Cryptocurrency Forensics Report

Generated on April 09, 2025

Executive Summary

This report investigates Ethereum address 0x2bf916f8169ed2a77324d3e168284fc252ae4087, which demonstrates behavior typical of MEV-based fund manipulation or laundering. Using Breadcrumbs' visualization and fund flow tracing, it is evident that this address is engaging in repeated, high-volume interactions with known MEV bots, validators, and routing hubs - potentially indicating exploit-related fund distribution.

Target Address

Address: 0x2bf916f8169ed2a77324d3e168284fc252ae4087

Type: Smart Contract

Transactions: 31,196 in | 2,053 out

Suspicious Activity: Repeated high-volume inbound/outbound transactions, obfuscation patterns, and interactions with high-risk entities.

Key Observations

1. Repeated Transfers to Funneling Hub

- Address: 0x000000000000000675d852c8638df22727949052b1208

- Function: Appears to act as a relay or obfuscation point

- Stats: 94 incoming TXs | 465 outgoing TXs | Total volume ~11.2 ETH

- Timeline: Jan 7 - Apr 9, 2025

2. Connections to MEV Bots & Builders

- Titan Builder (0x4438...59f7)

- MEV Bot: 0x0000...0000

- Symbolic Capital Partner MEV Bot Deployer

- Proposer Fee Recipient

- Lido Execution Layer Rewards Vault

3. Indicators of Malicious or Grey-Hat Behavior

- Batch TXs from a single smart contract to multiple endpoints

- Distribution to validator/proposer fee addresses

- Pattern suggests MEV sandwich/front-running attack proceeds distribution or post-exploit fund obfuscation

Tools Used

- Breadcrumbs.app - fund flow, node tracing, risk analysis

- Ethereum smart contract behavior review

- Label correlation with known infrastructure (Lido, MEV bots, validators)

Risk Classification

- MEV Involvement: Confirmed

- Fund Laundering: Highly Likely

- Exploit Routing: Possible

- Obfuscation Tactics: Confirmed

Recommended Action

1. Chainabuse.com - Public reporting for wallet addresses

2. ScamSniffer.io - Report phishing or malicious contracts

3. Etherscan Abuse Report - Flag malicious smart contracts

4. Institutional Escalation - Chainalysis, TRM Labs, or Indian Cybercrime Reporting Portal (IC3)