# North Korean hackers use fake US companies to target cryptocurrency developers



North Korean hackers have been found to be using a novel approach to infiltrate the cryptocurrency industry in the United States, according to cybersecurity firm Silent Push. The group, linked to the notorious Lazarus Group hacking collective, quietly established companies in New York and New Mexico under false identities as part of an elaborate campaign targeting crypto developers.

Silent Push revealed on Thursday that the North Korean-backed unit had registered two businesses, Blocknovas and Softglide, to create legitimate-seeming fronts for their operations. These companies were set up with fictitious names and addresses to lend credibility to their fraudulent activities. Notably, Blocknovas was reportedly the most active, while its listed address in South Carolina turned out to be an empty lot. Softglide was registered at a tax office in Buffalo, New York, further illustrating the deceptive nature of these entities.

The hacking group employed a sophisticated recruitment strategy designed to ensnare victims within the crypto community. By creating fake Linkedin-style profiles and job advertisements, the hackers invited potential targets to participate in seemingly genuine interviews. However, the recruitment process was a ruse to trick candidates into downloading malware disguised as tools necessary for job applications. This malware has been linked to at least three different virus strains previously associated with North Korean cyber operations, capable of stealing data, granting remote access, and facilitating further cyberattacks such as spyware or ransomware deployment.

Kasey Best, director of threat intelligence at Silent Push, remarked to Coindesk, “This is a rare example of North Korean hackers actually managing to set up legal corporate entities in the US in order to create corporate fronts used to attack unsuspecting job applicants.” The implications of this strategy highlight the evolving tactics used by nation-state cyber threat actors to exploit the growing interest and talent pool within the cryptocurrency sector.

The United States Federal Bureau of Investigation (FBI) has responded to these activities by seizing the domain for Blocknovas. According to a notice posted on the site, the domain was taken down “as part of a law enforcement action against North Korean cyber actors who utilised this domain to deceive individuals with fake job postings and distribute malware.”

North Korean hacking groups have a documented history of stealing billions in cryptocurrency through various cyberattack methods, and the discovery of these front companies represents a significant expansion in their operational tactics. The use of legitimate-appearing corporate fronts in the US marks a new level of sophistication and underscores the persistent threat posed by state-backed cybercriminal actors within the crypto ecosystem.

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

## Bibliography

1. <https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation> - This article supports the claim that North Korean hackers, particularly the Lazarus Group, have been involved in significant cryptocurrency thefts, including the ByBit heist. It highlights North Korea's use of hacking for financial gain and its implications on the global crypto market.
2. <https://thehackernews.com/2025/04/dprk-hackers-steal-137m-from-tron-users.html> - This report corroborates the involvement of North Korean hackers in stealing millions of dollars in cryptocurrency through various methods, including phishing attacks.
3. <https://www.ic3.gov/psa/2025/psa250226> - The FBI's PSA verifies that North Korea was responsible for the $1.5 billion Bybit hack, demonstrating the scale of cyber threats posed by North Korean hackers and the FBI's response to these activities.
4. <https://www.nknews.org/2024/12/north-korean-hackers-stole-308m-from-japanese-crypto-exchange-us-and-japan-say/> - This article documents North Korean hackers' involvement in stealing substantial amounts of cryptocurrency from various exchanges, further highlighting their tactics.
5. <https://therecord.media/us-japan-south-korea-urge-crypto-industry-of-north-korean-hackers> - This piece details the joint international efforts to combat North Korean hacking activities targeting the cryptocurrency industry and emphasizes the threat these actors pose to global financial stability.
6. <https://www.coindesk.com/> - This website may provide additional context or reports on North Korean hacking activities within the cryptocurrency sector, including Silent Push's findings mentioned in the article.
7. <https://www.coindesk.com/tech/2025/04/25/north-korean-hackers-targeting-crypto-developers-with-u-s-shell-firms> - Please view link - unable to able to access data