North Korean Tactics, Techniques, and Procedures for Revenue Generation

North Korea is evading US and UN sanctions by targeting private companies to illicitly acquire income and fund the regime's priorities, including its WMD and ballistic missile programs. This product provides an overview of the common tactics, techniques, and procedures (TTPs) North Korean cyber actors use to target and gain access to financial institutions and entities associated with cryptocurrency for cyber exploitation and revenue generation. In addition, this product provides mitigation measures to identify and deter North Korean IT workers deployed worldwide who pose as other nationalities to gain employment.

NORTH KOREAN CYBER OPERATIONS

North Korea's cyber actors employ a range of tactics in their operations to further their larger espionage and financial goals.

Spear Phishing or Social Engineering		North Korean cyber actors rely heavily on spear phishing with investment-, job-, and payroll-themed e-mails or social media messages to trick a target company's employees into downloading malware that will enable cyber actors to compromise the firm's network, exfiltrate wallet private keys, or hijack transaction validators to undermine the security and integrity of entire blockchains.
North Korean IT Worker–Enabled Malicious Access		North Korean IT workers living abroad use privileged access gained as contractors to support the regime's cyber operations by sharing access to virtual infrastructure, facilitating the sale of stolen data, or assisting with money laundering and virtual currency transfer.
Software Vulnerability Exploitation		North Korean cyber actors buy vulnerabilities and exploits from brokers or steal them from security researchers for use against unpatched networks. Advanced persistent threat (APT) 37 and the Lazarus Group are the most likely North Korean cyber groups to use software exploits and quickly weaponize zero-day vulnerabilities.
Supply Chain Attack		North Korean cyber actors compromise software firms or third-party IT providers to insert malicious code into a company's software and also target cryptocurrency customers through legitimate but compromised applications.

Indicators of Potential North Korean Cyber Operations

Custom Malware

The remote-access Trojan (RAT) Manuscrypt is among the most notable malware that North Korean actors—including Lazarus Group and APT38—use to target companies.

The actors also use AppleJeus, often disguised as a cryptocurrency trading application, to target both individuals and firms.

Self-Signed Certificate Services

Sectigo SSL and Let's Encrypt are among the popular certificate services used by the actors.

Trojanized Applications

North Korean actors—including Kimsuky and the Lazarus Group—deliver malware to victims through Trojanized two-factor authenticators, cryptocurrency trading applications, and software installers, especially in software supply chain attacks.

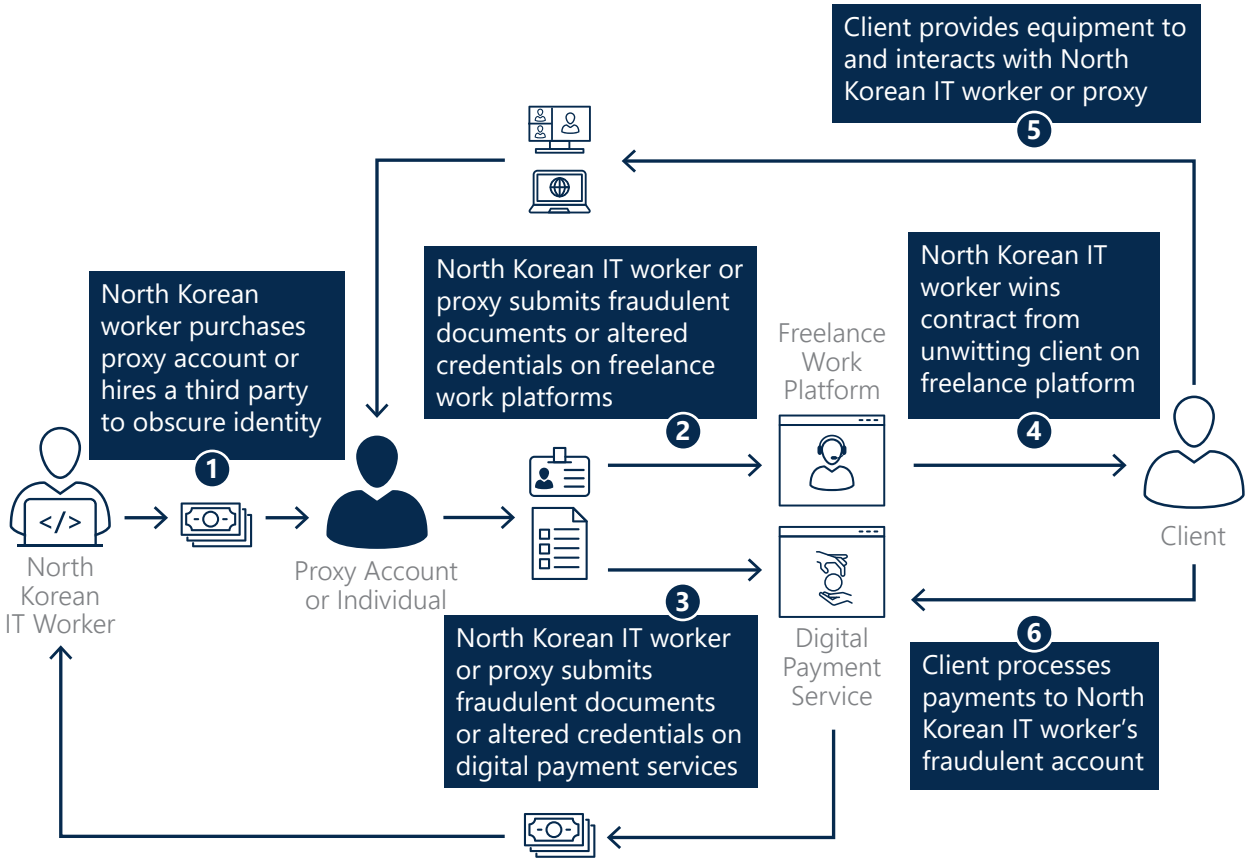
Free and Low-Cost Hosting and Registration Services

North Korean actors have used HostUS, Namecheap, and Porkbun to support their operations.

NORTH KOREAN IT WORKER OPERATIONS

Deployed North Korean IT workers target companies across North America, East Asia, and Europe to secure freelance contracts, often masquerading as teleworkers from North America, China, Eastern Europe, Japan, or South Korea. These workers use a variety of techniques to obfuscate their identities, such as hiring third-party subcontractors who are non–North Korean IT workers and finding non-North Korean nationals to serve as the nominal heads of regime-controlled front companies. Since 2022, North Korean IT workers have adapted to public disclosure of their TTPs by finding new ways to procure fraudulent documents and by contracting out work to other non-North Korean individuals.

North Korean IT Worker Hiring Process



North Korean Tactics, Techniques, and Procedures for Revenue Generation

North Korean IT Worker Red Flag Indicators and Potential Mitigation Measures

KEY: Freelance work or payment processing platforms | Companies hiring the IT workers

STEP ❶: North Korean IT worker purchases proxy account or hires a third party to obscure identity

STEP ❷: North Korean IT worker or proxy submits fraudulent documents or altered credentials on freelance work platforms

Red Flags

- Suspicious account logins
- Remote desktop use
- Fraudulent developer accounts
- Frequent use of document templates
- Suspicious developer ratings
- Extensive project bidding

Mitigation

- Require video verification
- Scrutinize documents for forgery
- Request law enforcement assistance
- Reject low-quality verification images
- Check for workers accessing platform using remote desktop, virtual private network (VPN), or virtual private server (VPS)
- Flag accounts using similar documentation
- Flag developer accounts with high bidding or low-bid acceptance rates
- Do not allow accounts full access without verification
- Scrutinize new accounts

STEP ❸: North Korean IT worker or proxy submits fraudulent documents or altered credentials on digital payment services

Red Flags

- Suspicious account logins
- Remote desktop use
- Frequent money transfers

Mitigation

- Flag accounts that use similar documentation for digital payment services accounts

STEP ❹: North Korean IT worker wins contract from unwitting client on freelance platform

Red Flags

- Requests to use different development or payment services account
- Inconsistencies in provided information
- Overly simple portfolio website or profile
- Direct messages from purported senior executives advertising services
- Requests to communicate on separate platforms

Mitigation

- Conduct video interviews
- Ensure IT worker's information is consistent across profiles
- Conduct preemployment background check
- Do not trust contact information provided by IT worker

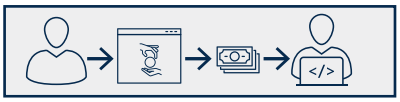
STEP ❺: Client provides equipment to and interacts with North Korean IT worker or proxy

Red Flags

- Developer cannot receive items at listed address

Mitigation

- Disable remote collaboration on computers supplied to IT developers
- Flag IT workers who cannot receive equipment at address listed on their identification documents



STEP ❻: Client processes payments to North Korean IT worker's fraudulent account

Red Flags

- Use of PRC-linked digital payment services
- Requests payment without meeting benchmarks
- Seeks virtual currency payments to avoid know your customer/ anti-money-laundering measures

Mitigation

- Be vigilant for unauthorized, small-scale transactions