# North Korean hackers use AI and fake companies to infiltrate Western businesses since 2016



North Korean hackers have become a persistent threat in the global job market, employing a range of sophisticated tactics to infiltrate Western businesses. Recent research from Sophos's Counter Threat Unit has unveiled a coordinated campaign, dubbed the Nickel Tapestry, which has been operating since 2016. This campaign primarily targets European and Japanese firms, suggesting a shift from previous strategies that focused heavily on American companies, perhaps due to heightened scrutiny in the U.S.

The nefarious operations involve cybercriminals impersonating skilled professionals from various nationalities, including Japanese, Vietnamese, and American identities. These fraudulent applicants are not just aiming to secure employment; they use their positions to extract sensitive information and exfiltrate data. In critical sectors such as aerospace, defence, and cybersecurity, these infiltrations pose severe risks, especially as they exploit remote access technologies to conduct their activities undetected.

The underlying objectives of these operations are financial in nature, with the revenue generated from these roles reportedly funnelling back to support the Democratic People's Republic of Korea's (DPRK) state interests, including its controversial ballistic missile programme. Notably, the Lazarus Group, a key player in these campaigns, has amassed staggering revenues from various cyber scams—$1.5 billion, with a significant portion being irrecoverable funds linked to cryptocurrency operations.

Compounding the issue is the advancement in tactics employed by these hackers. A recent report highlights their use of generative artificial intelligence (GenAI) tools, which allow them to craft believable resumes, conduct mock interviews, and engage prospective employers convincingly. This evolution in approach not only enhances their credibility but also expands their reach, as they exploit platforms like LinkedIn and Upwork to trick both job seekers and employers into downloading malware or providing sensitive credentials.

In addition to elaborate impersonation schemes, North Korean operatives have established fake businesses, such as Blocknovas LLC and Softglide LLC, specifically targeting cryptocurrency developers. These companies utilized fictitious identities to bypass regulatory scrutiny and propagate malware attacks on unsuspecting victims, violating U.S. Treasury and United Nations sanctions in the process. The FBI has intervened to seize assets linked to these operations, underscoring the national security implications of these persistent cyber incursions.

Reports indicating that thousands of remote IT workers from North Korea are masquerading as employees in U.S., UK, and Australian companies reveal a growing trend in the utilisation of false identities and fictitious employment credentials. These strategies have continuously evolved, with indications that some workers even accessed their jobs using stolen credentials from established U.S. residents or employed questionable tactics to emulate local workers.

As remote work becomes increasingly common, organisations must adopt robust verification measures to guard against these threats. Experts warn that verifying identities, scrutinising CVs, and even conducting in-person interviews can help mitigate the risks posed by these sophisticated cybercriminals. Additionally, companies are encouraged to monitor for strange behaviour patterns typical of insider threats and to enforce strict cybersecurity protocols to safeguard sensitive information.

The evolving landscape of North Korean cyber activities illustrates the intricate interplay between technology, employment, and national security. With state-sponsored groups leveraging advanced tools to infiltrate legitimate workplaces, the implications for businesses and governments alike are profound. As the global workforce increasingly shifts to remote models, constant vigilance will be paramount in preventing these unscrupulous schemes from undermining cybersecurity efforts and national integrity.

### Reference Map

Paragraph 1: [[1]](https://www.techradar.com/pro/security/these-north-korean-it-workers-have-been-infiltrating-western-businesses-since-2016)Paragraph 2: [[1]](https://www.techradar.com/pro/security/these-north-korean-it-workers-have-been-infiltrating-western-businesses-since-2016), [[3]](https://apnews.com/article/f3df7c120522b0581db5c0b9682ebc9b)Paragraph 3: [[1]](https://www.techradar.com/pro/security/these-north-korean-it-workers-have-been-infiltrating-western-businesses-since-2016), [[3]](https://apnews.com/article/f3df7c120522b0581db5c0b9682ebc9b)Paragraph 4: [[2]](https://www.reuters.com/sustainability/boards-policy-regulation/north-korean-cyber-spies-created-us-firms-dupe-crypto-developers-2025-04-24/), [[4]](https://www.techradar.com/pro/security/north-korean-hackers-are-using-advanced-ai-tools-to-help-them-get-hired-at-western-firms)Paragraph 5: [[2]](https://www.reuters.com/sustainability/boards-policy-regulation/north-korean-cyber-spies-created-us-firms-dupe-crypto-developers-2025-04-24/), [[6]](https://www.infosecurity-magazine.com/news/north-korea-it-worker-extort/)Paragraph 6: [[3]](https://apnews.com/article/f3df7c120522b0581db5c0b9682ebc9b), [[7]](https://www.securityweek.com/north-korean-fake-it-workers-extort-employers-after-stealing-data/)Paragraph 7: [[4]](https://www.techradar.com/pro/security/north-korean-hackers-are-using-advanced-ai-tools-to-help-them-get-hired-at-western-firms), [[6]](https://www.infosecurity-magazine.com/news/north-korea-it-worker-extort/)

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

## Bibliography

* <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
* <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.
* <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.
* <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.
* <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.
* <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.
* <https://www.securityweek.com/north-korean-fake-it-workers-extort-employers-after-stealing-data/> - Hundreds of companies in the US, UK, and Australia have fallen victim to the North Korean fake IT worker schemes, and some of them received ransom demands after the intruders gained insider access, Secureworks reports. Using stolen or falsified identities, these individuals apply for jobs at legitimate companies and, if hired, use their access to steal data and gain insight into the organization’s infrastructure. More than 300 businesses are believed to have fallen victim to the scheme, including cybersecurity firm KnowBe4, and Arizona resident Christina Marie Chapman was indicted in May for her alleged role in assisting North Korean fake IT workers with getting jobs in the US. According to a recent Mandiant report, the scheme Chapman was part of generated at least $6.8 million in revenue between 2020 and 2023, funds likely meant to fuel North Korea’s nuclear and ballistic missile programs. The activity, tracked as UNC5267 and Nickel Tapestry, typically relies on fraudulent workers to generate the revenue, but Secureworks has observed an evolution in the threat actors’ tactics, which now include extortion.