Where's my crypto, Dude?

The Ultimate Guide to Crypto Money Laundering

(and how to track it)

Thomas Roccia | @fr0gger_

Sr. Threat Researcher @ Microsoft

DEFCON

Las Vegas - Aug 7-10

WHOAMI

Thomas Roccia

Sr. Threat Researcher at MSFT

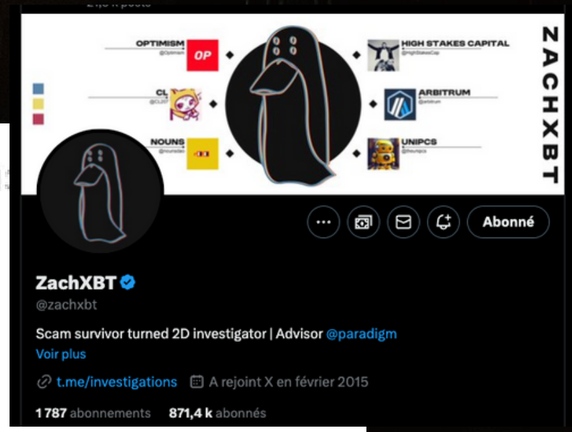
SecurityBreak.io

@fr0gger_

What we will cover

- Overview of the ByBit Case Study
- Crypto Money Laundering techniques
- Investigation Methods
- Can we track the money with an AI Agent?

The ByBit Case



$1.46 BILLION

STOLEN • FEBRUARY 21, 2025

The ByBit Case

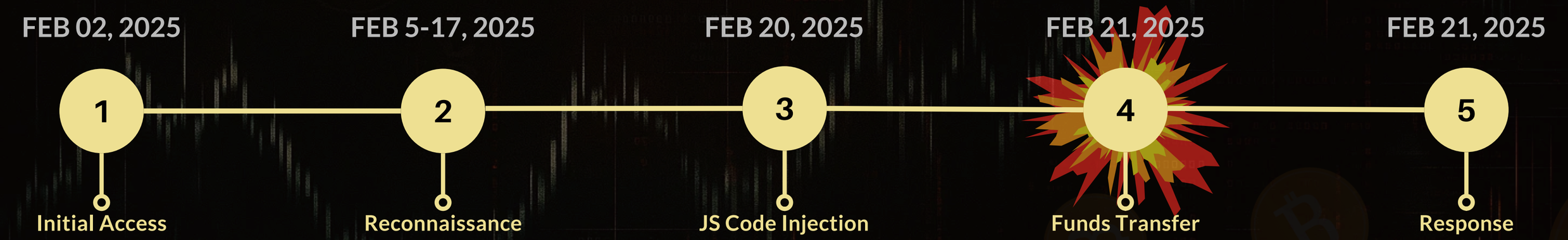
Incident Update: Unauthorized Activity Involving ETH Cold Wallet

Feb 22, 2025 ETH

What happened:

On February 21, 2025, at approximately 12:30 PM UTC , Bybit detected unauthorized activity within one of our Ethereum (ETH) Cold Wallets during a routine transfer process. The transfer was part of a scheduled move of ETH from our ETH Multisig Cold Wallet to our Hot Wallet. Unfortunately, the transaction was manipulated by a sophisticated attack that altered the smart contract logic and masked the signing interface, enabling the attacker to gain control of the ETH Cold Wallet. As a result, over 400,000 ETH and stETH worth more than $1.4 billion were transferred to an unidentified address.

The Timeline



Initial Access

Safe{Wallet} developer's **compromised via a Docker project.**

Reconnaissance

- AWS infrastructure mapping
- Web interface deployment pipeline identified
- Preparation for code injection

JS Code Injection

- Code injection
- Manipulated transaction visualization
- Preserved malicious parameters

Funds Transfer

- Standard token transfer disguise
- **Delegatecall** to attacker's contract
- Malicious code removed post-exploitation
- Funds moved via sweep functions to attacker wallets

Response

- Unusual transaction alerts
- Security team mobilized
- Initial damage: $1.46B
- Emergency protocols activated

What happened in details?

Bybit Cold Wallet

2

0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4

Blind Signing

Runs inside proxy context via delegatecall

execTransaction()

1 **Off-chain Attack**

Safe{Wallet}

- **Monitoring**: Tracked transactions linked to Bybit
- **Tampering**: Modified data live without UI change
- **Cleanup**: Reverted view and deleted code from AWS

The code ran only when Bybit's Ethereum multisig cold wallet was accessed.

UI

3 **Gnosis Safe (masterCopy)**

The wallet is a proxy: it holds storage and delegates execution to the masterCopy contract at slot 0.

0 = CALL, 1 = DELEGATECALL

Delegate Call

The sstore(0x0, newImpl) command replaced the Safe's logic with attacker's contract.

0x34CfAC646f301356fAa8B21e94227e3583Fe3F5F

4 **Attacker's Contract**

Deployed a spoofing contract with a function that can overwrite slot 0

Goal: change masterCopy when run via delegatecall.

0x96221423681A6d52E184D440a8eFCEbB105C7242

5

SweepETH

Transfers **all ETH held by the contract to a specified address.**

SweepERC20

Moves the **entire balance of a given ERC-20 token** from the contract.

6

-$1.5 billion USD

February 21, 2025, at 14:13:35 UTC

CryptoMoney Laundering 101

(DPRK Edition)

Immediate Asset Conversion
Swapped large amounts of stolen tokenized assets

No-KYC Exchanges
Using unregulated instant swap services

Layering via Multiple Wallets
"Money distribution across multiple addresses

ETH to BTC Conversion
Converting to Bitcoin for better liquidity and anonymity

Cross-Chain Bridges
Moving assets across different blockchain networks

Mixers & CoinJoin
Mixing dirty money with clean money, join transactions

DEX Swaps
Anonymous token exchanges via decentralized protocols

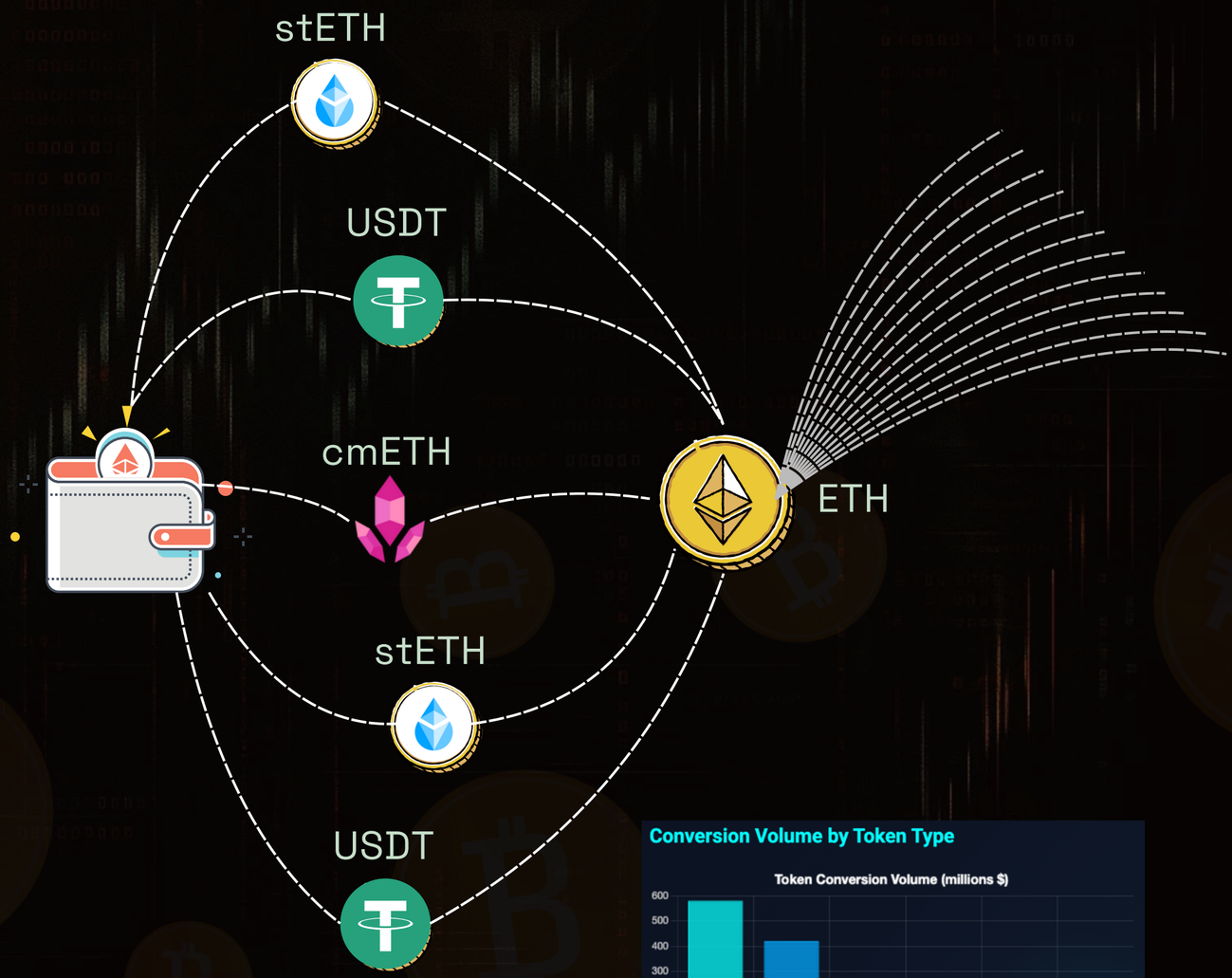
OTC Cash-Out
Converting crypto to fiat via underground networks

1 - Immediate Asset Conversion

The rapid conversion of stolen tokens into more fungible "native" crypto assets to avoid freezes and increase anonymity.

Within minutes threat actor converted stolen tokenized assets (stETH, cmETH) into plain Ether (ETH) via decentralized exchanges.

- Tokenized assets can be frozen
- DEXs provide immediate liquidity without KYC
- Base assets like ETH have no central authority
- Conversion breaks initial transaction trail



1 - Tracking Opportunity

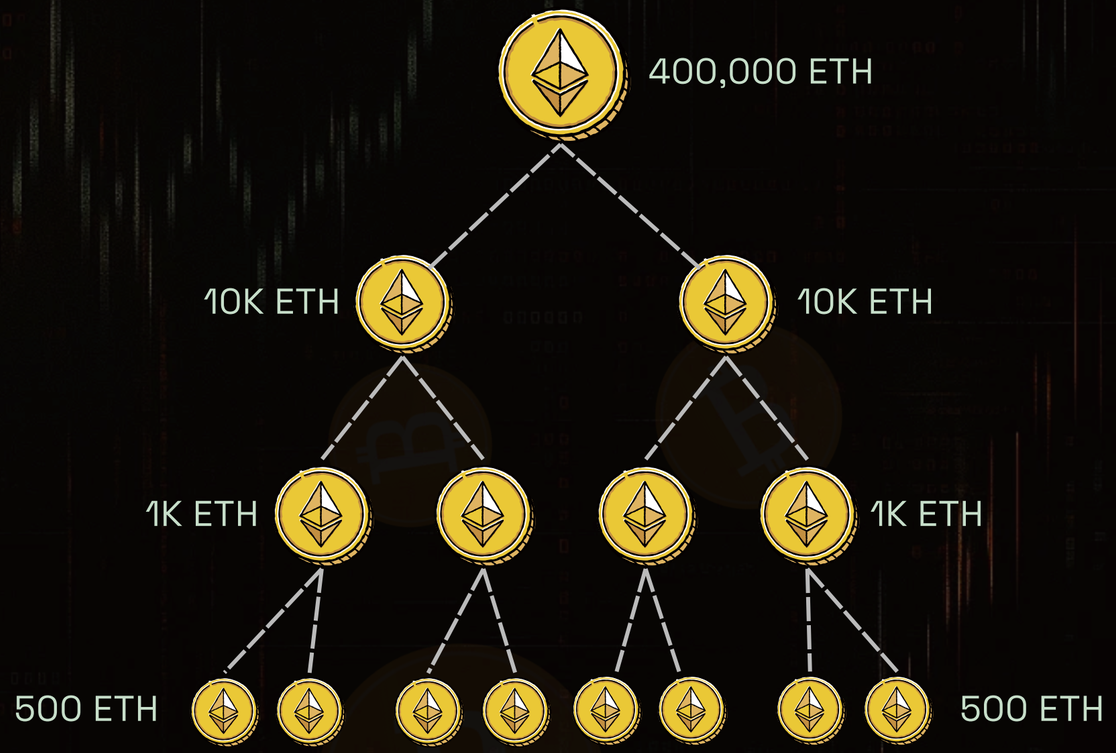
- Monitor gas price patterns for batch operations
- Track MEV bot interactions during swaps
- Analyze slippage tolerance settings
- Correlate with known stolen token addresses

2 - Money Dispersing

The distribution of stolen funds across multiple wallet addresses in a **fractional or dispersing pattern** to obscure the money trail.

Threat actor distributed the stolen ETH across 50+ initial wallets, then further split into thousands of addresses using automated scripts.

- Initial distribution to ~50 wallets with 10,000 ETH each
- Secondary distribution to ~500 wallets with 1,000 ETH each
- Automated transaction batching with consistent gas fees



2 - Tracking Opportunity

Gas Usage

- Monitor Gas usage
- Similar amount can indicate automation or script

Multi-Hop Analysis

- Trace funds beyond immediate hops
- Identify convergence points
- Map complete laundering networks

Token Flow

- Get all outbound transactions
- Where did those addresses send funds next?
- How much? When?
- Are they interacting with CEXs, DeFi protocols, mixers, etc.?

Temporal Clustering

- Cross-reference timing patterns
- Identify coordinated activities
- Detect automation signatures

Subgraph Extraction

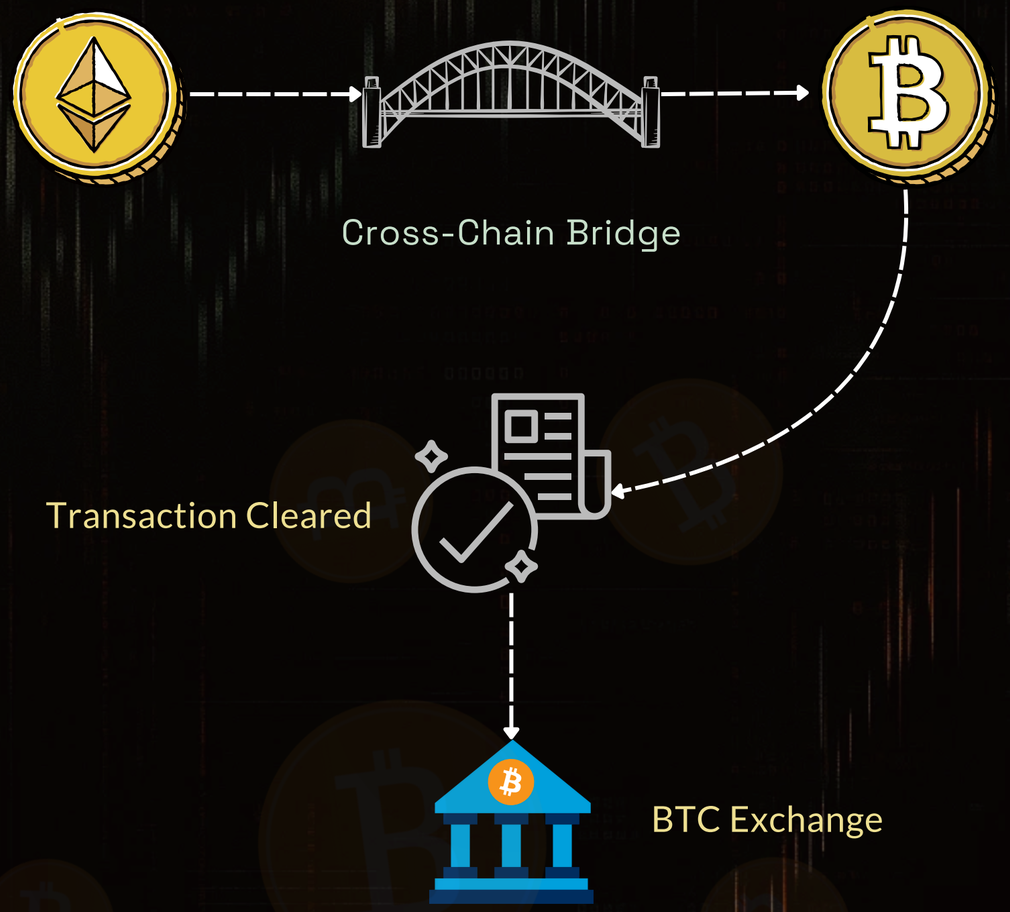
- Isolate subgraphs
- Analyze structural properties
- Compare against known patterns

3 - Cross-Chain Bridges

The movement of cryptocurrency assets **across different blockchain networks** to break the transaction trail and leverage different anonymity features.

Threat actor **moved ETH and ERC-20 tokens to Bitcoin, Tron, and other chains** using cross-chain bridges like ChainFlip, Multichain, and Thorchain.

- ETH → BTC conversion via Chainflip (atomic swaps)
- ETH → TRX conversion via Multichain (lock and mint)
- Use of wrapped tokens (WBTC, renBTC) as intermediaries



3 - Tracking Opportunity

Label Known DPRK Wallets

Use Arkham, TRM, ChainAnalysis or public intelligence and blacklists.

Track Token Flow

- Use token transfer events (ERC-20) to see jumps.
- Correlate timestamps with other chain actions.

Monitor Bridges, Watch inflow/outflow

Chainflip, Multichain, THORChain

Correlate Patterns

Match addresses by behavior, not just hash.
Use volume, token type, and usage patterns.

4 - DEX Swaps

Usage of decentralized exchanges for anonymous wallet-to-wallet asset conversion without regulatory oversight or KYC requirements. **Uniswap** **Dodo** **Paraswap**

1
Stolen Assets
ETH & derivative tokens

2
DEX Swapping
Convert to stablecoins & wrapped assets

3
Asset Juggling
Route through liquidity pools (ETH, BTC, DAI)

4
Trail Obfuscation
Create complexity through parallel transactions

- DeFi protocols were integral to obscuring fund origins according to blockchain forensics experts
- Processing flows were **"wallet-to-wallet exchanges"** rather than traditional mixers in initial phases
- DEXs functioned as de facto mixers by permuting assets and scattering transactions outside regulated intermediaries
- Large volume parallel swaps through liquidity pools added investigative complexity and noise to transaction traces

4 - Dex Swap Tracking Opportunity

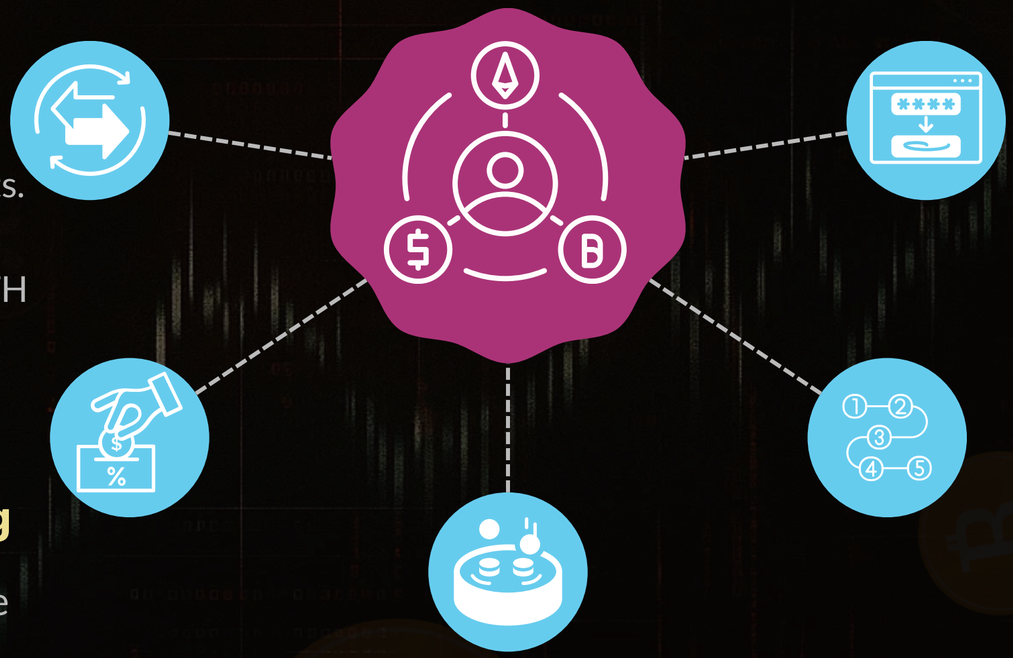
Trace Swap Transactions

Filter for Swap, AddLiquidity, RemoveLiquidity events in DEX contracts.
Look for patterns like:

- ETH → USDT → obscure token → ETH
- Many rapid swaps with slippage
- Use of aggregators (1inch, Matcha)

Detect Wrapping/Unwrapping

- WETH, renBTC, stETH, etc. can hide movement.
- Log Deposit/Withdraw or token contract events.



Pool Liquidity Impact

- Monitor Sync, Swap, and Transfer events
  - ΔTokenIn / ΔTokenOut
  - Pre/post-swap reserve imbalance can reveal forced swaps or laundering behavior.
  - Slippage %

Obfuscation Patterns

- Tornado Cash (check interactions with mixing contracts)
- Using many small wallets (peeling chains)
- Use of flash loans or MEV-like behavior to hide trails.

Multi-Hop Path Reconstruction

- Parse the Swap events from router contracts within 1–2 blocks or under 60 sec
- Extract:
  - Each hop (token in → token out)
  - Path sequence
  - Amounts
  - Timestamp

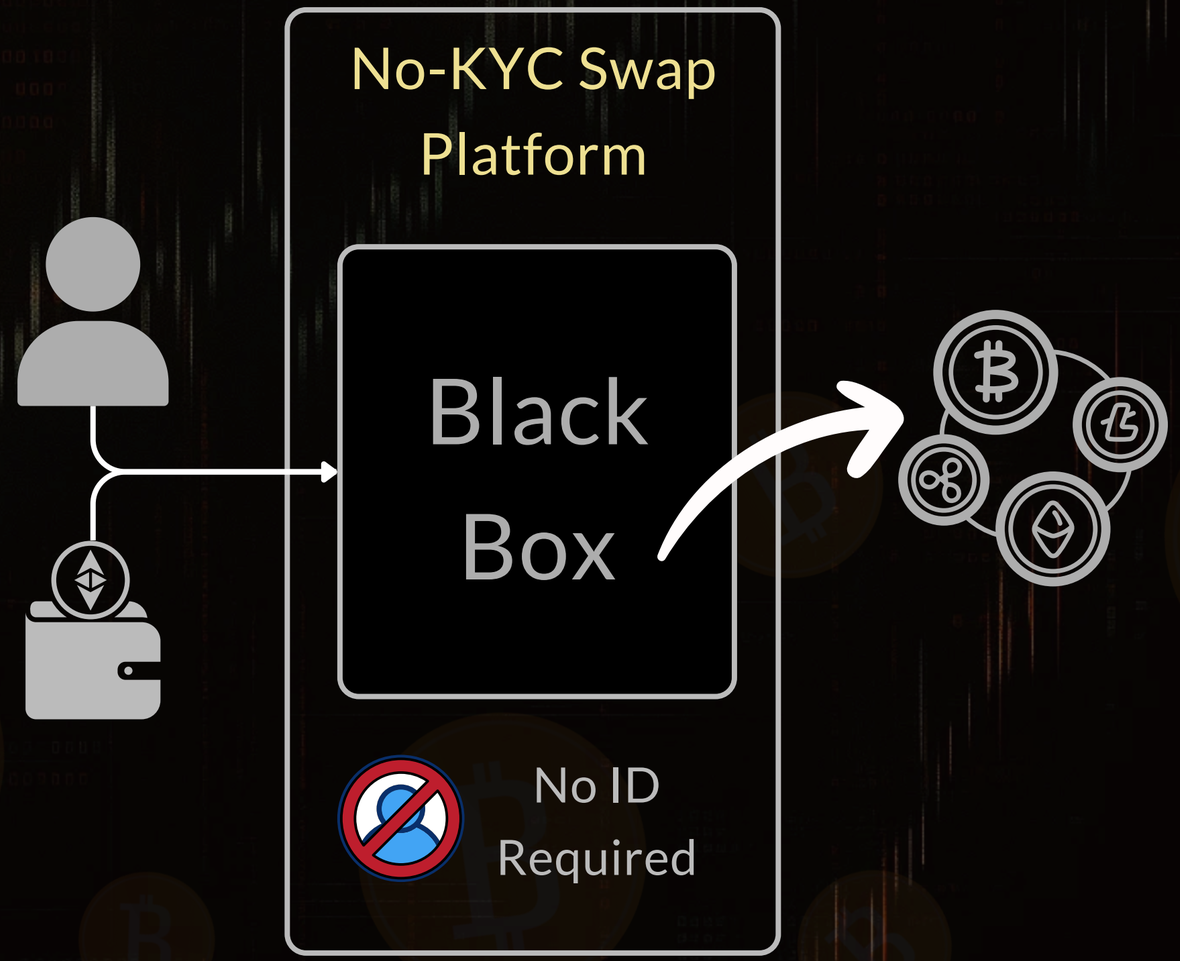
5 - No-KYC Exchanges

Cryptocurrency exchange platforms that allow users to swap different digital assets without requiring Know Your Customer (KYC) identity verification documents.

The threat actor used eXch as a primary laundering mechanism to launder $200 million stolen from Bybit.

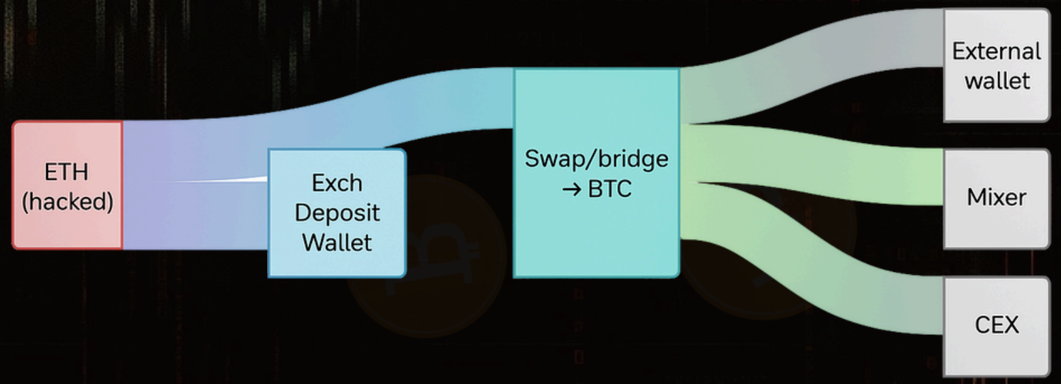
FAIL

eXch's capacity was temporarily overwhelmed by the volume of transactions, forcing threat actor to pause operations until processing resumed.



5 - No KYC Tracking Opportunity

- Match transactions with known eXch deposit wallets
  - Look for wallets that receive funds → go quiet
- Trace outflows in BTC
  - Check BTC address clusters
  - Flag mixers or known cash-out exchanges
- Reconstruct the swap flow:
  - ETH (hacked) → eXch Deposit Wallet
  - Swap/bridge → BTC
  - eXch Withdrawal Wallet → External wallet → Mixer or CEX



6 - ETH to BTC Conversion

The strategic conversion of stolen Ethereum assets to Bitcoin to leverage Bitcoin's greater liquidity, wider acceptance, and different tracing challenges.

The threat actor converted approximately 60% of the stolen ETH to BTC through various methods, including wrapped tokens, atomic swaps, and cross-chain bridges.

- Use of wrapped tokens (WBTC, renBTC) as intermediaries
- Atomic swaps via specialized services
- Cross-chain bridges with minimal KYC requirements
- Preference for services with high liquidity to minimize slippage

Initial ETH Preparation

ETH is split into multiple wallets to distribute risk and avoid large single transactions that could trigger alerts.

01

Wrapped Token Conversion

ETH is converted to wrapped Bitcoin tokens like WBTC or renBTC on Ethereum blockchain.

02

Cross-Chain Bridge Transfer

Wrapped tokens are sent through cross-chain bridges like ThorChain to convert from Ethereum-based tokens to native

03

Bitcoin Network Distribution

BTC is further distributed across multiple wallets on the Bitcoin network, creating a new layer of obfuscation.

04

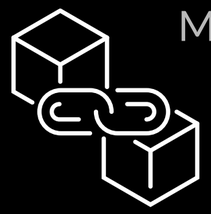
6 - ETH to BTC Tracking Opportunity

Initial ETH Prep

Detect wallet splitting via:

- Cluster analysis (creation time)
- Time-based heuristics (txs within seconds)
- Pattern matching (same flow logic)

Cross-Chain Bridge



Monitor:

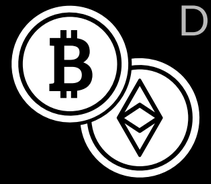
- Chainflip, THORChain, etc.
- Burn/Lock events on ETH side
- BTC output matching (value + timing)
- Known bridge BTC addresses

Wrapped Token Conversion

Watch ETH → WBTC via:

- Smart contract logs (Mint, Burn, Deposit)
- DEX swaps before wrapping
- Known wrapping contract usage

BTC Distribution



Detect:

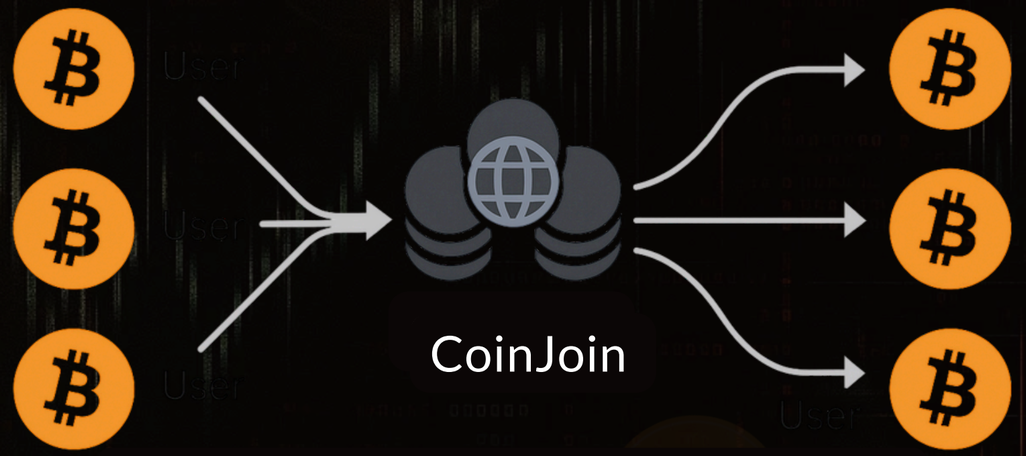
- Peeling chains (BTC hop wallets)
- Mixer/CEX usage
- One-time use wallets and timing link

7 - Mixers & CoinJoin

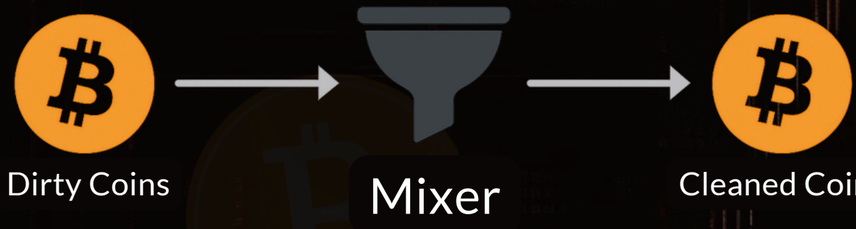
The use of specialized services that pool funds from multiple users and redistribute them to break the transaction trail between source and destination addresses.

The threat actor used Tornado Cash for ETH mixing and Wasabi Wallet's CoinJoin for Bitcoin but also CryptoMixer and Railgun, with careful timing and amount strategies to avoid pattern detection.

- Zero proofs to verify transactions without revealing links
- Fixed denomination deposits to prevent amount correlation
- Time-delayed withdrawals to break temporal patterns
- Multiple rounds of mixing to further obfuscate the trail



Multiple users collaboratively create a single transaction that mixes their inputs and outputs.



You send your crypto to a central service. They mix it with others and send back "cleaned" coins from a different pool.

7 - Mixers and Coinjoin Tracking Opportunity

Heuristic Analysis

Apply statistical heuristics to identify likely connections between pre-mixer and post-mixer transactions based on timing, amounts, and wallet behavior patterns.

Taint Analysis

Track the "taint" or contamination level of funds that have passed through mixers, flagging wallets that receive significant percentages of mixed funds.

Mixer Contract Monitoring

Monitor interactions with known mixer smart contracts (e.g., Tornado Cash) and flag wallets that interact with sanctioned mixing services.

8 - OTC Cash-Out

The final stage of money laundering where laundered cryptocurrency is converted to fiat currency through over-the-counter (OTC) brokers and money-laundering networks.

Threat actor used a network of OTC brokers in jurisdictions with minimal regulatory oversight to convert laundered cryptocurrency to fiat currency.

- Use of P2P platforms with minimal KYC requirements
- Strategic selection of jurisdictions with weak AML enforcement
- Coordination with established money laundering networks
- Gradual cash-out over extended periods to avoid detection

Key OTC Cash-Out Regions

Southeast Asia

High crypto adoption with varying regulatory frameworks

P2P Platforms | Crypto ATMs | Hawala Networks

Eastern Europe

Established OTC networks with connections to traditional financial systems

OTC Brokers | Shell Companies | Banking Connections

Latin America

High cash economies with established money laundering infrastructure

Cash Exchanges | Remittance Services | Informal Banking

8 - OTC Cash-Out - Tracking Opportunity

Track On-Chain Leads Up to the OTC Entry

Look for large DEX swaps to stablecoins (e.g., ETH → USDT).

Funds often land in:

- Known OTC wallet clusters
- Fresh wallets used once, then emptied
- Deposit addresses at CEXs linked to OTC desks

Identify OTC Brokers and Desks

- Use intel from:
  - Elliptic, TRM, Chainalysis (labeled OTC clusters)
  - Telegram, Discord, or WeChat OTC networks
- Flag wallets known to interact with OTC brokers

Watch for Behavior Signals

- Sudden fund stops after swap or consolidation
- One-time wallet use, followed by long dormancy
- Time-based correlation: multiple wallets emptying to same address in a short window

Check for CEX Entry/Exit Points

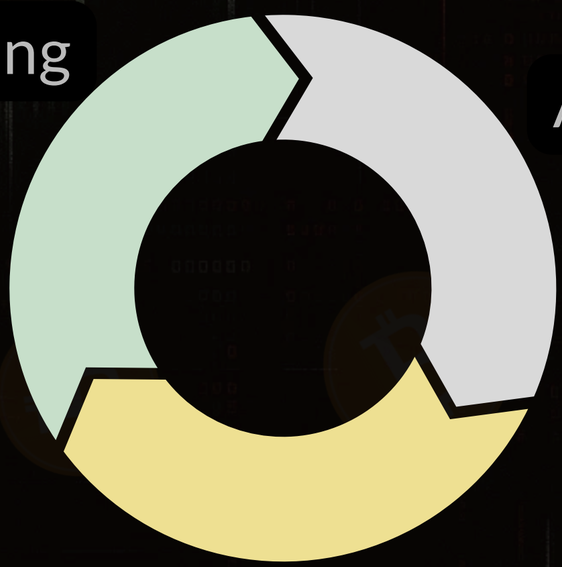
- OTC brokers often use:
  - Binance, Huobi, OKX, etc.
  - Look for shared deposit addresses or batched withdrawals
- Combine with KYT solutions to catch known off-ramps

Building an AI Agent

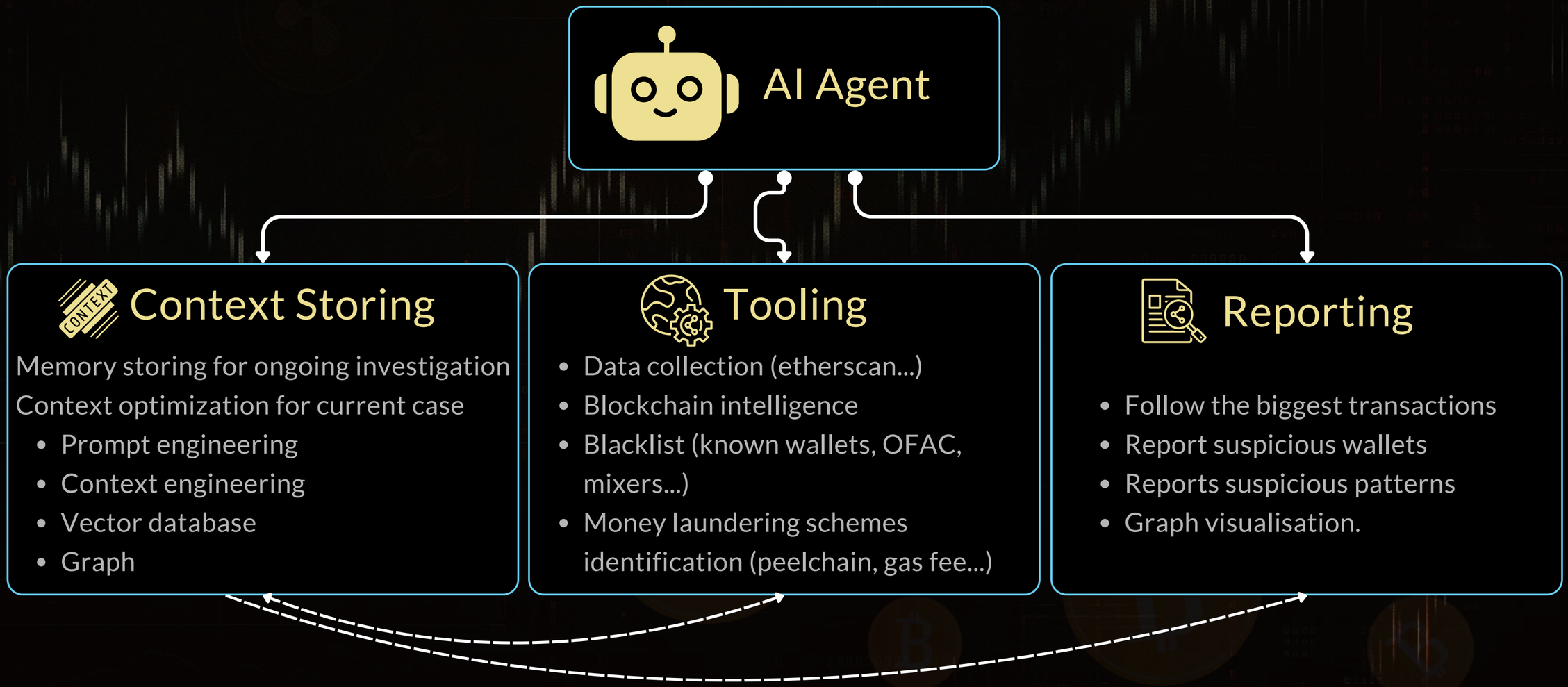
An AI agent is an autonomous system powered by an LLM.

It can plan, reason, and act on tasks.

With the right tools and data, we can build agents to help track money flows.



AI Agent for Tracking the Money



Model Context Protocol

- Open protocol to connect AI models with tools, data, and services
- Client-server architecture for structured communication
- Improves accuracy by giving models access to real-time context

MCP Etherscan

- Connects to the Etherscan API, Collects on-chain transaction data
- Timestamp, Amount transferred, Gas fee and gas used, Sender and recipient addresses, Tx hash and block number, Contract interactions and method names, Token transfers.

MCP Blockchain Intelligence

- Connect to blockchain intelligence providers
- Cross chain investigation
- DEX Swap

MCP Money Laundering Schemes

- Implementation of money laundering patterns
- Money distribution, Known Blacklists
- Gas fee pattern, money distribution, volume, frequency
- Wallet clustering

Demo

Challenges & Limitations

No Identity Ties

- Addresses aren't linked to real people. Without KYC, attribution is guesswork.

Too Much Data

- Millions of noisy transactions make finding patterns hard.

Obfuscation

- Mixers, CoinJoin, swaps, and shell wallets break the flow.

Cross-Chain Moves

- Money jumps chains. Tracking requires multi-network visibility.

Missing Context

- On-chain data lacks intent. Meaning often sits off-chain.

API Limits

- Free APIs are slow. Good data access costs.

Heavy Infra

- Live tracking needs strong infra and constant tuning.

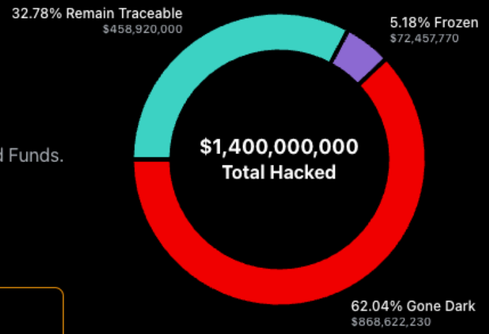
DPRK Money Tracking

BYBIT | LazarusBounty

Total Bounty	Awarded Bounty	Bounty Hunters
$140,000,000	$2,333,235	13

1. Bounties will be paid proportionate to the amount of Returned Funds, and will be distributed from the Returned Funds.
2. The total bounty is 10% of the recovered funds, distributed as follows:
   a. 5% to the entity that successfully froze the funds.
   b. 5% to the first reporters who helped trace the funds, leading to their freezing.

Submit a Lead | View Rules



Funds Sent to Untraceable or Freezable Destinations

The stolen funds have been transferred to untraceable or freezable destinations, such as exchanges, mixers, or bridges, or converted into stablecoins that can be frozen. We require cooperation from all involved parties to either freeze the funds or provide updates on their movement so we can continue tracing. Response time is measured from the moment the specific transaction is reported to the relevant party.

Mixers (4) | Bridge Actors (5) | Alert Actors (1) | Good Actors (18) | Collaborators (2)

Rank	Name	Total Inflow	Total Transactions	Chain	Status
1	Wasabi Wallet	$247,583,088	966	BTC	Pending Information
2	CryptoMixer	$9,414,365	66	BTC	Pending Information
3	TornadoCash	$2,516,783	75	ETH	Pending Information
4	RAILGUN	$1,733,062	7	ETH	Pending Information

Conclusion

- DPRK actors are highly familiar with cryptocurrency ecosystems
- They use advanced methods, from supply chain attacks to complex laundering schemes
- Tactics evolve fast and it makes large-scale tracking difficult
- AI and autonomous systems can support investigations when properly resourced
- These tools help analysts navigate the massive flow of crypto transactions effectively

Additional Resources

- https://www.nccgroup.com/au/research-blog/in-depth-technical-analysis-of-the-bybit-hack/
- https://certik.com/resources/blog/bybit-incident-technical-analysis
- https://lukka.tech/bybit-hack-deep-dive/
- https://research.checkpoint.com/2025/the-bybit-incident-when-research-meets-reality/
- https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/
- https://www.chainalysis.com/blog/bybit-exchange
- hack-february-2025-crypto-security-dprk/
- https://crystalintelligence.com/investigations/the-bybit-heist-how-the-hackers-took-control/
  https://cointelegraph.com/news/safe-wallet-releases-bybit-hack-post-mortem
- https://www.binance.com/en/square/post/03-06-2025-bybit-hack-safewallet-report-reveals-details-of-1-4-billion-cybersecurity-breach-21195682977506
- https://www.trmlabs.com/resources/blog/the-bybit-hack-following-north-koreas-largest-exploit
- https://www.trmlabs.com/resources/blog/exch-remains-active-despite-shutdown-how-the-bybit-hack-linked-exchange-continues-to-enable-laundering-of-csam-funds
- https://www.trmlabs.com/resources/blog/bybit-hack-update-north-korea-moves-to-next-stage-of-laundering
- https://www.trmlabs.com/resources/blog/trm-links-north-korea-to-record-1-5-billion-record-hack
- https://x.com/safe/status/1894768522720350673
- https://twitter.com/Bybit_Official/status/17609999999999999
- https://cointelegraph.com/news/zach-xbt-identifies-lazarus-group-bybit-hack-arkham-bounty
- https://twitter.com/zachxbt

Aymen Jaffry
TRM Labs

Umberto @misterserious
(recoveris.io)

JBK

Sean O’Connor
@Vhumint


Thank You
Thomas Roccia | @fr0gger_
DEFCON