CoinsPaid blames Lazarus hackers for theft of $37,300,000 in crypto

By Bill Toulas

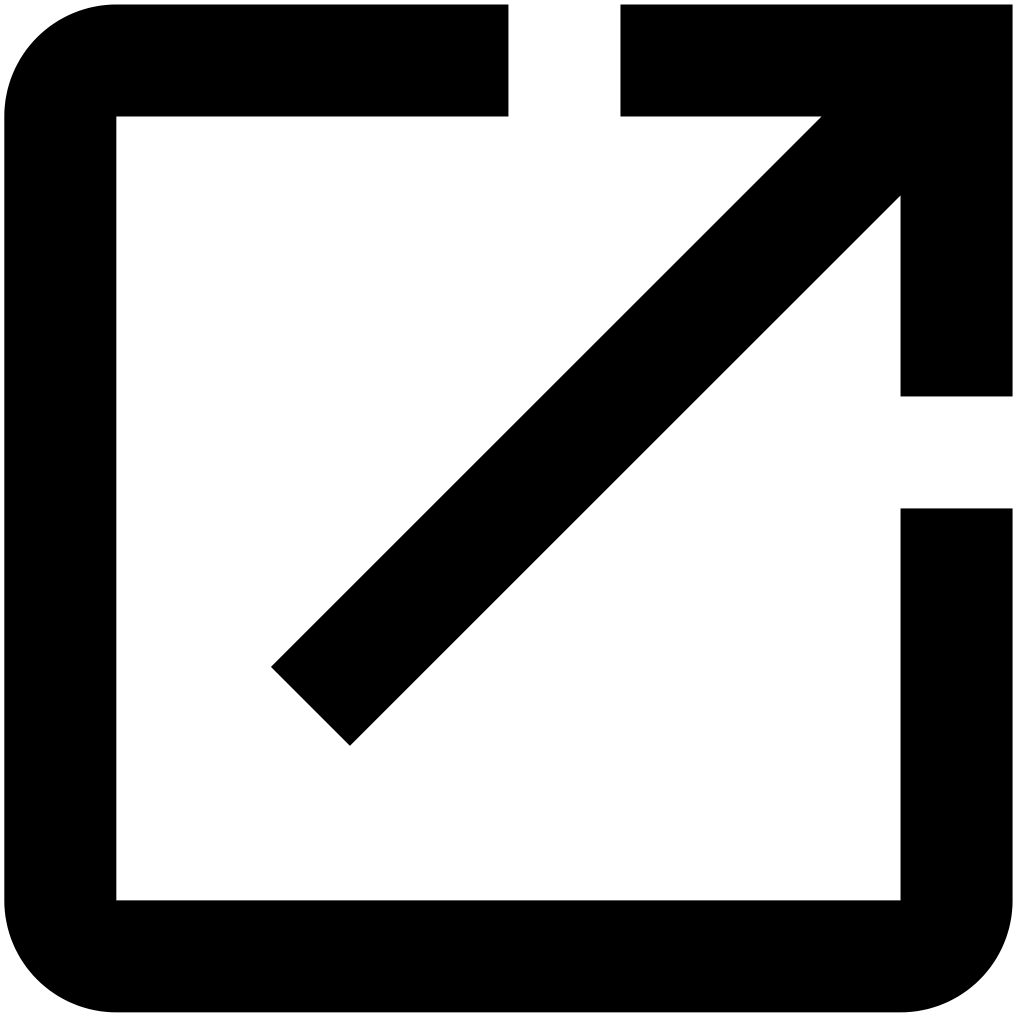
Published: 2023-07-27 · Archived: 2026-04-05 14:22:45 UTC

Estonian crypto-payments service provider CoinsPaid has announced that it experienced a cyber attack on July 22nd, 2023, that resulted in the theft of $37,200,000 worth of cryptocurrency.

Despite the significant economic damage and the adverse impact on the payment platform's availability, the company highlights that client funds are safe and fully available, so the incident does not have a material impact on the firm's business.

CoinsPaid is blaming the attack on the North Korean hacking group Lazarus, saying that the sophisticated financially-motivated state-backed actor was aiming for a higher cash-out.


DIE LINKE.
0:00



"We believe Lazarus expected the attack on CoinsPaid to be much more successful," reads the CoinsPaid press release.

"In response to the attack, the company's dedicated team of experts has worked tirelessly to fortify our systems and minimize the impact, leaving Lazarus with a record-low reward."

However, CoinsPaid has not shared any information on how they linked the attack to Lazarus, and BleepingComputer has not been able to confirm these statements independently.

The firm says services are gradually returning to normal as the engineers carefully restore them to a new, secure environment.

CoinsPaid expects the hit in its revenue to be fully offset in the following period, as it's poised to rebound swiftly, maintaining delivery of its services without further disruptions.

The company's CEO, Max Krupyshev, also stated that Chainalysis, Binance, Crystal, Match Systems, Staked.us, OKCoinJapan, and Valkyrieinvest are helping in the investigation. At the same time, the Estonian law enforcement authorities have also been notified and are participating in the tracking effort.

"We have no doubt the hackers won't escape justice," added Max Krupyshev.

Just yesterday, blockchain analysts blamed Lazarus for a $60,000,000 cryptocurrency heist impacting the payment processing platform Alphapo, that's still recovering from the incident.

Although no concrete proof of the North Korean group's involvement in that attack has been published yet, the incident reportedly carried distinct hallmarks associated with Lazarus.

Considering the similarity in the business type of the two firms, Alpapho and CoinsPaid, the Lazarus Group may have focused on cryptocurrency payment processors in this recent attack wave.

Previously, the threat actor stole $35 million from Atomic Wallet, $100 million from Harmony Horizon, and a record-breaking $617 million from the Axie Infinity blockchain-based game.

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.
