# North Korean hackers use AI-crafted identities to infiltrate Western businesses and fund weapons programmes



The infiltration of Western businesses by North Korean hackers, masquerading as job applicants, has become a pressing concern for cybersecurity experts. The campaign, dubbed Nickel Tapestry, has been in operation since 2016, with recent research revealing a marked increase in its scope and sophistication. According to the Sophos Counter Threat Unit's findings, these hackers have been targeting not only American firms but also expanding their efforts towards European and Japanese organizations. This shift in focus is likely tied to heightened vigilance among U.S. companies regarding such cyber threats.

At the heart of these operations is the use of advanced tools to craft convincing identities. These individuals have posed as professionals from various backgrounds—Japanese, Vietnamese, and American—using AI-generated resumes and cover letters to secure remote positions, often in sensitive sectors like defense, aerospace, and cybersecurity. Reports highlight that North Korean hackers are employing generative artificial intelligence (GenAI) to enhance their profiles, conduct mock interviews, and even manage communications, thus appearing more credible to potential employers. The utilisation of such technology reflects a significant evolution in their tactics, enhancing their chances of evading detection.

In addition to successfully securing employment, these hackers have also been engaged in more nefarious activities. A striking example includes their involvement in cryptocurrency scams, where they have stolen millions of dollars through malware deployed via recruitment scams. These efforts are reportedly linked to the Lazarus Group, known for orchestrating substantial cyberattacks that fund North Korea's weapons programme. It's alarming to note that the stolen wages from these fraudulent roles contribute not just to personal enrichment but directly support the state’s military ambitions.

Moreover, investigations have uncovered that many of these IT workers operate from China and Russia, using various means to mask their true identities, including false documentation. Previous reports from the FBI and the Department of Justice revealed that thousands of North Korean IT workers had funneled substantial sums into the regime's missile development efforts. The issue has gained momentum in the wake of the COVID-19 pandemic, which accelerated remote work trends, thereby providing more opportunities for infiltration.

To combat these sophisticated cyber activities, organisations are being urged to implement stringent verification processes for remote candidates. This includes thorough checks of resumes and personal details, and, where feasible, conducting in-person interviews. Experts recommend monitoring for signs of traditional insider threats, such as suspicious use of legitimate tools and unusual patterns of remote access.

The ramifications of these cyber operations extend beyond mere theft; they have the potential to compromise sensitive data and national security. For instance, North Korea's hacking efforts have previously targeted South Korean defense contractors, where malware was embedded in internal networks, leading to severe breaches of confidential information. Such incidents underscore the critical need for responsive and robust cybersecurity measures.

As the threat landscape continues to evolve, businesses must remain vigilant and proactive in safeguarding their systems against these insidious tactics. The convergence of AI technology and advanced cyber warfare will likely pose ongoing challenges, but by adopting comprehensive verification and monitoring strategies, organisations can better defend themselves against these sophisticated threats.

**Reference Map**

1. Paragraphs 1, 2, 6
2. Paragraph 3
3. Paragraphs 4, 5
4. Paragraph 2
5. Paragraph 3
6. Paragraph 4
7. Paragraph 5

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/these-north-korean-it-workers-have-been-infiltrating-western-businesses-since-2016> - Please view link - unable to able to access data
2. <https://www.reuters.com/sustainability/boards-policy-regulation/north-korean-cyber-spies-created-us-firms-dupe-crypto-developers-2025-04-24/> - North Korean cyber spies established fake companies, Blocknovas LLC in New Mexico and Softglide LLC in New York, to target cryptocurrency developers with malware, violating U.S. Treasury and UN sanctions. A third entity, Angeloper Agency, remains unregistered. These companies, created using false identities and addresses, aimed to attract unsuspecting job seekers and deliver malware to compromise crypto wallets and steal credentials. The operations are linked to the Lazarus Group, under North Korea’s Reconnaissance General Bureau. The FBI confirmed it seized the Blocknovas domain as part of a broader strategy to disrupt North Korean cyber activities, which it considers one of the most persistent national security threats. North Korea reportedly uses such cyber campaigns, including dispatching IT workers abroad and hacking, to financially support its nuclear program. Registration documents for the companies revealed false information and violated U.S. sanctions. Silent Push identified multiple victims from the Blocknovas campaign, with the hackers deploying known North Korea-linked malware strains to infiltrate systems and further propagate cyberattacks.
3. <https://apnews.com/article/f3df7c120522b0581db5c0b9682ebc9b> - Thousands of North Korean IT workers have secretly funneled millions of dollars from their wages to support North Korea's ballistic missile program, according to the FBI and Department of Justice. These IT workers, employed by US companies remotely, utilized false identities and were primarily stationed in China and Russia. They employed various methods, including paying Americans to use their home Wi-Fi, to masquerade as legitimate US-based workers. This scheme has generated significant funds for North Korea's weapons development and in some cases, allowed North Korean workers to infiltrate and steal data from these companies. The Justice Department has seized $1.5 million and 17 domain names as part of the investigation. The issue has escalated post-COVID-19 due to the increase in remote freelance employment. Companies are advised to rigorously verify the identity of remote workers to prevent such security breaches. The Justice Department continues to disrupt various schemes aiding North Korea's regime, which has focused increasingly on IT training and cyber-attacks.
4. <https://www.techradar.com/pro/security/north-korean-hackers-are-using-advanced-ai-tools-to-help-them-get-hired-at-western-firms> - New research from Okta reveals that North Korean hackers are leveraging generative artificial intelligence (GenAI) tools to infiltrate Western companies by securing remote technical jobs in sensitive sectors like defense, aerospace, and engineering. These hackers, backed by the Democratic People's Republic of Korea (DPRK), use GenAI to create credible resumes, cover letters, conduct mock interviews, manage communications, and maintain multiple job profiles—earning money for the regime. The schemes have become increasingly sophisticated, with a robust network of facilitators providing identity documents, technical infrastructure, and legitimate business fronts to support the deception. In addition to infiltrating firms, the hackers also target job seekers through fake interviews, using platforms like LinkedIn and Upwork to spread malware and steal data. The report urges job applicants and recruiters to be vigilant, as these cyber threats exploit both sides of the employment process.
5. <https://www.axios.com/2023/03/31/supply-chain-cyberattack-north-korea> - Thousands of companies using the 3CX video conferencing tool are now at risk due to an ongoing supply chain cyberattack carried out by North Korean hackers. This attack involves attaching malware to the Windows and MacOS versions of the application. The malware has been infecting users' devices since February. The precise number of affected customers remains unclear, but the attack represents a significant escalation in North Korea's hacking capabilities beyond typical email phishing and hacking crypto firms. Supply chain attacks are notably difficult to prevent due to businesses' limited ability to monitor their vendors' cybersecurity. 3CX CEO Nick Galea advises customers to uninstall the app and avoid using it unless absolutely necessary. It will take weeks to fully understand the attack's duration, impact, and the extent of access obtained by North Korea.
6. <https://www.reuters.com/technology/cybersecurity/north-korea-hacking-teams-hack-south-korea-defence-contractors-police-2024-04-23/> - For over a year, major North Korean hacking groups Lazarus, Kimsuky, and Andariel have been conducting extensive cyber attacks on South Korean defense companies, infiltrating their internal networks and stealing technical data, according to South Korean police. These groups, associated with North Korea's intelligence agencies, embedded malicious codes either directly in the defense companies' systems or through subcontractors, taking advantage of security lapses such as the use of identical passcodes for private and official email accounts. Investigations revealed the source IP addresses, signal re-routing architecture, and malware signatures used. The police have not disclosed the targeted companies or the specific nature of the stolen data. South Korea has become a significant global defense exporter, raising concerns about the potential impact of these cyber breaches. North Korean hacking activities have previously targeted South Korean financial institutions, news outlets, foreign defense companies, and the country's nuclear power operator. North Korea, however, denies involvement in hacking operations and crypto heists believed to fund its weapons programs.
7. <https://www.infosecurity-magazine.com/news/north-korea-it-worker-extort/> - The practice of North Korean nationals using stolen or falsified identities to obtain employment with Western companies under false pretenses has been documented in the US, UK and Australia for several years. This activity is primarily designed to generate revenue for the Democratic People’s Republic of Korea (DPRK), contributing to the regime’s weapons program. The Nickel Tapestry North Korean threat actor has historically been at the forefront of these schemes. Secureworks has recently observed an evolution in tactics that it believes have been used by the actor. One tradecraft of the group is to avoid using corporate laptops by rerouting them to facilitators at laptop farms. In some instances, the contractors requested permission to use a personal laptop instead of a company-issued device and displayed a strong preference for a virtual desktop infrastructure (VDI) setup. In one case where a ransom demand was issued, the attacker accessed company data using IP addresses within Astrill VPN address space and residential proxy addresses to mask the actual source IP address used for the malicious activity. Soon after the organization terminated the contractor’s employment due to poor performance, the company was sent a series of emails from an external Outlook email address. One of the emails included ZIP archive attachments containing proof of the stolen data, and another demanded a six-figure ransom in cryptocurrency to avoid publication of the stolen documents. The threat actors were also observed using Chrome Remote Desktop and AnyDesk for remote access. Historically, North Korean IT workers avoided enabling video during calls, sometimes claiming to experience issues with webcams on company-issued laptops. However, Nickel Tapestry appears to be using the free SplitCam software, advertised as a virtual video clone, enabling them to facilitate company calls. The threat actors have also been observed updating the bank account for receiving paychecks multiple times within a brief period. This includes the use of digital payment services to bypass traditional banking systems.