를 활용해 북미, 유럽, 동아시아 등 전 세계의 클라이언트와 프리랜서 고용 계약을 맺는다. 북한 IT 근로자는 많은 경우 미국 기반 및/또는 북한에 거주하지 않는 재택근무자로 행세한다. 북한 IT 근로자는 북한인이 아닌 사람에게 작업 하청을 맡겨 자신의 신원 및/또는 위치를 더욱 파악하기 어렵게 만들 수 있다. 일반적으로 북한 IT 근로자는 악성 사이버 활동과 구별되는 IT 업무에 종사하지만, 북한에서 악성 사이버 침입을 수행할 수 있게 계약자로서 획득한 액세스 권한을 사용하고 있다. 이와 더불어, 해당 근로자가 강제 노동의 대상인 경우도 있을 수 있다.

본 권고에서는 북한 IT 근로자 운용 방식에 대한 상세 정보, 프리랜서 개발자를 고용하는 기업과 프리랜서 플랫폼, 지불 플랫폼에서 북한 IT 근로자를 구별할 수 있는 적신호, 북한 IT 근로자를 부주의로 고용하거나 작업이 용이하게끔 돕지 않도록 기업을 더 확실히 보호할 일반적인 완화 조치를 제공한다. 부록에서는 유엔 1718 제재 위원회의 북한 전문가 패널이 작성한 보고서에서 제공된 북한 IT 근로자에 대한 추가 정보를 제공한다. FBI 는 북한 IT 근로자로 의심되는 모든 활동을 포함해 의심스러운 활동을 현지 지부에 보고하도록 미국 기업을 장려한다.

북한 IT 근로자: 배경

북한 IT 근로자는 무기 개발 프로그램 등 북한 정권에서 가장 중요한 경제 및 보안 우선 순위에 자금을 지원하는 주요한 수익 흐름을 제공한다. 북한 김정은 위원장은 외화 및 주요 공급책으로서 IT 근로자의 중요성을 인식하고 이들의 작업을 지원한다.

수많은 북한 IT 근로자가 해외에 파견되거나 북한 내에 위치해 있으며 수익을 창출하여 북한 정부로 송금하고 있다. 북한 IT 근로자는 주로 중화인민공화국(PRC)과 러시아에 위치하고 있으며 적게는 아프리카와 동남아시아에 위치해 있다. 북한 IT 근로자는 해외 연락처를 이용해 프리랜서 직업을 얻고 고객과 더욱 직접적으로 접촉하는 경우가 많다.

모든 북한 IT 근로자는 북한 김정은 위원장 정권을 뒷받침하기 위해 돈을 번다. 대다수는 유엔이 금지한 북한 WMD 및 탄도 미사일 프로그램과 더불어 첨단 재래식 무기 개발 및 무역 부문에 직접적으로 관여하는 단체에 속해 있으며 해당 단체를 위해 일하고 있다. 이로 인해 북한 IT 근로자가 창출한 수익은 북한에서 미국 및 유엔 제재를 위반하여 WMD 와 탄도 프로그램을 개발하는 데 사용된다. 유엔과 미국은 이러한 단체 대다수를 제재 대상으로 지정했다. 북한 IT 근로자를 파견하는 북한 단체는 다음과 같다.

- **군수산업부(MID)의 313 총국**. 핵무기 및 탄도 미사일, 기타 군사 장비를 포함하여 북한에서의 연구 및 개발, 무기 생산을 관리한다. MID 는 조선로동당 중앙위원회 산하에 있으며 313 총국을 통해 북한의 IT 근로 인력 대부분을 해외로 파견한다. 조선로동당의 모든 자산과 자산에 대한 이익은 행정명령(E.O.) 13722 에 의하여 차단된다.

- **원자력공업성.** 북한의 핵무기 개발에 중요한 역할을 수행하며 북한 핵무기 프로그램의 일상적 운영을 맡고 있다. 원자력공업성은 E.O. 13382 에 의하여 지정되어 있다.

- **인민무력성**에 예속된 군사 조직. 조선인민군은 특별지정 제재대상(Specially Designated Nationals) 및 차단 자산 목록(Blocked Property List)에 지정되어 있다.

- **북한 교육위원회의 대외무역소** 및 **중앙위원회 과학교육부의 평양정보기술국** 등 잘 알려지지 않은 기관. 북한 정부의 모든 자산과 자산에 대한 이익은 E.O. 13722 에 의하여 차단된다.

해외의 북한 IT 근로자는 해외 공장 또는 건설 프로젝트에서 근로하는 기존 북한 노동자보다 최소 10 배 이상의 금액을 번다. 경우에 따라 북한 IT 근로자는 개인으로 연간 300,000 달러 이상을 벌며 IT 근로자 팀은 단체로 연간 3 백만 달러 이상을 벌 수 있다. 총 소득의 상당 부분은 북한 정부의 WMD 프로그램 등 우선 순위를 뒷받침한다.

일반적으로 북한 IT 기업과 근로자는 다음과 같이 다양한 복잡성과 난이도로 구성된 광범위한 IT 개발 업무에 종사한다.

- 모바일 애플리케이션 및 웹 기반 애플리케이션
- 가상화폐 거래 플랫폼 및 디지털 코인 구축
- 일반 IT 지원
- 그래픽 애니메이션
- 온라인 도박 프로그램
- 모바일 게임
- 데이트 애플리케이션
- 인공지능 관련 애플리케이션
- 하드웨어 및 펌웨어 개발
- 가상현실 및 증강현실 프로그래밍
- 안면 인식 및 생체 인식 소프트웨어
- 데이터베이스 개발 및 관리

북한 IT 근로자가 개발한 애플리케이션 및 소프트웨어는 비즈니스, 건강 및 피트니스, 소셜 네트워킹, 스포츠, 엔터테인먼트, 라이프스타일 등 다양한 분야와 부문에 걸쳐 있다. 북한 IT 근로자가 가상화폐와 관련된 프로젝트를 맡을 때도 있다. 일부 북한 IT 근로자들은 가상화폐 거래소를 설계하거나 가상화폐 거래자가 사용할 분석 도구 및 애플리케이션을 제작하여 제품을 시장에 직접 제공한다.

북한은 시민을 대상으로 수학 및 과학 교육의 중요성을 수십 년 동안 강조해왔다. 역사상 김정권의 우선 순위였던 과학 및 기술 선진화를 강조하는 데에는 관련 연구 분야에 투입된 자원과 인력 투자가 반영되어 있다. 오늘날 북한에서 수행되는 사이버 및 IT 교육은 선진화를 추진하는 이러한 동력에 기반해 수립되었으며, 그 결과 로동당, 연구 센터, 군과 함께 편성된 통합 커리큘럼이 나타났다.

- 최근 몇 년 동안 김정은 정권은 IT 관련 과목 교육과 훈련에 중점을 늘렸고 북한의 최상위 교육 기관, 특히 김일성종합대학, 김책공업종합대학, 평양과학기술대학 등 여러 곳에서는 수준 높은 IT 학위 프로그램을 개발했다. 이와 같은 상위 대학에서만 약 30,000 명의 학생이 정보통신 기술 관련 과목을 공부하고 있다.

- 2019 년 기준, 대학 37 곳에서 첨단 과학, 기술, 엔지니어링, 수학(STEM) 과목 강좌를 제공하는 프로그램 85 개를 마련했고, 각 도에서는 유망한 학생을 육성하기 위해 최소 하나 이상의 중등 학교를 신설한 것으로 알려져 있다.

- 북한의 교육 시스템은 매우 경쟁적이며 상위 학생만 엘리트 과학 기술 프로그램에 들어갈 수 있다. 학생들은 어린 나이에 금성학원 및 금성 제 1 고등중학교와 같은 중등 학교에 모집된다.

- 북한 IT 근로자는 기술을 더 개발할 수 있도록 종종 북한 내의 지역 IT 연구 센터를 통해 해외와 북한 조직에서 추가 교육을 받는다. 북한 IT 근로자는 지금껏 동아프리카, 동남아시아, 남아시아에서 교육을 받아 왔으며 해외 교육을 크게 활용했다.

북한 IT 근로자 운용 방식

북한 IT 근로자는 북미, 유럽, 동아시아 국가를 포함해 부유한 국가에 위치한 고용주와 프리랜서 계약을 맺는 것을 목표로 한다. 북한 IT 근로자는 많은 경우 한국, 중국, 일본, 동유럽, 미국에 기반을 둔 재택근무자로 행세한다.

북한 IT 근로자가 제 3 자 하청 계약자를 주선하여 신원을 더욱 파악하기 어렵게 하는 경우도 있다. 이러한 하청 계약자는 북한인이 아니며, 북한 IT 근로자를 대신해 계약을 완료하는 프리랜서 IT 근로자이다. 북한 IT 관리자는 북한인 고용주의 실제 신원을 모르거나 고용주가 북한 회사라는 사실을 대개 알지 못하는 비 북한인 IT 근로자로 이루어진 자체 팀도 고용했다. 소프트웨어를 구매하고 북한 IT 근로자를 노출시킬 가능성이 있는 상황에서 고객과 상호작용해야 할 때 북한 IT 관리자는 외주 직원을 이용한다.

일반적으로 북한 IT 근로자는 가상화폐 거래소 또는 웹사이트 개발과 같이 악성 목적이 아닌 IT 업무에 종사하지만, 북한에서 악성 사이버 침입을 수행할 수 있도록 계약자로서 획득한 액세스 권한을 사용하고 있다. 해외 주재 북한 IT 근로자 중 일부가 북한 기반 악성 사이버 행위자에게 군수지원을 제공하긴 했으나, IT 근로자가 직접 악성 사이버 활동에 개입할 확률은 낮다. 북한 IT 근로자는 가상 인프라를 이용할 액세스를 공유하거나 북한 사이버 행위자가 탈취한 데이터 판매를 촉진하거나 북한이 돈세탁과 가상화폐 송금을 수행하도록 지원할 수도 있다.

북한 IT 근로자는 금지된 북한의 무기 프로그램을 위해 WMD 및 탄도 미사일 관련 품목을 조달하도록 북한 공무원을 지원했다.

근로자가 강제 노동 등 인신매매되는 사례가 있다. 신뢰할 수 있는 보고에 따르면 해외의 여러 북한 근로자는 근무 시간이 과도하며, 북한 정부 보안 요원에게 지속적이고 면밀한 감시를 받고, 생활 여건이 안전하지 않고 위생적이지 않으며 이동의 자유가 적다. 북한 정부는 해외 근로자의 임금 중 최대 90%를 징수하여 정부에 연간 수억 달러의 수익을 창출하고 있다.

북한 IT 근로자: 기술 및 플랫폼

해외 북한 IT 팀은 주로 다양한 온라인 플랫폼을 이용해 프리랜서로 취직한다. 기업에서는 이러한 플랫폼을 사용해 프리랜서 IT 개발자가 입찰할 수 있는 프로젝트 계약을 알린다. 드물게, 북한 IT 팀은 현지 비 북한인을 찾아 실제로는 북한인이 관리하는 기업에서 명목상 책임자 역할을 맡기기도 한다. 서류상으로는 북한 IT 팀이 합법적 현지 기업에서 일하는 것처럼 보이나 개별적으로 자체 사업을 추진하는 사례도 있으며, 북한 IT 팀은 북한 국적을 숨겨주는 대가로 해외 기업에 대가를 지불한다. 북한 IT 팀에는 영어나 중국어 등 외국어에 능통한 구성원이 포함되는 경우가 많다.

북한 IT 근로자는 다양한 주류 플랫폼과 IT 산업별 프리랜서 계약 플랫폼, 소프트웨어 개발 도구 및 플랫폼, 메시징 애플리케이션, 소셜 미디어와 네트워킹 웹사이트를 이용해 전 세계 기업에서 개발 계약을 따내며 업무에 대한 보수를 받는 데 다양한 디지털 결제 플랫폼과 웹사이트를 활용한다. 북한 IT 근로자는 마찬가지로 가상화폐 거래소와 거래 플랫폼도 사용해 계약 작업으로 받은 디지털 지불금을 관리하고 받은 자금을 세탁하여 옮긴다.

북한 IT 근로자: 신원 은폐

북한 IT 근로자는 의도적으로 신원, 위치, 국적을 파악하기 어렵게 하며 한국 이름이 아닌 가명을 사용하곤 한다. 이들은 또한 눈에 띄지 않는 위치에서 인터넷에 접속하는 것처럼 보이게 하고 북한 위치나 관련성을 조사할 가능성을 줄이기 위해 가상 사설 네트워크(VPN), 가상 사설 서버(VPS)를 사용하거나 제 3 국 IP 주소를 활용한다. 일반적으로 북한 IT 근로자는 재택근무 방식으로 인한 익명성을 이용하고, 계정을 생성하고 유지하는 데 대리인을 이용하며, 영상 통화 대신에 텍스트 기반 채팅으로 이루어지는 중개 및 통신 이용을 선호한다.

북한 IT 근로자는 대리 계정을 사용하여 프리랜서 소프트웨어 개발자 웹사이트에 게시된 프로젝트에 입찰하고 낙찰 받으며 일하고 보수를 받는다. 이러한 대리 계정은 제 3 자 개인의 소유이며, 일부 개인들은 북한 IT 근로자에게 자신의 신분증과 계정 정보를 판매한다. 어떤 경우에는 북한 IT 근로자가 합법적인 플랫폼 계정을 사용하기 위해 이러한 개인에게 대가를 지불한다. 북한 IT 근로자는 대리인의 실제 소속과 업무 경험으로 프리랜서 플랫폼 프로필을 작성할 수도 있다.

때로 북한 IT 근로자는 개발 프로젝트에 협업을 제안하려는 목적으로 플랫폼에서 다른 비 북한인 프리랜서 근로자를 고용한다. 북한 IT 근로자는 이러한 사업 관계를 활용해 새로운 계약에 접근하고 미국이나 유럽의 가상 인프라를 통해 IT 작업을 수행하는 데 사용되는 가상화폐 계정에 대한 액세스 권한을 얻고, 부정 사용을 방지할 목적의 보안 조치를 우회한다. 다른 프리랜서 근로자의 도움을 받아 계정을 만드는 경우 북한 IT 근로자는 돈을 더 많이 벌기 위해 미국이나 기타 서구의 신분 증명서와 프리랜서 플랫폼 계정이 필요한 제 3 국 국적을 내세울 수도 있다.

북한 IT 근로자는 실제 위치를 은폐함으로써 온라인 플랫폼과 활동 시 사용하는 서비스의 서비스 약관을 따르지 않을 수 있다. 북한 IT 근로자는 간첩 활동의 일환으로 계정, 특히 은행 서비스에 각각 전용 기기 하나만 사용할 수 있으며, 이렇게 하여 사기 방지, 제재 준수, 자금 세탁 방지 조치로 인해 적발되는 상황을 모면하려고 한다.

북한 IT 근로자는 신분 증명서 등 위조, 변조, 조작된 문서와 위조 서명을 일상적으로 사용하며, 이는 Photoshop 등의 소프트웨어를 사용해 직접 제작하거나 변조하도록 문서 위조 회사에 보수를 지불하여 해당 IT 근로자의 사진이나 제공된 사진을 실제 인물의 신원 정보와 결합한 것이다. 일반적으로 북한 IT 근로자는 다음과 같은 위조 문서를 구입한다.

- 운전 면허증
- 사회보장카드
- 여권
- 주민등록증
- 재류 외국인 카드
- 고등학교 졸업장 및 대학교 졸업장
- 취업 비자
- 신용 카드, 은행, 공과금 내역서

어떤 경우에 이러한 신원은 도용된 것이고, 또 다른 경우 북한 IT 근로자가 비 북한인에게 자신의 개인 정보나 액세스할 수 있는 정보를 이용해 계정을 개설하도록 요청한 다음 비용을 지불하여 북한 IT 근로자가 계정 관리 권한을 획득한다. 이 방법으로 신원을 숨기고 북한 IT 근로자는 원격 데스크톱 액세스로 실제 예금주의 인프라를 이용하여 온라인 상으로 클라이언트에게 프로젝트를 입찰하고 프리랜서로 프로젝트를 완료할 수 있다.

각각의 IT 근로자는 여러 신원과 계정을 사용하곤 하며, 같은 팀 내 IT 근로자들 사이에 공유할 수 있다. 이러한 계정과 신원에는 세계 각지의 국가를 내세운다.

북한 IT 근로자는 프리랜서 플랫폼, 결제 공급업체, 북한 IT 근로자를 고용하는 기업에 신원을 입증하기 위해 미국이나 국제 은행의 고객 계좌 정보를 도용할 수도 있다. 북한 IT 근로자는 도용한 은행 계좌 정보를 사용해 수표를 위조한 사례가 최소 한 건 있다. 북한 IT 근로자의 대리 신원과 관련된 계정 및 이력서에는 위조되었으나 실제적이고 자세한 교육 및 고용 내역 정보가 포함된 경우가 많으며, 교육 기관과 이전 고용주의 허위 연락처 정보도 이에 해당된다.

북한 IT 근로자는 프로젝트를 입찰할 때 평판이 좋은 미국인이나 유럽인처럼 보이기 위해 소규모 또는 중소 서구 기업의 이름으로 온라인 개발자 프로필의 고용란을 작성할 수도 있다. 실제 직원의 이름과 합법적인 서구 기업 도메인과 유사해 보이는 이메일 주소를 사용할 수도 있다.

북한 IT 근로자는 프리랜서 고용 플랫폼과 함께 사용할 업무 기술 계약서, 송장, 클라이언트 연락 문서, 기타 문서를 추가로 위조하여, 플랫폼에서 사용자 활동의 적법성을 보장하기 위해 마련한 고객 확인 절차 및 자금 세탁 방지(KYC/AML) 조치나 이와 유사한 조치를 충족할 가능성이 높다. 이러한 위조 문서에는 검증할 수 없도록 연락처 세부 정보가 최소한으로 포함되어 있을 수 있다.

북한 IT 근로자는 자신을 대한민국 국민, 또는 간단히 “한국” 시민으로 표현하여 국적을 감추려고 할 수도 있다.

기업에서 알아차리지 못하게 프리랜서로 취직한 북한 IT 근로자는 취직 이후에 다른 북한 IT 근로자들을 프리랜서로 고용하도록 기업에 추천하는 것으로도 알려져 있다.

북한 IT 근로자 이력

북한 IT 근로자는 시스템 및 프로그램 개발 작업, 데이터베이스 관리 시스템 작업, 다양한 공통 언어, 프레임워크, 도구, 클라우드 리소스 사용 기술을 내세운다. 다양한 코딩 언어와 마크업 언어를 다루는 높은 수준의 기술이 포함되는 경우가 흔하다. 북한 IT 근로자의 프로젝트 대다수는 모바일 및 웹 앱 개발과 관련된다. 북한 IT 근로자는 데이터와

워크플로를 관리하는 데 협업 플랫폼이나 호스팅 서비스도 사용한다. 근로자들은 다양한 데이터베이스에 대한 경험을 가지고 있으며 주요 공급업체가 제공하는 클라우드 및 분석 제품과 서비스에 익숙하다. 이와 더불어, 북한 IT 근로자는 자신들의 업무에 디지털 결제와 전자상거래 플랫폼을 포함한다.

북한 IT 근로자는 프리랜서 개발자라는 조작 인물의 신뢰성을 높이려는 목적으로 보통 간단한 디자인으로 “포트폴리오” 웹사이트를 구축한다. 이와 같은 가상 포트폴리오는 북한 IT 근로자가 조작한 인물의 작업을 보여주며 흔히 온라인 프리랜서 개발자 계정에 연결되어 있다. 연락처 정보, 위치를 포함하여 근무 이력과 교육 정보 등 웹사이트 내의 정보는 거짓일 가능성이 높다.

적신호

프리랜서 업무 및 결제 플랫폼 기업은 해당 플랫폼을 이용하는 북한 IT 근로자를 암시하거나 이들의 행동일 수 있는 다음 활동을 인지하고 있어야 한다.

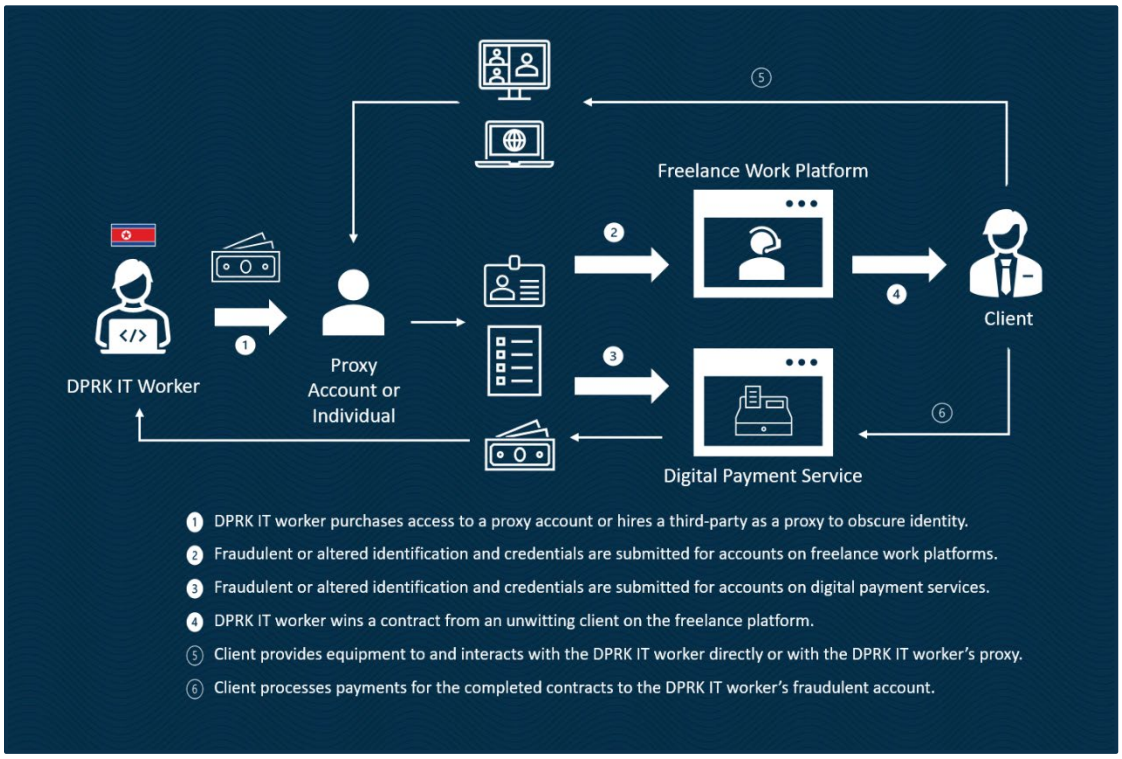
- 상대적으로 짧은 시간 내에 다양한 IP 주소로 한 계정에 여러 번 로그인하며, 특히 IP 주소가 각기 다른 국가에 연결되어 있는 경우 해당됨.
- 개발자가 IP 주소 한 곳에서 동일한 플랫폼의 여러 계정에 로그인함.
- 개발자가 한 번에 하루 이상 계정에 계속 로그인되어 있음.
- 계정에 액세스하는 데 사용된 라우터의 3389 포트 등 원격 데스크톱 공유 소프트웨어 사용과 관련된 라우터 포트나 기타 기술 구성, 특히 원격 데스크톱 공유 소프트웨어를 사용하는 것이 기업의 표준 관행이 아닌 경우 해당됨.
- 개발자 계정의 평가를 높이기 위해 개발자 계정에서 사기성 클라이언트 계정을 사용하지만, 클라이언트 및 개발자 계정이 돈을 송금/인출하는 데 동일한 PayPal 계정을 사용함(자신의 돈으로 스스로에게 보수를 지불함).
- 입찰 문서 및 프로젝트 소통 방법 등 문서 템플릿을 빈번하게 사용함. 특히 서로 다른 개발자 계정에 걸쳐 동일한 템플릿이 사용됨.
- 단기간에 하나의 클라이언트 계정에서 높은 평가를 받는 여러 개발자 계정으로, 개발자 계정 및/또는 클라이언트 계정을 만드는 데 유사하거나 동일한 문서를 사용함.
- 프로젝트를 폭넓게 입찰하고, 개발자가 입찰한 프로젝트 수와 비교해 수락된 프로젝트의 수가 적음.
- 결제 플랫폼을 통해, 특히 중화인민공화국에 위치한 은행 계좌로 돈을 빈번하게 송금함. 자금의 최종 목적지를 숨기기 위해 하나 이상의 기업을 통해 전달할 때도 있음.

프리랜서 개발자를 고용하는 기업은 북한 IT 근로자를 암시하거나 이들의 행동일 수 있는 다음 활동을 인지하고 있어야 한다.

- 프리랜서 소프트웨어 개발 웹사이트 또는 결제 플랫폼 계정이 정지되었거나 다른 계정을 사용하도록 근로자가 고용인에게 연락한 경우, 특히 다른 이름으로 등록되어 있는 경우.
- 디지털 결제 서비스, 특히 중화인민공화국에 연결된 서비스를 사용함.
- 개발자의 프리랜서 플랫폼 프로필, 소셜 미디어 프로필, 외부 포트폴리오 웹사이트, 결제 플랫폼 프로필, 평가한 위치와 시간에 따라 이름 철자, 국적, 주장한 근무 위치, 연락처 정보, 교육 이력, 근무 이력, 기타 세부 정보가 일치하지 않음.
- 포트폴리오 웹사이트, 소셜 미디어 프로필, 또는 개발자 프로필이 놀라울 정도로 간단함.
- 소프트웨어 개발 회사의 고위 간부 급 임원이라고 주장하는 개인이 서비스를 권유하거나 숙련성을 홍보하려는 목적으로 다이렉트 메시지나 콜드콜을 보냄.
- 클라이언트가 IT 근로자를 만난 기존 프리랜서 플랫폼 웹사이트가 아닌 별도의 플랫폼에서 클라이언트 및 잠재 클라이언트와 소통하겠다고 요청함.
- 고용주가 문서를 보내거나 랩톱 등 업무 관련 장비를 보낼 것을 개발자에게 제안하면 개발자의 신분 증명서에 나타나 있지 않은 주소로 해당 품목을 보내도록 개발자가 요청함. 개발자가 신분 증명서 상의 주소로 품목을 받지 못한다고 주장하면 특히 의심해야 함.
- KYC/AML 조치와 정식 금융 시스템 사용을 피하기 위한 활동으로 보수를 가상화폐로 받으려고 함.
- 프로덕션 벤치마크나 체크인 미팅을 이행하지 않고 계약에 대한 보수를 요청함.
- 필수 업무시간 내에 비즈니스를 수행할 수 없음.
- 연락처 정보, 특히 전화 번호 및 이메일이 잘못되었거나 변경됨.

- 지원자와 인적 정보가 일치하지 않는 것으로 보임.
- 적시에 업무를 완료하지 못했거나 업무에 응답하지 못함.
- 적시에 연락할 수 없음. 특히 “인스턴트” 소통 방식을 이용할 수 없음.
- 다른 계약을 성사하기 위해 개인 정보 일부를 빌려 달라고 동료들에게 요청함.

북한 IT 근로자 운용 방식 개요



잠재적 완화 조치

프리랜서 업무 및 결제 플랫폼 기업의 경우

- 검토 및 계약 실사 절차의 일환으로 제출 문서를 확인함. 예를 들어 제출 문서에 제공된 연락 정보가 아니라 비즈니스 데이터베이스에 있는 연락처 정보를 사용하여 제시된 클라이언트에게 연락하여 송장 및 업무 계약서를 개별적으로 확인함.
- 제출된 신원 확인 증명서가 위조되었는지 면밀히 살핌. 지방 법집행기구에 도움을 요청하는 것도 가능함. 신원 확인을 위해 제출한 이미지가 저화질이면 거부해야 함.
- 계정을 만들기 위해 제공된 웹사이트가 있는지 확인함. 사용되지 않는 웹사이트를 사용하여 만든 계정은 더 면밀히 조사함.
- 초기 실사 계약 프로세스 및 갱신 정책의 일환으로, 동영상 신원 검증을 제출하도록 요구하거나 신원을 확인할 영상 인터뷰를 수행함.

- 정기적으로 포트 확인 기능을 사용해 데스크톱 공유 소프트웨어나 VPN 또는 VPS 을 통해 원격으로 플랫폼에 접속했는지 확인함. 특히 원격 데스크톱 공유 소프트웨어나 VPN 서비스를 사용해 계정에 접속하는 것이 표준 관행이 아닐 경우 해당됨.

- 동일하거나 유사한 문서로 계정을 만들었거나 동일한 디지털 결제 서비스 계정을 사용하는 클라이언트나 개발자 계정을 추가로 검토하도록 자동 표시함.

- 입찰하고 프로젝트 소통을 진행하는 데 각기 다른 개발자 계정에서 동일하거나 유사한 문서 템플릿을 사용하는 상황을 추가로 검토하도록 자동 표시함.

- 단기간에 하나의 클라이언트 계정에서 높은 평가를 받는 여러 개발자 계정을 추가로 검토하도록 자동 표시함. 특히 계정을 만드는 데 유사하거나 똑같은 문서를 사용했을 경우 해당됨.

- 프로젝트 입찰 횟수에 비교하여 프로젝트 입찰 승인 횟수가 적은 개발자 계정뿐만 아니라 입찰 비율이 높은 개발자 계정을 추가로 검토하도록 자동 표시함. 추가로, 계정 로그인 횟수와 비교해 프로젝트 입찰 횟수가 많은 계정을 표시함.

- 전체 계정을 확인하기 전에 새로 생성된 계정으로 활동하지 않게 함.

- 새로 생성된 계정을 추가로 면밀히 검토함.

프리랜서 플랫폼에서 프로그래머와 개발자를 고용하는 기업의 경우

- 프리랜서 근로자가 될 수 있는 사람의 신원을 확인하기 위해 영상 인터뷰를 수행함.

- 고용 전 신원 조사, 약물 검사, 지문/생체 측정 로그인을 수행해 신원과 주장한 위치를 확인함. 가상화폐로 지불하지 않고 기타 신분 증명서와 상응하는 은행 정보를 입증하도록 요구함.

- 원격 데스크톱 애플리케이션과 같은 원격 협업 애플리케이션으로 프리랜서 개발자와 상호작용할 때는 각별히 주의함. 프리랜서 개발자에게 제공한 컴퓨터에서 원격 협업 애플리케이션 사용을 중지할 것을 고려함.

- 직원이 될 수도 있는 사람에게 직접 받았거나 프로필에서 확인한 연락처 정보가 아니라, 검색 엔진이나 기타 비즈니스 데이터베이스를 통해 파악한 연락처 정보를 사용하여 제시된 기업과 교육 기관에 고용 및 고등교육 이력을 직접 검증함.
- 개발자의 프리랜서 플랫폼 프로필, 소셜 미디어 프로필, 외부 포트폴리오 웹사이트, 결제 플랫폼 계정, 평가한 위치와 시간에 따라 고용될 가능성이 있는 사람의 이름 철자, 국적, 주장한 위치, 연락처 정보, 교육 이력, 근무 이력, 기타 세부 정보가 일관적인지 확인함. 간단한 포트폴리오 웹사이트, 소셜 미디어 프로필, 또는 개발자 프로필에 각별한 주의를 기울임.
- 기업이 처음 IT 근로자를 만난 기존 프리랜서 플랫폼 웹사이트가 아닌 별도의 플랫폼에서 소통하자는 개발자의 요청에 주의함.
- 개발자에게 문서나 랩톱 등의 업무 관련 장비를 보낼 경우에는 개발자의 신분 증명서에 기재된 주소로만 보내고 개발자가 랩톱이나 기타 품목을 확인되지 않은 주소로 보내라고 요청할 경우 추가 문서를 확보함. 개발자가 신분 증명서 상의 주소로 품목을 받지 못할 경우에는 의심해야 함.
- 계약한 IT 근로자가 속여 수행할 수 있는 비승인 소규모 거래를 주의해야 함. 미국 기업에 개발자로 고용된 북한 IT 근로자가 해당 미국 기업의 계정에 사기로 청구하고 약 몇 개월에 걸쳐 30 번 소액으로 나누어 50,000 달러 이상을 가로챈 사례도 있음. 해당 미국 기업은 개발자가 북한인이라는 사실을 몰랐고 금액이 적어 진행 중인 절도 행위도 인지하지 못했음.

금지되었거나 제재 대상이 될 수 있는 행위에 참여하는 데 따르는 결과

관련 금융 거래를 처리해주는 것을 포함해, 북한 IT 근로자 관련 활동에 참여하거나 지원하는 개인 및 단체는 금지되었거나 제재 대상이 될 수 있는 행위에 참여하는 데 따르는 잠재적 법적 결과를 인지해야 한다.

유엔 안전보장이사회(Security Council) 결의안 2321 호, 2371 호, 2397 호에서는 해외 북한 근로자가 창출하는 수익이 북한의 핵무기 및 탄도 미사일 프로그램을 지원하고 있다는 점을 강조한다. 유엔 안전보장이사회 결의안 2375 호는 유엔 안전보장이사회의 1718

위원회가 사전에 승인하지 않는 한, 유엔 회원국이 해당 국가 입국과 관련하여 관할권 내의 북한인에게 새로운 근로 허가를 제공하거나, 만료된 허가를 갱신하는 것을 금지한다. 유엔 안전보장이사회 결의안 2397 호에 따라 모든 회원국은 문제의 북한인에게 근로 허가가 발행된 시기, 발행되었는지 여부와 관계 없이 2019 년 12 월 22 일까지 관할권 내에서 소득이 있는 북한인을 본국으로 송환해야 한다.

재무부의 해외자산통제국(Office of Foreign Assets Control, OFAC)은 특히 다음 내용에 해당하는 것으로 확인된 모든 사람에게 금융 제재를 가할 권한이 있다.

- 북한 정부나 조선로동당을 대신하여 사이버 보안을 약화시키는 중대한 활동에 참여함.
- IT 업계에서 북한을 대신하여 운영함.
- 기타 특정한 악성 사이버 이용 활동에 참여함.
- 재화, 서비스, 기술을 북한에서 수입하거나 북한에 수출하는 하나 이상의 업무에 참여함.
- 북한이나 이를 대신하여 행동하는 사람, 북한 정부나 조선로동당을 대신하는 사람과 소프트웨어를 직간접적으로 판매, 공급, 이전, 구매 행위를 하며, 이로 인해 수령한 수익이나 재화가 북한 정부나 조선로동당에게 이익이 될 수 있는 경우.
- 북한 정부나 조선로동당을 지원하거나 원조하기 위하여 물질적으로 지원하거나, 후원하거나, 재정적, 물질적, 기술적 지원이나 재화 또는 서비스를 제공함.

예를 들어 미국은 2018 년에 중국에 기반을 둔 기술 회사인 Yanbian Silverstar Network Technology Co., Ltd 를 제재 대상으로 지정했다. 명목상 이 회사는 중국 IT 기업이었으나 실제로는 북한인들이 관리하고 통제했다. 이 회사는 프리랜서 직업 포럼의 신원 확인 요건을 면하기 위해 러시아에 기반한 유령 회사 Volasys Silver Star 까지 설립했다.

이와 더불어 재무장관이 국무장관과 협의하여 해외 금융 기관이 북한과의 중요한 무역을 고의로 수행 또는 용이하게 했거나, 북한 관련 행정명령 또는 북한 관련 활동에 대한 행정명령 13382 호(대량 살상 무기 확산자 및 지지자)에 지정된 사람을 대신해 중요한

거래를 고의로 수행 또는 용이하게 했다고 판단하는 경우, 해당 기관은 다른 잠재적 제한 사항 중 미국에서 환거래 계좌나 대리지불계좌를 유지할 능력을 상실하게 될 수도 있다.

경제 제재 집행 지침(Economic Sanctions Enforcement Guidelines, 31 C.F.R. 501 부분, 부록 A)에 요약된 바와 같이 OFAC 은 제재 규정을 명백하게 위반하는 행위를 조사하여 집행 권한을 행사한다. 북한 제재 규정(North Korea Sanctions Regulation, 31 C.F.R. 510 부분)을 위반하는 사람은 적용 가능한 법정 최대 벌금 중 가장 큰 금액이나 근거하는 거래액의 두 배에 해당하는 금액을 최고 벌금으로 하는 민사금전벌을 받을 수 있다.

또한 대북제재 및 정책 강화법(North Korea Sanctions and Policy Enhancement Act of 2016, 22 U.S.C. § 9241 이하)을 개정한 제재를 통한 적대국 대응법(Co 유엔 tering America's Adversaries Through Sanctions Act, CAATSA. 공법 115-44)의 321(b)절(22 U.S.C. § 9241a)에서는 세계 어디서든 북한 국적의 사람이나 북한 시민이 전부이든 일부이든 채굴, 생산, 제조한 중요 재화, 물건, 상품, 물품을 관세법(Tariff Act of 1930, 19 U.S.C. § 1307)에 따라 수입이 금지된 강제 노동 재화로 반박 가능한 추정을 작성했다. 이는 미국 내 모든 항구에 이러한 재화가 들어올 자격이 주어지지 않아야 하며 억류, 압수, 몰수 대상이 될 수도 있다는 의미이다. 위반 시에는 민사 처벌과 함께 형사 소추가 초래될 수도 있다. 그러나 CAATSA 에 따라, 명확하고 설득력 있는 증거를 통해 미국 관세국경보호청(Customs and Border Protection, CBP)의 청장이 재소자 노동, 강제 노동, 연기계약 노동으로 해당 재화가 생산되지 않았다는 것을 확인할 경우 이러한 재화를 수입할 수도 있다. 관세법(Tariff Act of 1930)으로 형사적 제재에 하에 재소자 노동, 강제 노동 또는 연기계약 노동(강제 또는 연기계약 아동 노동 포함)으로 생산된 재화 수입이 금지되었으며 이에 따라 약 90 년 동안 시행되어 왔다.

법무부(Department of Justice)는 적용 가능한 연방법에 대한 조사 및 기소를 담당하며, 국제위기경제권한법(International Emergency Economic Powers Act, "IEEPA"), 50 U.S.C. §§ 1701 이하, 은행비밀법(Bank Secrecy Act, BSA), 31 U.S.C. §§ 5318 및 5322 가 포함된다. IEEPA 에 따라, 북한 관련 행정명령(예: 행정명령 13722 호와 13810 호), 행정명령 13382 호, 북한제재규정(the North Korean Sanctions Regulations, 31 C.F.R. 510 부분)을 포함해 IEEPA 에 의거한 허가, 명령, 규정, 금지 사안을 고의로 위반하거나, 위반하려고 시도하거나, 위반하려고 계획하거나, 위반을 초래하는 것은 범죄에 해당한다. 고의로 IEEPA 를 위반하는 사람은 20 년 이하의 징역에 처하거나, 100 만 달러 이하의 벌금이나 총수익의 두 배에 해당하는 금액 중 더 큰 액수의 벌금을 물거나, 이러한 거래에 관련된 모든 자금이

몰수될 가능성이 있다. BSA 에 따라 특히 금융 기관은 효율적인 자금세탁 방지 프로그램을 유지하고 특정 보고서를 FinCEN 에 제출해야 한다. BSA 를 위반하는 사람은 5 년 이하의 징역에 처하거나, 250,000 달러 이하의 벌금을 물거나, 위반 행위와 관련된 자산이 몰수될 가능성이 있다. IEEPA, BSA, 기타 적용 가능한 연방 법을 위반하는 기업 및 기타 단체도 형사 소추될 수 있다. 또한 법무부는 해외 파트너와 협력해 미국과 해외에서 수행되는 범죄 수사와 기소를 뒷받침할 증거를 공유한다.

31 U.S.C. § 5318(k)에 의거하여, 재무장관이나 법무장관은 해외에 저장된 기록으로 미국 내에 환거래 은행 계좌를 유지하고 있는 해외 금융 기관을 소환할 수도 있다. 재무장관이나 법무장관이 해외 금융 기관이 이러한 소환장에 불응했다는 서면 통지를 미국 금융 기관에 보내는 경우, 미국 금융 기관은 영업일 10 일 이내에 환거래계약을 종료해야 한다. 이를 이행하지 않으면 미국 금융 기관은 일일 기준 민사 처벌의 대상이 될 수 있다.

북한 관련 정의에 대한 보상(REWARDS FOR JUSTICE)

과거 또는 진행 중인 작전을 포함하여 북한이 수행하는 사이버 공간 상 불법 활동에 대한 정보가 있다면 해당 정보를 국무부의 정의에 대한 보상 프로그램에 제공하면 최대 5 백만 달러의 보상을 받을 자격을 갖출 수 있다. 다음 주소를 방문해 자세한 내용을 확인할 수 있다. https://rewardsforjustice.net/index/?north-korea=north-korea.

부록

북한 IT 근로자에 대한 국제 연합 전문가 패널의 보고

유엔 안전보장이사회 1718 대북제재 위원회는 유엔 회원국, 관련 유엔 기관, 유엔 안전보장이사회 대북 결의안에 서술된 조치를 이행하는 기타 당사자를 통해 정보를 수집, 검토, 분석하는 전문가 패널(이하 패널)의 지원을 받는다. 패널은 1718 위원회에 중간 보고서와 최종 보고서를 모두 제공하여 제재 이행 시 개선할 방법 권고안도 제시한다. 해당 보고서는 다음 사이트에서 찾아볼 수 있다.
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

패널은 유엔에서 지정한 군수산업부(MID)에 예속된 근로자 등 북한 IT 근로자 사례를 다양하게 조사했으며, 패널 반기 보고서에 다음 내용을 포함한 조사 정보를 제시했다.

패널은 2019 년 중기 보고서에서 처음 북한 IT 근로자를 보고했다. 이때 북한의 핵 및 탄도 미사일 프로그램 개발에서 맡은 감독 역할로 인해 제재 대상으로 지정된 MID 에 주목했고, MID 는 외화를 벌기 위하여 소프트웨어 프로그래머 및 개발자 등 북한 정보기술 근로자를 해외에 배치하는 데 산하 무역 기업을 이용하고 있었다. 당시 유럽, 아시아, 아프리카, 중동에 위치한 북한 IT 근로자들은 신원을 위장하고 프리랜서로 취직하는 데 해외 웹사이트를 활용했다. 북한 IT 근로자는 악성에 해당하지 않는 정보기술 작업과 함께, 금융 제재를 피하고 있는 북한의 사이버 행위자를 뒷받침하여 가상화폐 등의 자산 도용에 관련된 불법 작업을 수행했다.

패널은 2020 년 최종 보고서에서 북한 IT 근로자 조사를 이어갔으며, 대부분의 해외 북한 IT 근로자가 MID 산하 기업에 고용되어 있다는 점을 밝혔다. MID 는 수익 창출을 목적으로 2019 년까지 최소 1,000 명 이상의 IT 근로자를 파견하며, 산하 단체나 유령 회사를 자주 이용한 것으로 추정되었다. 그러나 이들이 우회 기법을 사용하므로 해외 및 북한 내 실제 IT 근로자의 수는 명확하지 않았다. 패널은 북한 IT 근로자가 신원을 드러내지 않고 프리랜서 IT 작업을 맡기 위해 인지하지 못한 전 세계의 클라이언트, 특히 중국, 러시아, 우크라이나, 세르비아, 캐나다, 미국의 클라이언트를 이용해 프리랜서 개발자 플랫폼에 계정을 생성하는 등 다양한 방법을 사용한다는 점을 언급했다. 패널은 북한 IT 근로자 팀과 중국, 네팔, 베트남에 위치한 관련 회사에 대한 특정 사례 여러 건을 추가로 조사했다.

패널은 중국과 러시아의 여러 북한 IT 근로자 팀을 조사했고 2020 년 중간 보고서에서 조사 내용을 상세히 기술했다. 패널은 MID 에 예속된 북한 IT 근로자 수백 명이 2019 년과 2020 년에 중국에서 활동했으며, 제 3 국 개인의 이름으로 프리랜서 플랫폼 계정에 대한 액세스 권한을 불법적으로 획득했다고 밝혔다. 패널은 북한 MID 산하 IT 근로자로 구성된 여러 단체가 2019 년과 2020 년에 러시아에서 활동했으며, 정보기술 프리랜서 플랫폼, 가상화폐 웹사이트, 결제 웹사이트에 액세스하는 데 가짜 해외 신원을 활용했다는 점도 언급했다.

패널의 2021 년 최종 보고서에 따르면, 북한 IT 근로자는 가짜 신원 증명 제공, VPN 서비스 사용, 유령 회사 설립 등 북한에서 국제 금융 시스템에 액세스하는 데 활용한 것과 유사한 우회 기법을 이용하여 고용주의 실사 활동과 KYC/AML 프로토콜을 피해갈 수 있다. 패널은 추가적으로 북한과 연계된 대부분의 계정이 중국 내 위치에서 운영된다는 점을 언급했다. 면밀한 검토를 피하기 위해 이러한 계정은 IT 서비스를 이용하려는 잠재 고객과 접촉한 다음 “사이트 외부”로 향한다. 북한과 연계된 사용자는 보안 수준이 낮거나 실사 절차가 비교적 엄격하지 않은 IT 프리랜서 플랫폼을 대상으로 삼기도 한다. 패널은 준수 의무를 이행하는 과정과 북한에서 수행되는 국제 결제 시스템 액세스를 의도치 않게 용이하도록 해주는 과정에서 IT 프리랜서 플랫폼이 겪게 되는 위험을 특히 경고하면서, 유엔 회원국에게 프리랜서 IT 기업과 협력하여 제재 준수 이행 능력과 역량을 강화할 것을 권고한다.