BitoPro exchange links Lazarus hackers to $11 million crypto heist

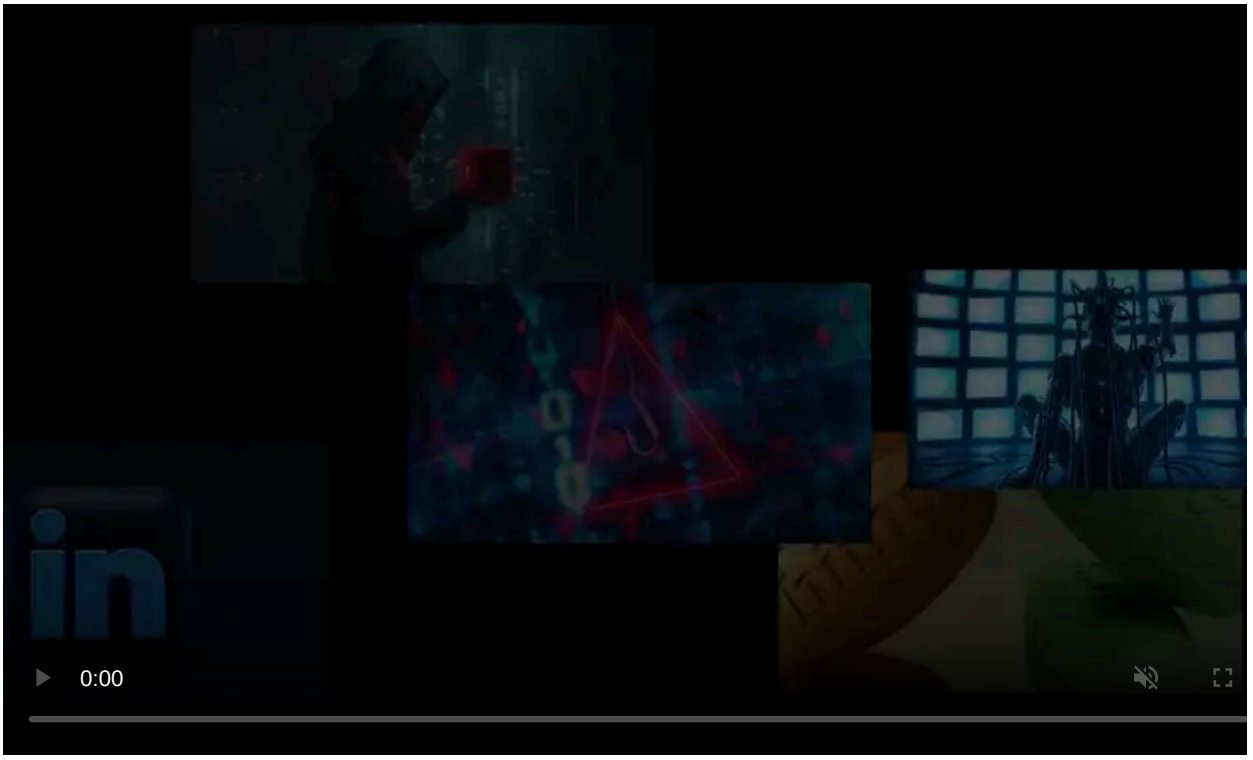
By Bill Toulas

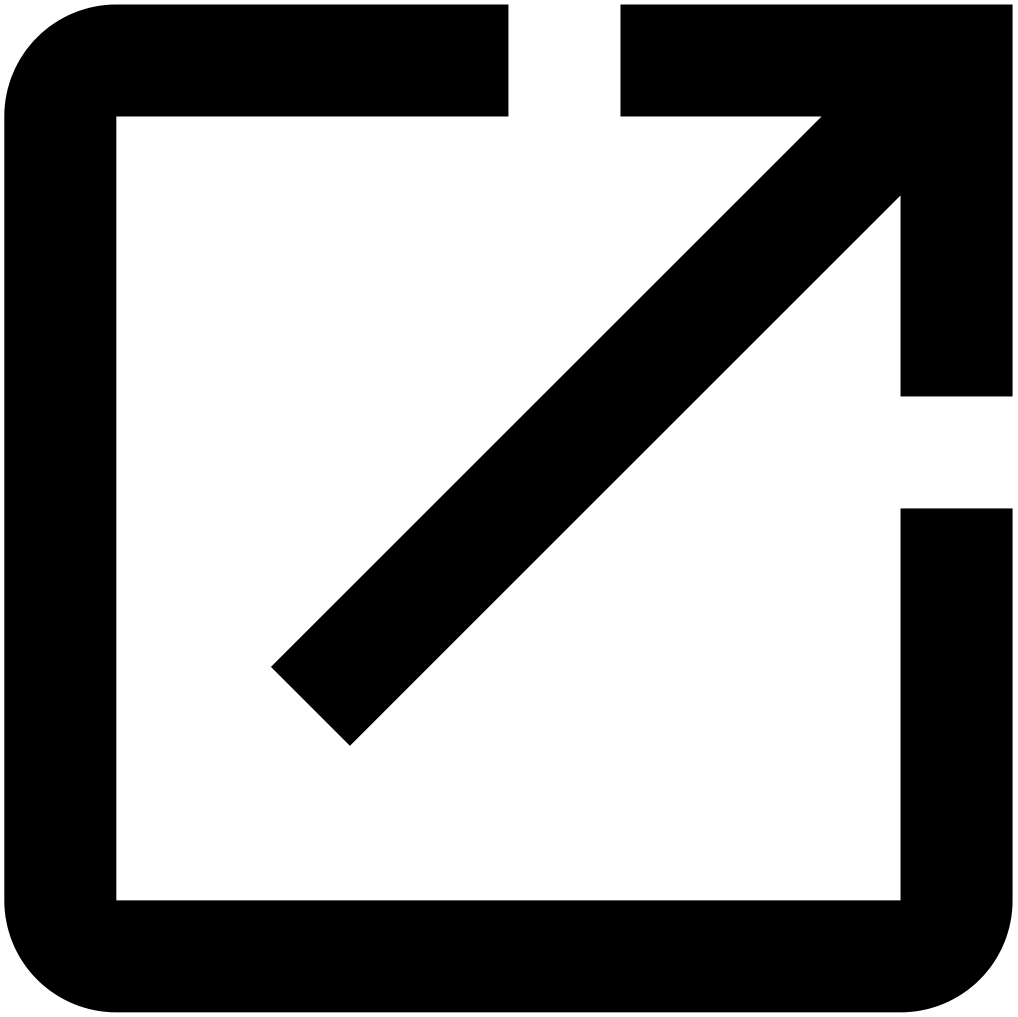
Published: 2025-06-20 · Archived: 2026-04-05 18:37:51 UTC

The Taiwanese cryptocurrency exchange BitoPro claims the North Korean hacking group Lazarus is behind a cyberattack that led to the theft of $11,000,000 worth of cryptocurrency on May 8, 2025.

The company has attributed the attack to Lazarus based on the evidence recovered from its internal investigations. It notes that the attack patterns and methodology closely resemble those used in past cyberattacks.

"The attack methodology bears resemblance to patterns observed in multiple past international major incidents, including illicit transfers from global bank SWIFT systems and asset theft incidents from major international cryptocurrency exchanges," reads the announcement.


0:00



"These attacks are attributed to the North Korean hacking organization Lazarus Group."

BitoPro is a cryptocurrency exchange that caters primarily to Taiwanese users, supporting fiat deposits and withdrawals in TWD and a selection of crypto assets.

It has over 800,000 registered users and a daily trading volume of roughly $30 million.

On May 8, 2025, during a hot wallet system update, hackers performed unauthorized withdrawals from an old hot wallet across multiple blockchains, including Ethereum, Tron, Solana, and Polygon.

After the theft, stolen funds were laundered through DEXs and mixers like Tornado Cash, ThorChain, and Wasabi Wallet.

BitoPro was slow in admitting the incident, only confirming it publicly on June 2, noting that all operations were unaffected and impacted hot wallets were replenished by available reserves.

The investigation into the hack now confirmed that there was no internal involvement, even though the attackers launched a social engineering attack and implanted malware on the device of an employee managing cloud operations.

Through this infection, the attackers hijacked AWS session tokens to bypass multi-factor authentication (MFA) and gain control over BitPro's cloud infrastructure.

Next, the command-and-control (C2) server delivered commands to the implant that injected scripts into the hot wallet host as the attack was being prepared.

When the wallet was upgraded and assets transferred, the attackers stole crypto while simulating normal operational behavior to evade immediate detection.

Once BitoPro detected the compromise, they shut down the hot wallet system and rotated the cryptographic keys. However, roughly $11 million worth of cryptocurrency had already been stolen.

The company informed the applicable authorities and engaged with an external cybersecurity expert to investigate the incident, a process completed on June 11.

The North Korean Lazarus group is notorious for targeting cryptocurrency and decentralized finance entities. The hacking group is believed to be responsible for record-breaking digital asset heists, most recently, the $1.5 billion theft from Bybit.

Source: https://www.bleepingcomputer.com/news/security/bitopro-exchange-links-lazarus-hackers-to-11-million-crypto-heist/