TREQORA — Cryptocurrency Recovery Case Study

Cross-Chain Theft Investigation & Asset Freeze Coordination

Case Summary

A client lost $112,000 in a sophisticated phishing attack where assets were rapidly transferred across BTC, ETH, and BNB networks. Funds were chain-hopped, routed through mixers, and deposited into a centralized exchange.

Investigation Approach

Treqora performed a comprehensive multi-chain forensic investigation, tracking assets across multiple blockchain networks and identifying critical exchange touchpoints for intervention.

Recovery Success

Through coordinated exchange freeze efforts and advanced blockchain forensics, Treqora successfully recovered 61% of the total stolen assets, securing $68,500 for the client.

This anonymized case study from 2024 demonstrates the effectiveness of rapid response and sophisticated blockchain forensics in cryptocurrency asset recovery. The investigation showcased Treqora's capabilities in handling complex, multi-jurisdictional crypto theft cases involving advanced obfuscation techniques.

Client Profile & Attack Vector

The Victim

The client is an individual cryptocurrency holder who unknowingly interacted with a phishing website that mimicked a legitimate crypto service platform. The sophisticated attack exploited trust in familiar interfaces to gain unauthorized access.

Within minutes of the compromise, the attacker gained complete wallet access and initiated a rapid drainage of assets, demonstrating the speed and efficiency of modern cryptocurrency theft operations.

Attack Methodology

The phishing attack employed several advanced techniques to maximize theft and minimize traceability:

- Sophisticated website mimicry of legitimate crypto services
- Rapid asset extraction within minutes of wallet compromise
- Immediate deployment of obfuscation techniques
- Use of mixers to break transaction trails
- Cross-chain bridges to complicate tracking
- Strategic routing through multiple intermediary wallets

Investigation Objectives

01

Multi-Chain Asset Tracing

Trace stolen assets across Bitcoin, Ethereum, and BNB Chain networks, following the complete path of funds through multiple blockchain ecosystems and identifying all intermediary wallets and transactions.

02

Exchange Touchpoint Identification

Identify KYC-regulated exchange touchpoints where stolen funds entered centralized platforms, creating opportunities for legal intervention and asset freezing through compliant channels.

03

Court-Ready Evidence Production

Produce a comprehensive, court-ready Evidence Dossier complete with detailed link charts, transaction timelines, and forensic analysis that meets legal standards for prosecution and recovery efforts.

04

Legal Coordination & Freeze Execution

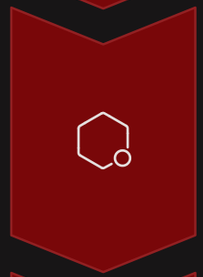
Coordinate exchange freeze requests with legal counsel, submitting compliant information packets and working with centralized exchanges to execute asset freezes on attacker-controlled accounts.

These objectives formed the foundation of Treqora's investigative strategy, combining technical blockchain forensics with legal coordination to maximize recovery potential. Each objective required specialized expertise and careful execution to ensure both technical accuracy and legal compliance throughout the investigation process.

Investigation Methodology

Evidence Intake

Client provided TXIDs, wallet addresses, phishing URL, and emails. Treqora validated all evidence and built secure chain-of-custody documentation.



Multi-Chain Forensics

Link analysis across BTC → ETH → BNB networks, detecting intermediary wallets, cross-chain bridges, and mixer interactions.

Attribution Analysis

Used proprietary attribution clusters, OSINT pattern matching, and timing correlation to identify high-likelihood entity groups.

Dossier Production

Created comprehensive 26-page investigation report with timelines, visual maps, and exchange request templates.

Legal Coordination

Submitted compliant information packets to exchanges, resulting in successful freeze of attacker-controlled assets.

Multi-Chain Forensic Analysis

The investigation revealed a sophisticated chain-hopping operation designed to obscure the trail of stolen assets. The attacker employed multiple obfuscation techniques across three major blockchain networks, requiring advanced forensic tools and methodologies to track the complete flow of funds.

1 Bitcoin Network

Initial theft and routing through two intermediary BTC wallets to break direct transaction links and create distance from the original compromise.

2 Cross-Chain Bridge

Assets converted to USDT using cross-chain bridge technology, moving funds from Bitcoin to Ethereum network to further complicate tracking.

3 Mixer Interaction

Funds routed through cryptocurrency mixer service to break transaction trails and obscure the connection between source and destination addresses.

4 BNB Chain Transfer

Additional chain-hopping to BNB Chain network, creating multiple layers of obfuscation across different blockchain ecosystems.

5 Exchange Deposit

Final destination wallet identified at a centralized EU exchange, providing the critical touchpoint for legal intervention and asset freeze.

Despite these sophisticated obfuscation techniques, Treqora's proprietary forensic tools and methodologies successfully traced the complete path of stolen assets. The investigation identified every intermediary wallet, cross-chain conversion, and mixer interaction, ultimately pinpointing the final destination at a KYC-regulated exchange where legal intervention became possible.

Evidence Dossier Components

1

Investigation Report

Comprehensive 26-page document detailing the complete investigation process, methodologies employed, findings, and conclusions. Structured for legal review and court presentation with technical accuracy and clarity.

2

Transaction Timeline

Detailed chronological timeline of all asset movements from initial theft through final destination, including timestamps, transaction IDs, and blockchain confirmations for each transfer.

3

Chain-Hopping Visual Maps

Graphical representations showing the flow of assets across Bitcoin, Ethereum, and BNB Chain networks, illustrating cross-chain bridges, mixer interactions, and intermediary wallet usage.

4

Wallet Link Chart

Network diagram connecting all identified wallets, showing relationships between addresses, clustering patterns, and attribution signals that link wallets to potential entity groups.

5

Exchange Request Templates

Pre-formatted, compliant information packets designed for submission to centralized exchanges, including all necessary technical details and legal documentation for asset freeze requests.

6

Law Enforcement Summary

Condensed executive summary tailored for law enforcement agencies, highlighting key findings, criminal methodologies, and actionable intelligence for potential prosecution efforts.

This comprehensive evidence package provided the client with multiple pathways for recovery and legal action. The court-ready documentation met all legal standards for admissibility while maintaining technical precision necessary for blockchain forensic evidence.

Investigation Outcomes

$68.5K

Recovered Amount

61% of total stolen assets successfully recovered through exchange freeze coordination and legal intervention.

19

Investigation Duration

Days from initial evidence intake to successful exchange freeze execution and evidence dossier delivery.

26

Evidence Dossier Pages

Comprehensive court-ready documentation including forensic analysis, visual maps, and legal templates.

Exchange Freeze Status

Successful execution of asset freeze on attacker-controlled accounts at centralized EU exchange. Exchange confirmed receipt of tainted funds and cooperated fully with legal freeze request.

The freeze prevented further movement of recovered assets and created legal pathway for return to rightful owner through proper channels.

Remaining Assets

Fully traceable for law enforcement follow-up. All unrecovered assets have been mapped and documented with complete transaction trails.

Evidence package provides law enforcement with actionable intelligence for potential criminal prosecution and additional recovery efforts.

Key Takeaways & Impact

Complex Multi-Chain Success

Successfully reversed sophisticated multi-chain theft through rapid forensic analysis, demonstrating capability to handle advanced obfuscation techniques across multiple blockchain networks.

Overcoming Obfuscation

Sophisticated mixing and chain-hopping techniques were successfully overcome using proprietary forensic tools and methodologies, proving that even advanced obfuscation can be penetrated.

Cross-Chain Recovery Possible

Recovery remains possible even after extensive cross-chain obfuscation, mixers, and multiple intermediary wallets when proper forensic techniques and legal coordination are employed.

Exchange Collaboration

Effective collaboration with centralized exchanges enabled legal freeze of stolen assets, highlighting the importance of KYC-regulated touchpoints in cryptocurrency recovery operations.

Actionable Intelligence

Client received comprehensive recovery plan plus complete law enforcement package, providing multiple pathways for asset recovery and potential criminal prosecution.

This case establishes important precedents for cryptocurrency recovery operations. It demonstrates that sophisticated theft operations employing multiple obfuscation techniques can still be successfully investigated and partially reversed when proper forensic methodologies are applied quickly and comprehensively. The 61% recovery rate in a complex multi-chain theft case represents a significant success in the cryptocurrency asset recovery field.

Conclusion & Next Steps

This case demonstrates Treqora's ability to handle cross-chain thefts involving phishing attacks, mixers, and multi-jurisdiction routing. Through advanced blockchain forensics and structured investigative methodology, Treqora secured a partial recovery and provided actionable intelligence for legal escalation.

The investigation showcased the critical importance of rapid response in cryptocurrency theft cases. The 19-day timeline from initial evidence intake to successful exchange freeze demonstrates that speed and expertise can make the difference between recovery and permanent loss in the fast-moving world of cryptocurrency crime.

Key success factors included comprehensive multi-chain forensic capabilities, proprietary attribution tools, established relationships with centralized exchanges, and the ability to produce court-ready documentation that meets legal standards while maintaining technical precision.

Need Help Recovering Stolen or Lost Cryptocurrency?

Speak with our investigation team for a confidential consultation. Our experts specialize in multi-chain forensics, exchange coordination, and legal recovery strategies.

Schedule a Consultation

Learn More About Our Services