2025-04-26 - News Report

# North Korean Hackers Spread Malware via Fake Crypto Firms and Job Interview Lures

Summary:  
 North Korea-linked threat actors have set up front companies to distribute malware during the fake hiring process. Contagious Interview is one of the several job-themed social engineering campaigns orchestrated by North Korea. The attacks lead to the deployment of a JavaScript stealer and loader called BeaverTail, which is then used to drop a Python backdoor referred to as InvisibleFerret. The use of front companies for malware propagation marks a new escalation for the threat actors, who have been observed using various job boards to lure victims. The FBI seized the BlockNovas domain as part of a law enforcement action against North Korean cyber actors. The domain was used to "deceive individuals with fake job postings and distribute malware" North Korean threat actors are also using artificial intelligence (AI)-powered tools like Remaker to create profile pictures. These efforts have dual motivations, designed to steal sensitive data and pursue financial gain by funneling a chunk of the monthly salaries back to the Democratic People's Republic of Korea (DPRK) The company will not reveal how much money it will make from the deal. The deal is expected to be worth more than $1 billion, the company said. It will be available in the U.S. and Europe in the coming months, according to the company. The company has not yet revealed how much the deal will earn it, but said it will be in the region of $1.5 billion to $2 billion. It is not yet clear if the company will be able to make a profit from the sale of the business.

Link: https://thehackernews.com/2025/04/north-korean-hackers-spread-malware-via.html