Lazarus hackers linked to $60 million Alphapo cryptocurrency heist

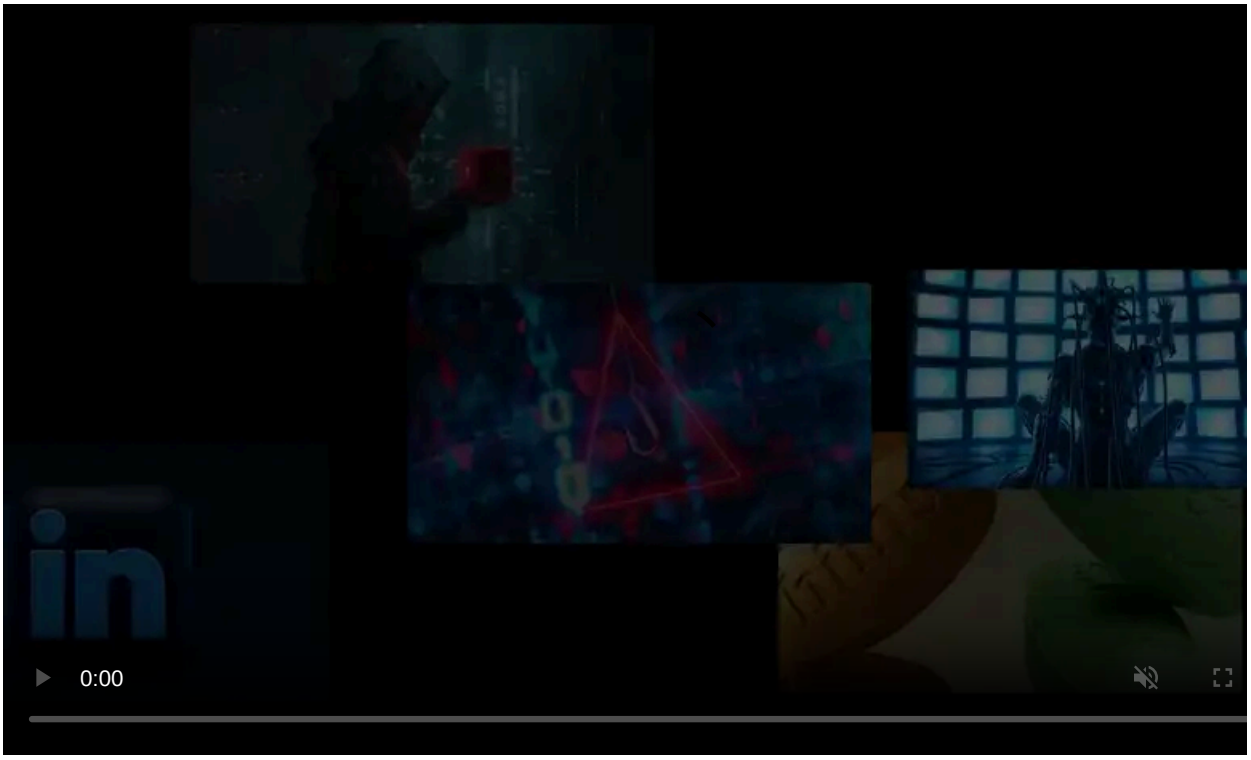
By Bill Toulas

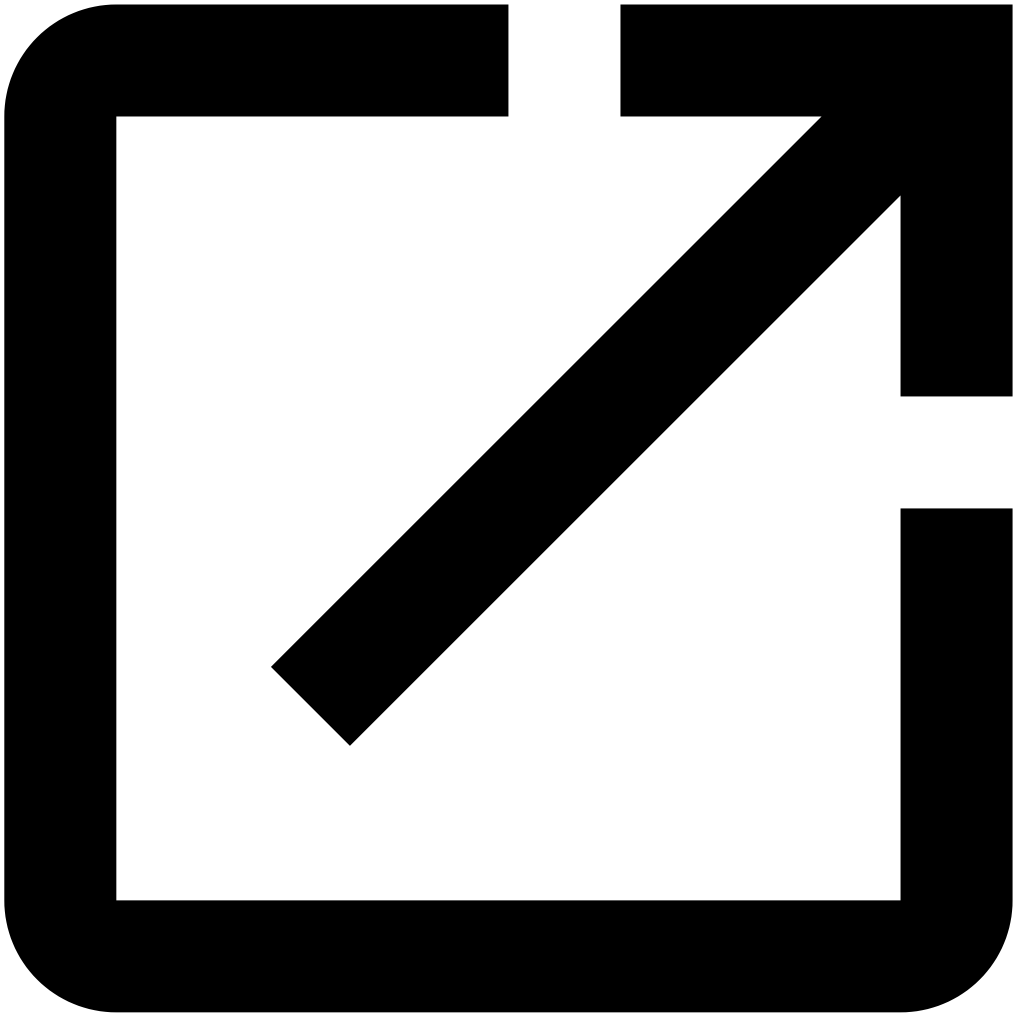
Published: 2023-07-26 · Archived: 2026-04-05 17:36:48 UTC

Blockchain analysts blame the North Korean Lazarus hacking group for a recent attack on payment processing platform Alphapo where the attackers stole almost $60 million in crypto.

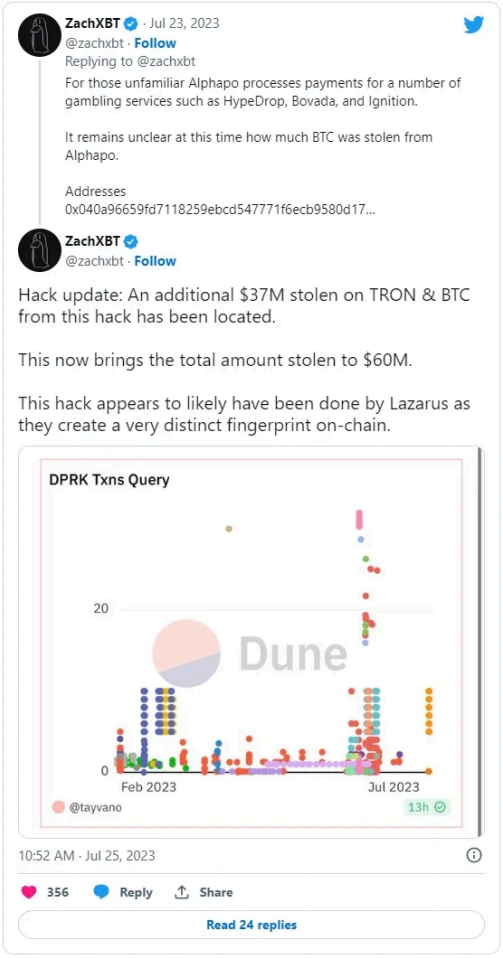
Alphapo is a centralized crypto payment provider for gambling sites, e-commerce subscription services, and other online platforms, which was attacked on Sunday, July 23rd, with the initial stolen amount estimated to be $23 million.

This theft included over 6 million USDT, 108k USDC, 100.2 million FTN, 430k TFL, 2.5k ETH, and 1,700 DAI, all drained from hot wallets, likely made possible by a leak of private keys.


0:00



Well-known crypto chain investigator "ZackXBT" warned yesterday that the attackers also drained an additional $37M of TRON and BTC, as seen on Dune Analytics data, raising the total amount stolen from Alphapo to $60,000,000.



Moreover, ZackXBT claimed that the attack appears to carry characteristics of a Lazarus heist and backed the claim by saying that Lazarus creates "a very distinct fingerprint on-chain," but no further details were provided.

The Lazarus Group is a North Korean threat actor with ties to the North Korean government, previously linked to the $35 million Atomic Wallet heist, the $100 million Harmony Horizon hack, and the $617 million Axie Infinity theft.

Typically, Lazarus uses fake job offers to lure employees of crypto firms to open infected files, compromising their computers and losing account credentials.

This creates an attack avenue into the victim's employer network, where they can get unauthorized access and meticulously plan and execute attacks costing millions of dollars.

Analysts tracking the movement of the stolen funds to cryptocurrency exchanges report seeing laundering attempts through Bitget, Bybit, and others. At the same time, Lazarus is also known for using small cryptocurrency mixing services.

Dave Schwed, COO of blockchain security company Halborn, told BleepingComputer that the attackers likely stole private keys, allowing access to the wallets.

> While we lack specifics, it seems that the alleged "hack" likely pertains to the theft of private keys. This inference comes from observing the movement of funds from independent hot wallets and the sudden halting of trading. Moreover, the subsequent transactions have led ZachXBT, a renowned "on-chain sleuth", to surmise that North Korea's notorious Lazarus group is the perpetrator of this attack.
>
> Given their history of similar exploits, I find myself agreeing with this theory. - D. Schwed

At this time, BleepingComputer has not been able to independently confirm the involvement of the North Korean threat group in the Alphapo hack with blockchain analysis firms or law enforcement agencies.

We will update this post as soon as we know more.

Source: https://www.bleepingcomputer.com/news/security/lazarus-hackers-linked-to-60-million-alphapo-cryptocurrency-heist/