Internet Crime Complaint Center (IC3)

Published: 2025-01-23 · Archived: 2026-04-05 19:50:41 UTC

The Federal Bureau of Investigation (FBI) is providing an update to previously shared guidance regarding Democratic People's Republic of Korea (North Korea) Information Technology (IT) workers to raise public awareness of their increasingly malicious activity, which has recently included data extortion. FBI is warning the public, private sector, and international community about North Korean IT workers' continued victimization of US-based businesses. In recent months, in addition to data extortion, FBI has observed North Korean IT workers leveraging unlawful access to company networks to exfiltrate proprietary and sensitive data, facilitate cyber-criminal activities, and conduct revenue-generating activity on behalf of the regime.

Extortion and Theft of Sensitive Company Data

- After being discovered on company networks, North Korean IT workers have extorted victims by holding stolen proprietary data and code hostage until the companies meet ransom demands. In some instances, North Korean IT workers have publicly released victim companies' proprietary code.
- North Korean IT workers have copied company code repositories, such as GitHub, to their own user profiles and personal cloud accounts. While not uncommon among software developers, this activity represents a large-scale risk of theft of company code.
- North Korean IT workers could attempt to harvest sensitive company credentials and session cookies to initiate work sessions from non-company devices and for further compromise opportunities.

Tips to Protect Your Business

Recommendations for Data Monitoring

- Practice the Principle of Least Privilege on your networks, to include disabling local administrator accounts and limiting privileges for installing remote desktop applications.
- Monitor and investigate unusual network traffic, to include remote connections to devices or the installation/presence of prohibited remote desktop protocols or software. North Korean IT workers often have multiple logins into one account in a short period of time from various IP addresses, often associated with different countries.
- Monitor network logs and browser session activity to identify data exfiltration through easily accessible means such as shared drives, cloud accounts, and private code repositories.
- Monitor endpoints for the use of software that allows for multiple audio/video calls to take place concurrently.

Recommendations for Strengthening Remote-Hiring Processes

- Implement identity-verification processes during interviewing, onboarding, and throughout the employment of any remote worker. Cross-check HR systems for other applicants with the same resume

content and/or contact information. North Korean IT workers have been observed using artificial intelligence and face-swapping technology during video job interviews to obfuscate their true identities.
- Educate HR staff, hiring managers, and development teams regarding the North Korean IT worker threat, specifically focusing on changes in address or payment platforms during the onboarding process.
- Review each applicant's communication accounts as North Korean IT workers have reused phone numbers (particularly voice-over-IP numbers) and email addresses, on multiple resumes purportedly belonging to different applicants.
- Verify third-party staffing firms conduct robust hiring practices and routinely audit those practices.
- Use "soft" interview questions to ask applicants for specific details about their location or education background. North Korean IT workers often claim to have attended non-US educational institutions.
- Check applicant resumes for typos and unusual nomenclature.
- Complete as much of the hiring and onboarding process as possible in person.

Reporting

If you suspect you have been approached or victimized by a North Korean IT worker, FBI recommends taking the following actions:

- Report the suspicious activity to the FBI's Internet Crime Complaint Center (IC3) at www.IC3.gov as quickly as possible.
- Evaluate network activity from the suspected employee and their assigned device(s), and use internal intrusion-detection software to capture activity on the suspected device(s).

Reference

In 2022 and 2023, the United States, along with foreign partners, issued public advisories regarding how North Korean IT workers operate and provided red-flag indicators and due-diligence measures for businesses to avoid hiring North Korean freelance developers. In May 2024, FBI provided further guidance regarding North Korean IT workers and their use of witting and unwitting US-based individuals.
