



THE BYBIT HEIST

098 / 21 FEB 2025 / BYBIT / RARE

THE APPROVAL WAS THE DISGUISE

The courier has the right badge, the case carries Ethereum's symbol, and three green checks clear the doorway. Everything looks authorised. Only the dark reflection gives the game away, turning an ordinary departure into something far more sinister.

On 21 February 2025, Bybit was arranging a routine transfer from an Ethereum cold wallet to a warm wallet. Attackers had compromised the Safe web interface used in the signing process. What appeared to be a familiar transfer concealed a transaction that would hand them control of the wallet.

Investigators found malicious code in the interface resources loaded by the three signers. Their approvals authorised a change to the wallet's controlling code, after which the attackers could move its assets without further multisignature approval. Approximately \$1.5 billion in virtual assets was stolen. The failure lay in the compromised signing workflow, rather than Ethereum's consensus mechanism.

On 26 February, the FBI attributed the theft to North Korean actors it calls TraderTraitor. The card stays with the earlier moment of deception: a guard sees a permitted departure while the glass reveals another intention. The Ethereum-marked case carries the value out through a doorway glowing green.

DETAILS IN THE ART

01 The face in the glass

The plausible courier becomes a darker figure in the reflection. That mismatch echoes the gap between the transfer shown to signers and the transaction they actually authorised.

02 Three green checks

Three green checks echo the three signers involved in the transaction. Each light appears reassuring, even though all three approvals belonged to the same deceptive process.

03 The Ethereum case

The purple diamond marks the assets leaving the Ethereum wallet. Its reflected counterpart follows the same cargo into the scene's darker version.

04 The cleared doorway

A guard remains at his desk beside the open entrance. The badge and approval lights make the courier's exit look routine; the BYBIT sign fixes the date at 21 FEB 2025.

SOURCE & ART NOTE

Sources: Sygnia, investigation findings; Bybit, incident timeline; CertiK, transaction analysis; FBI, 26 February attribution. The courier, guard, vault and reflection are fictional metaphors for a deceptive signing interface, not a physical theft or an accusation against an employee. The caption is editorial.