

CoinStats says North Korean hackers breached 1,590 crypto wallets

By **Bill Toulas**



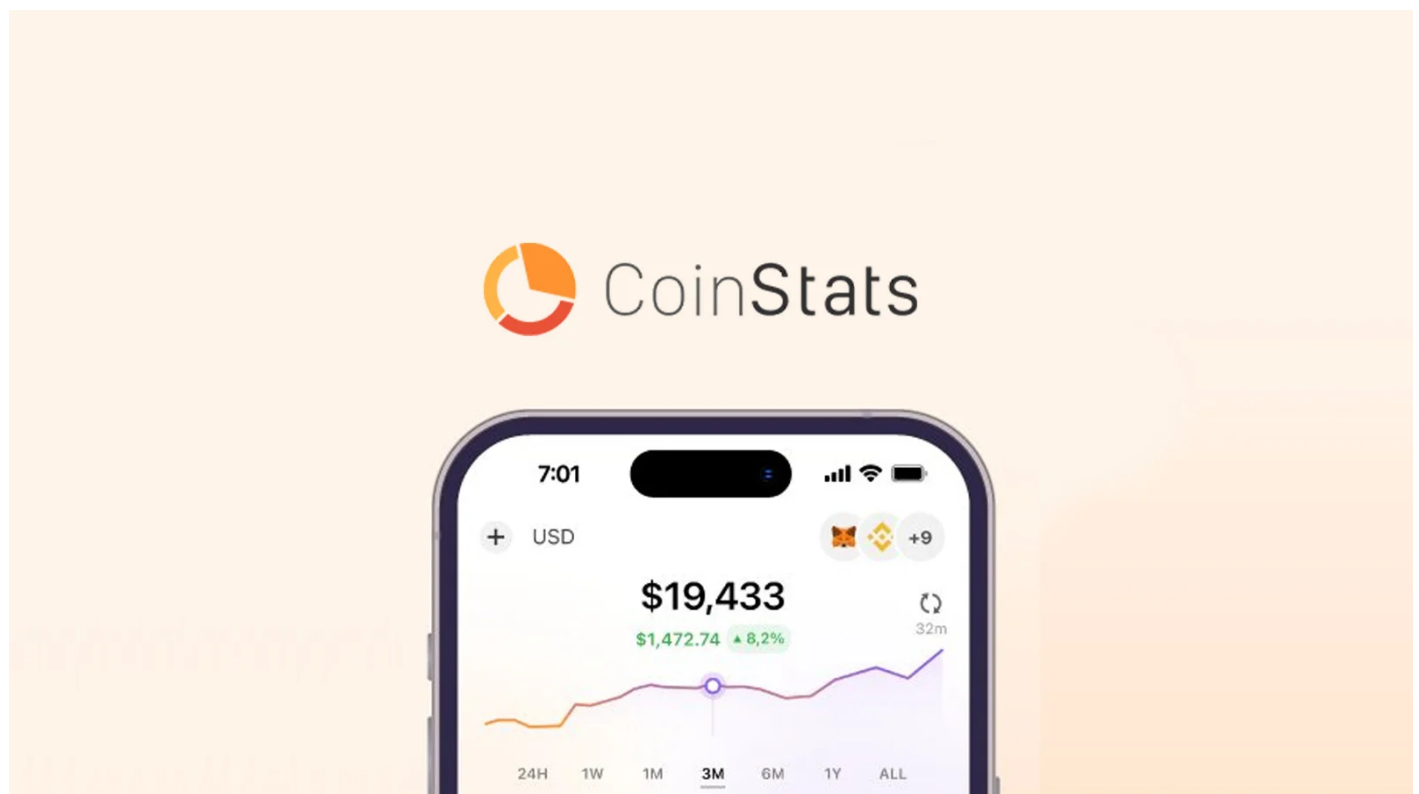
June 24, 2024



10:56 AM



0



CoinStats suffered a massive security breach that compromised 1,590 cryptocurrency wallets, with the attack suspected to have been carried out by North Korean threat actors.

CoinStats is a comprehensive cryptocurrency portfolio management app with 1,500,000 users. It is used for investment tracking, real-time data, news aggregation, and custom alerts. It also allows users to create CoinStats wallets, which are hosted by the platform.

For users who want to use the portfolio management features, the platform requires read-only access to connected external crypto wallets and were not affected by the breach.

However, those users who hosted their wallets on CoinStats were potentially impacted by the hack.

In an announcement on X yesterday, CoinStats told users they suffered a cyberattack that affected 1,590, or 1.3%, of all hosted wallets on the platform.

The company shared a list of impacted wallets on [this spreadsheet](#), but some [users reported](#) that funds were stolen from wallets that were not on this list. Therefore, the actual scope of the incident might be more significant than what CoinStats has verified.



Those who find their wallet address on the list and still contain funds are urged to transfer them immediately to an external wallet.

While the hack is underway, the CoinStats website and the app remain unavailable as the company investigates and mitigates the attack.

The attack did not impact users' connected wallets and centralized exchanges, so it's safe for people to continue using those.

Although the investigation is ongoing, CoinStats' CEO stated on X that they hold significant evidence suggesting that North Korean hackers carried out the attack, sharing a [CISA document](#) about the North Korean Lazarus hacking group.



narek

@narek_gevorgyan · Follow



We also have a significant evidence to assume that attack was a part of this group of hacks, described by FBI report with ties to North Korea cisa.gov/sites/default/...

9:49 AM · Jun 23, 2024



The Lazarus Group is believed to be a state-sponsored hacking group notorious for carrying out massive crypto heists over the years, targeting cryptocurrency platforms.

In late 2023, Recorded Future estimated that North Korean state-backed hackers [had stolen \\$3 billion](#) worth of crypto since January 2017, which equates to roughly \$500,000,000/year.

Scammers are already attempting to take advantage of the CoinStats breach by promoting fake refund programs in responses under the official announcement on X, using unverified accounts with typosquatting handles, such as '@CoinStals'.



Fake refund announcement by scammers

Source: BleepingComputer

The scammers attempt to trick users into visiting a cloned site that requests them to connect their wallets to receive a refund, which is then drained of all assets.

At the time of writing this, the official CoinStats platform has not announced a refund program, so all related claims should be seen as scams and ignored.

[COINSTATS](#)[CRYPTO WALLET](#)[CRYPTOCURRENCY](#)[CRYPTOTHEFT](#)[MONEY](#)[NORTH KOREA](#)



BILL TOULAS  

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

[< PREVIOUS ARTICLE](#)

[NEXT ARTICLE >](#)