FBI links North Korean hackers to $308 million crypto heist

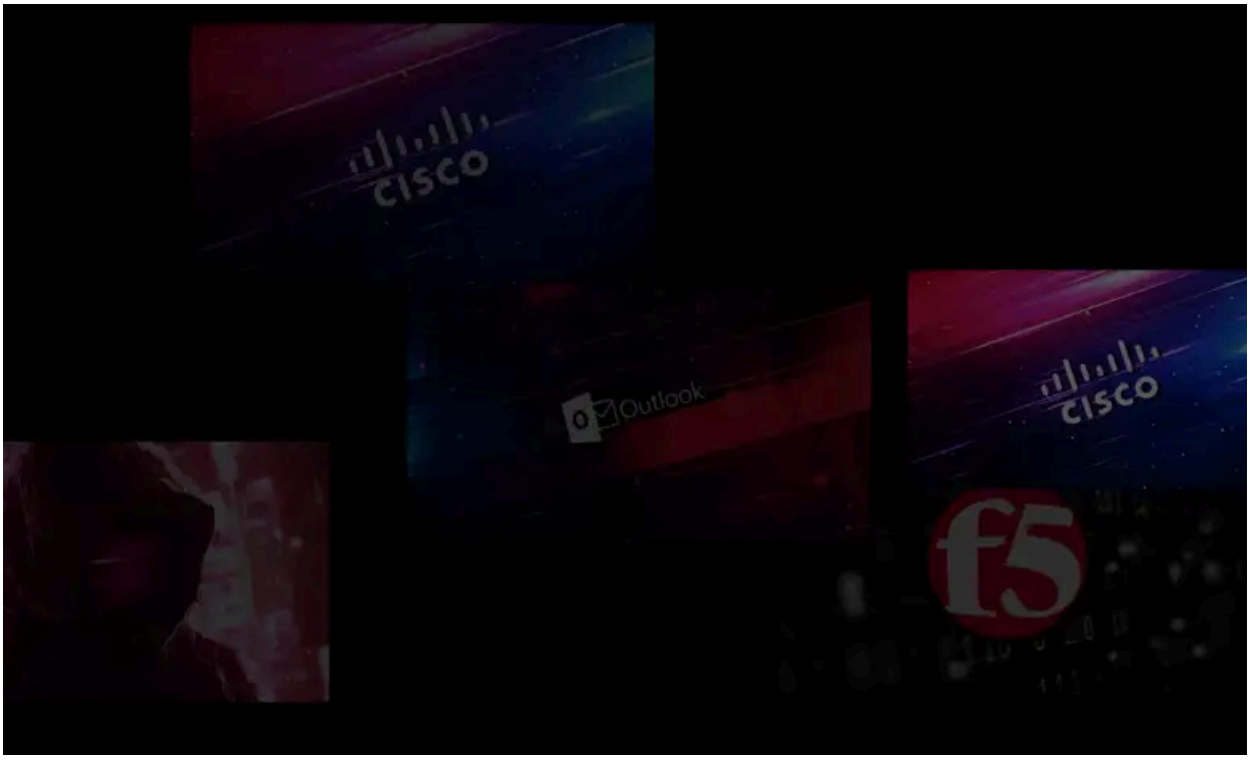
By Bill Toulas

Published: 2024-12-24 · Archived: 2026-04-02 11:41:29 UTC

The North Korean hacker group ‘TraderTraitor’ stole $308 million worth of cryptocurrency in the attack on the Japanese exchange DMM Bitcoin in May.

In a short post, the FBI attributed the attack to the state-affiliated threat actor TraderTraitor, also tracked as Jade Sleet, UNC4899, and Slow Pisces.

The crypto heist occurred in May 2024 and forced the platform to restrict account registration, cryptocurrency withdrawals, and trading until the completion of the investigations.


cisco
Outlook
cisco
f5

Earlier this week, a report from blockchain intelligence firm Chainalysis attributed the attack to North Korean threat actors but did not share any specific details.

Attack chain

In a short announcement, the FBI says that TraderTraitor's attack on DMM Bitcoin started in late March 2024, when one of the attackers pretended to be a legitimate recruiter on LinkedIn and approached an employee of Ginco, a Japanese enterprise cryptocurrency wallet software company.

The hacker sent the Ginco employee, who had access to his employer's wallet management system, a job proposal involving a pre-employment test on GitHub. This tactic has been popular with North Korean threat groups this year [1, 2].

The victim received a piece of malicious Python code to copy to their personal GitHub page in order to carry out the conduct the test. The code, however, compromised the computer and allowed TraderTraitor to infiltrate Ginco and then move laterally to DMM.

"After mid-May 2024, TraderTraitor actors exploited session cookie information to impersonate the compromised employee and successfully gained access to Ginco's unencrypted communications system," explains the FBI.

"In late May 2024, the actors likely used this access to manipulate a legitimate transaction request by a DMM employee, resulting in the loss of 4,502.9 BTC, worth $308 million at the time of the attack," the agency says.

U.S. authorities have been monitoring the activity of TraderTraitor since 2022 when the threat actor started to target the blockchain space with fake apps.

In 2023, GitHub warned of a social engineering campaign conducted by the particular threat actors on the platform, targeting the accounts of developers in the blockchain, cryptocurrency, online gambling, and cybersecurity sectors.

Later, the FBI warned that TraderTraitor was preparing to cash out 1,580 Bitcoin (valued at the time at around $41 million) stolen from various sources that year.

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
