

Investigate Ethereum Address Activity

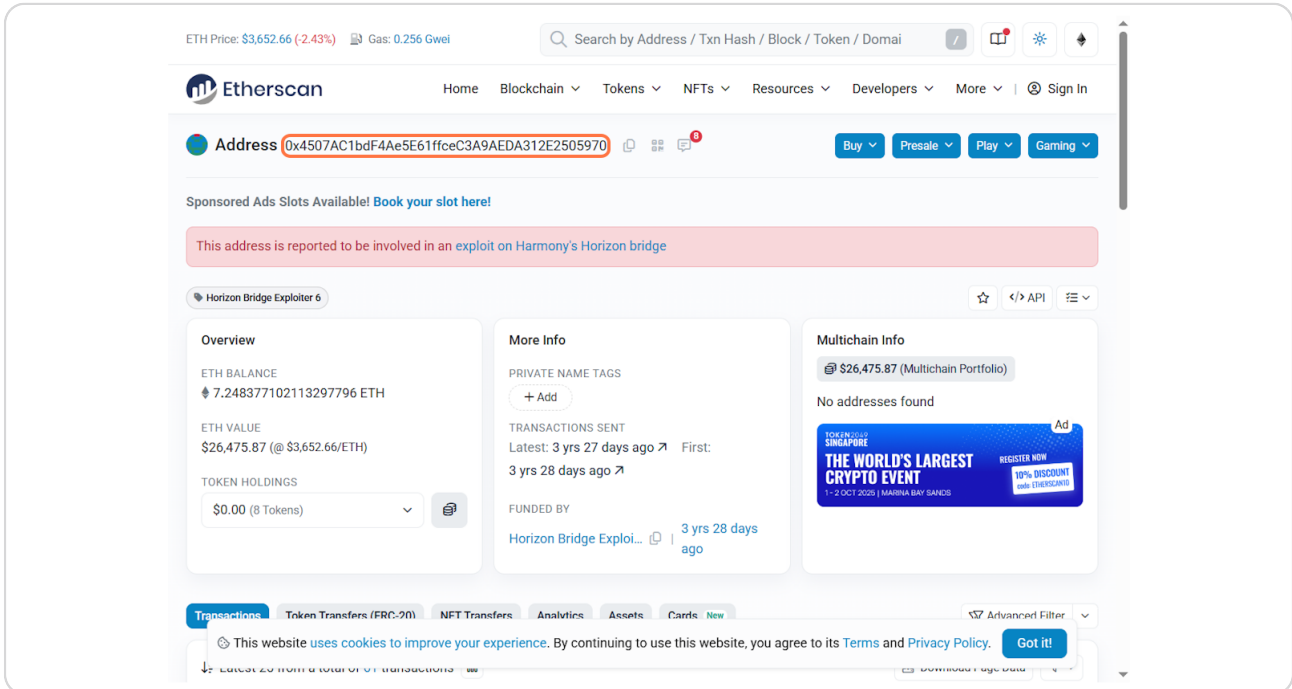
16 Steps [View most recent version on Tango.ai](#) 

Created by	Creation Date	Last Updated
Shad Shaho	Jul 26, 2025	Jul 27, 2025

STEP 1

Open the wallet on Etherscan

This is the wallet that received funds from Lazarus Group. We'll investigate its activity on-chain



The screenshot shows the Etherscan website interface. At the top, the ETH Price is \$3,652.66 (-2.43%) and Gas is 0.256 Gwei. The search bar is set to "Search by Address / Txn Hash / Block / Token / Domain". The main header includes navigation links: Home, Blockchain, Tokens, NFTs, Resources, Developers, More, and Sign In.

The address **0x4507AC1bdF4Ae5E61fcec3A9AEDA312E2505970** is highlighted in the address field. Below the address, there are buttons for Buy, Presale, Play, and Gaming. A red banner states: "This address is reported to be involved in an exploit on Harmony's Horizon bridge".

The "Horizon Bridge Exploit" section shows the following details:

- Overview:**
 - ETH BALANCE: 7.248377102113297796 ETH
 - ETH VALUE: \$26,475.87 (@ \$3,652.66/ETH)
 - TOKEN HOLDINGS: \$0.00 (8 Tokens)
- More Info:**
 - PRIVATE NAME TAGS: + Add
 - TRANSACTIONS SENT: Latest: 3 yrs 27 days ago, First: 3 yrs 28 days ago
 - FUNDED BY: Horizon Bridge Exploit... 3 yrs 28 days ago
- Multichain Info:**
 - \$26,475.87 (Multichain Portfolio)
 - No addresses found

At the bottom, there are tabs for Transactions, Token Transfers (ERC-20), NFT Transfers, Analytics, Assets, and Cards. A cookie notice is visible at the bottom of the page.

STEP 2

Open the wallet's transaction history

To view all incoming and outgoing transfers, open the Transactions tab

7.248377102113297796 ETH

ETH VALUE
\$26,475.87 (@ \$3,652.66/ETH)

TOKEN HOLDINGS
\$0.00 (8 Tokens)

+ Add

TRANSACTIONS SENT
Latest: 3 yrs 27 days ago ↗ First:
3 yrs 28 days ago ↗

FUNDED BY
Horizon Bridge Exploi... | 3 yrs 28 days ago

Transactions

Token Transfers (ERC-20)

NFT Transfers

Analytics

Assets

Cards New

↓ Latest 25 from a total of 61 transactions

Transaction Hash	Method	Block	Age	From
0xe833ec4678...	Deposit	15036362	1123 days ago	Horizon Bridge Exploi...
0x34619d5608...	Deposit	15036341	1123 days ago	Horizon Bridge Exploi...

STEP 3

Open Lazarus Group 6,010 ETH transaction

Click the Txn Hash to view the full details of the 6,010 ETH transfer from a Lazarus-labeled address.

ETH Price: \$3,758.01 (+0.83%) Gas: 0.259 Gwei

Search by Address / Txn Hash / Block / Token / Domain

Address	Type	Hash	Time	From	Label	Amount	To
0x931af07c302...	Deposit	15034892	1124 days ago	Horizon Bridge Explo...	OUT	100 ETH	Tornado.Cash: Rou...
0x4099c2e889...	Deposit	15034862	1124 days ago	Horizon Bridge Explo...	OUT	100 ETH	Tornado.Cash: Rou...
0x991b4a5568...	Deposit	15034823	1124 days ago	Horizon Bridge Explo...	OUT	100 ETH	Tornado.Cash: Rou...
0x061653bbb6...	Deposit	15034797	1124 days ago	Horizon Bridge Explo...	OUT	100 ETH	Tornado.Cash: Rou...
0xa98aca90cb...	Deposit	15034794	1124 days ago	Horizon Bridge Explo...	OUT	100 ETH	Tornado.Cash: Rou...
0x85b629e00e...	Deposit	15034719	1124 days ago	Horizon Bridge Explo...	OUT	100 ETH	Tornado.Cash: Rou...
0xda29359a50f...	Transfer	15034102	1124 days ago	Horizon Bridge Explo...	IN	6,012 ETH	Horizon Bridge Explo...

Show: 50 Records

First < Page 2 of 2 > Last

[Download: CSV Export]

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Back to Top

This website uses cookies to improve your experience. By continuing to use this website, you agree to its [Terms](#) and [Privacy Policy](#). [Got It!](#)

Powered by Ethereum


STEP 4

Verify Lazarus Group as sender

The sender address is publicly labeled "Lazarus Group – North Korea" on Etherscan, confirming the source is tied to a known cybercriminal group.

ETH Price: \$3,758.01 (+0.83%) Gas: 0.24 Gwei

Search by Address / Txn Hash / Block / Token / Domain

 **TRANSACTION ACTION**
Transfer 6,012 (\$22,593,179.77) ETH to [Horizon Bridge Exploi...](#)

Transaction Hash:

0xda29359a50fb1e22d523b70493947f74272949b3485c9ccf6a7bfb7ca770c042

Status:

Success

Block:


15034102 7968306 Block Confirmations

Timestamp:

1124 days ago (Jun-27-2022 11:17:40 AM UTC)

Sponsored:

Advertise on

 **BscScan**
Scan Original

From:

0x1Ec6F83b55C3F4CeFc630442716872BA15f16430 (Horizon Bridge Exploiter 4)

To:

0x4507AC1bdF4Ae5E61fcecC3A9AEDA312E2505970 (Horizon Bridge Exploiter 6)

Value:

6,012 ETH \$22,593,179.77

Transaction Fee:

0.00100356569502 ETH \$3.77

Gas Price:

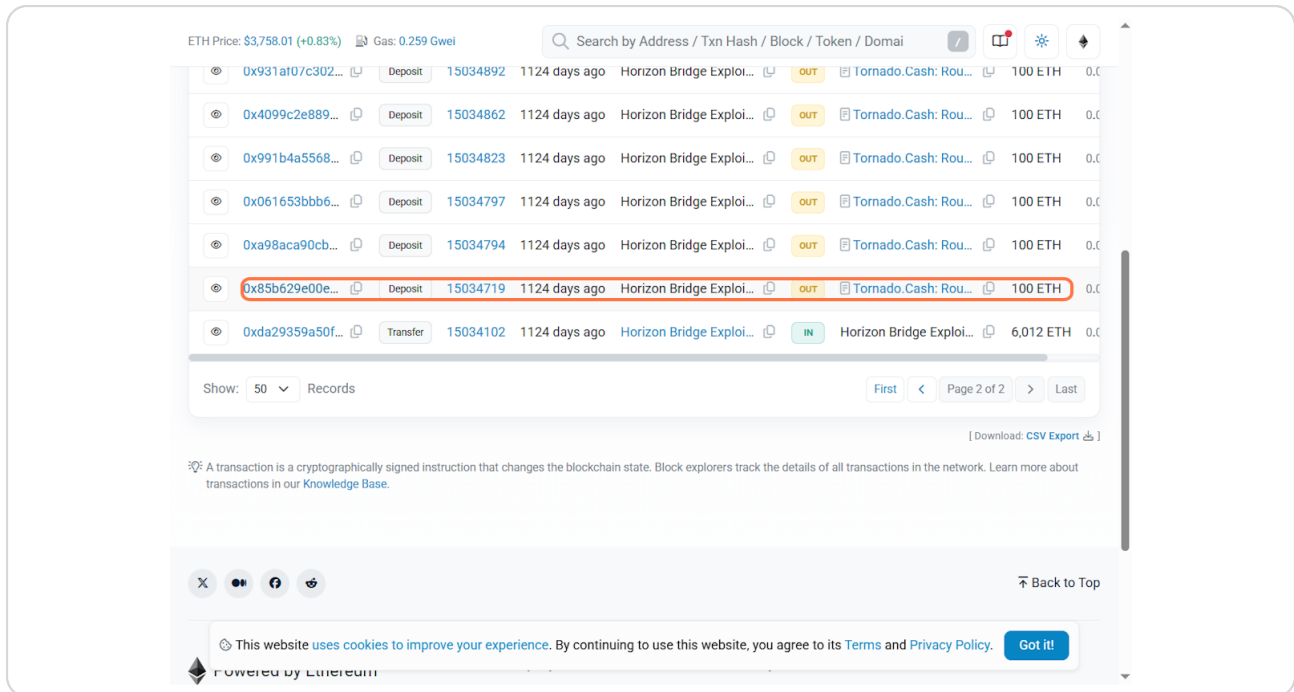
47.78884262 Gwei (0.00000004778884262 ETH)

This website uses cookies to improve your experience. By continuing to use this website, you agree to its [Terms](#) and [Privacy Policy](#). [Got It!](#)

STEP 5

Review full transaction details

This transaction shows that Lazarus Group sent 6,010 ETH to this wallet. The amount, timestamp, and sender label confirm the origin of the funds.



ETH Price: \$3,758.01 (+0.83%) Gas: 0.259 Gwei

Search by Address / Txn Hash / Block / Token / Domain

Address	Type	Amount	Time	From	To	Label
0x931af07c302...	Deposit	15034892	1124 days ago	Horizon Bridge Exploi...	OUT	Tornado.Cash: Rou...
0x4099c2e889...	Deposit	15034862	1124 days ago	Horizon Bridge Exploi...	OUT	Tornado.Cash: Rou...
0x991b4a5568...	Deposit	15034823	1124 days ago	Horizon Bridge Exploi...	OUT	Tornado.Cash: Rou...
0x061653bbb6...	Deposit	15034797	1124 days ago	Horizon Bridge Exploi...	OUT	Tornado.Cash: Rou...
0xa98aca90cb...	Deposit	15034794	1124 days ago	Horizon Bridge Exploi...	OUT	Tornado.Cash: Rou...
0x85b629e00e...	Deposit	15034719	1124 days ago	Horizon Bridge Exploi...	OUT	Tornado.Cash: Rou...
0xda29359a50f...	Transfer	15034102	1124 days ago	Horizon Bridge Exploi...	IN	Horizon Bridge Exploi...

Show: 50 Records

First < Page 2 of 2 > Last

[Download: CSV Export]

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Back to Top

This website uses cookies to improve your experience. By continuing to use this website, you agree to its [Terms](#) and [Privacy Policy](#). [Got It!](#)

Powered by Ethereum

STEP 6

Find first Tornado Cash transaction (100 ETH)

“After receiving funds, this wallet fragmented the ETH into smaller amounts. We’ll start by tracing the first 100 ETH deposit to Tornado Cash Router.

The screenshot displays a transaction page on a blockchain explorer. At the top, it shows the ETH price as \$3,756.57 (+0.79%) and the gas price as 0.265 Gwei. A search bar is located at the top right. The transaction details are as follows:

- Transaction Hash:** 0x85b629e00ec6a6935fcb8b900af66d955f23329ec4835e98a7692276a8ea38a0
- Status:** Success
- Block:** 15034719 (7967697 Block Confirmations)
- Timestamp:** 1124 days ago (Jun-27-2022 02:04:41 PM UTC)
- Sponsored:** Advertise on SnowScan Scan Original
- From:** 0x4507AC1bdF4Ae5E61ffceC3A9AEDA312E2505970 (Horizon Bridge Exploiter 6)
- To:** 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b (Tornado.Cash: Router)
- Internal Transactions:** All Transfers | Net Transfers
 - Transfer 100 ETH \$375,656.83 From Tornado.Cash: Router To Tornado.Cash: 100 ETH
- Value:** 100 ETH \$375,656.83
- Transaction Fee:** 0.085992636 ETH \$323.04
- Gas Price:** 93 Gwei (0.000000093 ETH)

A cookie notice at the bottom states: "This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got It!"

STEP 7

Copy wallet address to investigate visually

We will now trace this wallet visually in Breadcrumbs to better understand the movement of funds.

Breadcrumbs is a blockchain graph analysis tool. Paste the wallet address and visualize its connections.

ETH Price: \$3,652.66 (-2.43%) Gas: 0.256 Gwei

Search by Address / Txn Hash / Block / Token / Domain

Etherscan Home Blockchain Tokens NFTs Resources Developers More Sign In

Copy Address

Address 0x4507AC1bdF4Ae5E61ffceC3A9AEDA312E2505970 Buy Presale Play Gaming

Sponsored: Rollbit: Best rewards program. Deposit BTC, ETH, SOL, PEPE & more. Instant withdrawals! Play Now!

This address is reported to be involved in an exploit on Harmony's Horizon bridge

Horizon Bridge Exploiter 6

Overview

ETH BALANCE
7.248377102113297796 ETH

ETH VALUE
\$26,475.87 (@ \$3,652.66/ETH)

TOKEN HOLDINGS
\$0.00 (8 Tokens)

More Info

PRIVATE NAME TAGS
+ Add

TRANSACTIONS SENT
Latest: 3 yrs 27 days ago First: 3 yrs 28 days ago

FUNDED BY
Horizon Bridge Exploi... | 3 yrs 28 days ago

Multichain Info

\$26,475.87 (Multichain Portfolio)

No addresses found

Advertise on SnowScan

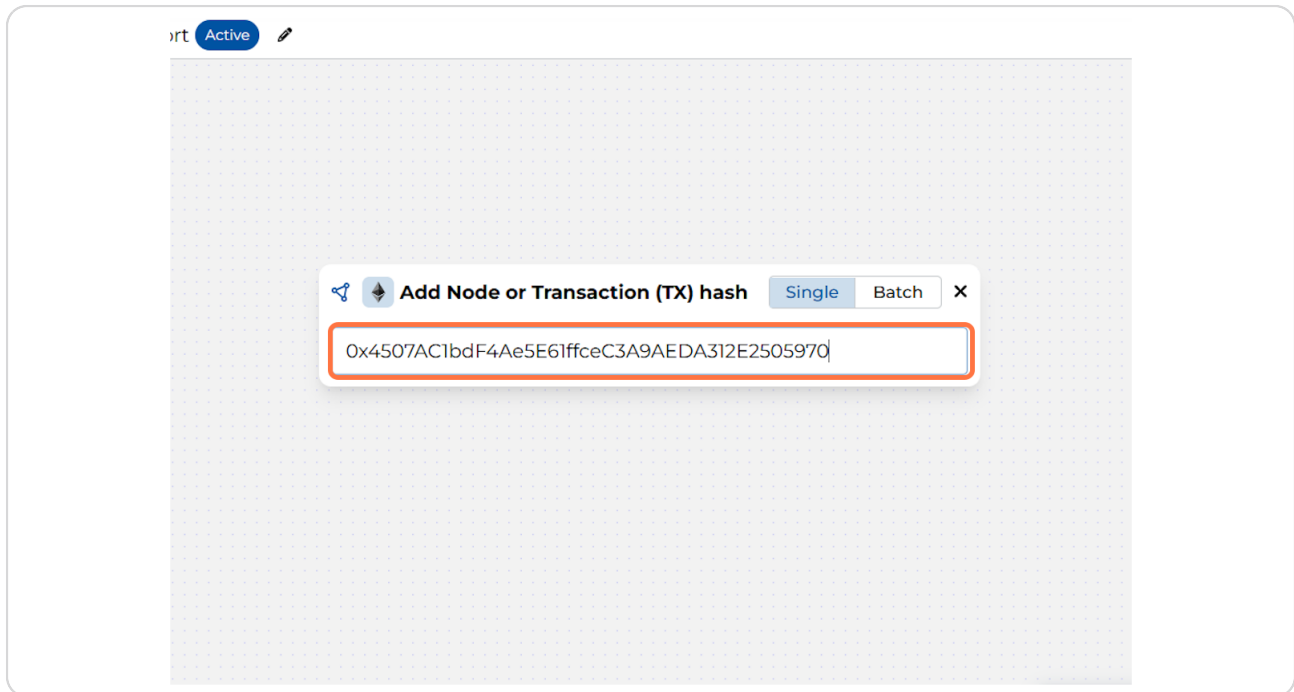
Transactions Token Transfers (ERC-20) NFT Transfers Analytics Assets Cards New

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

STEP 8

Locate wallet node in Breadcrumbs graph

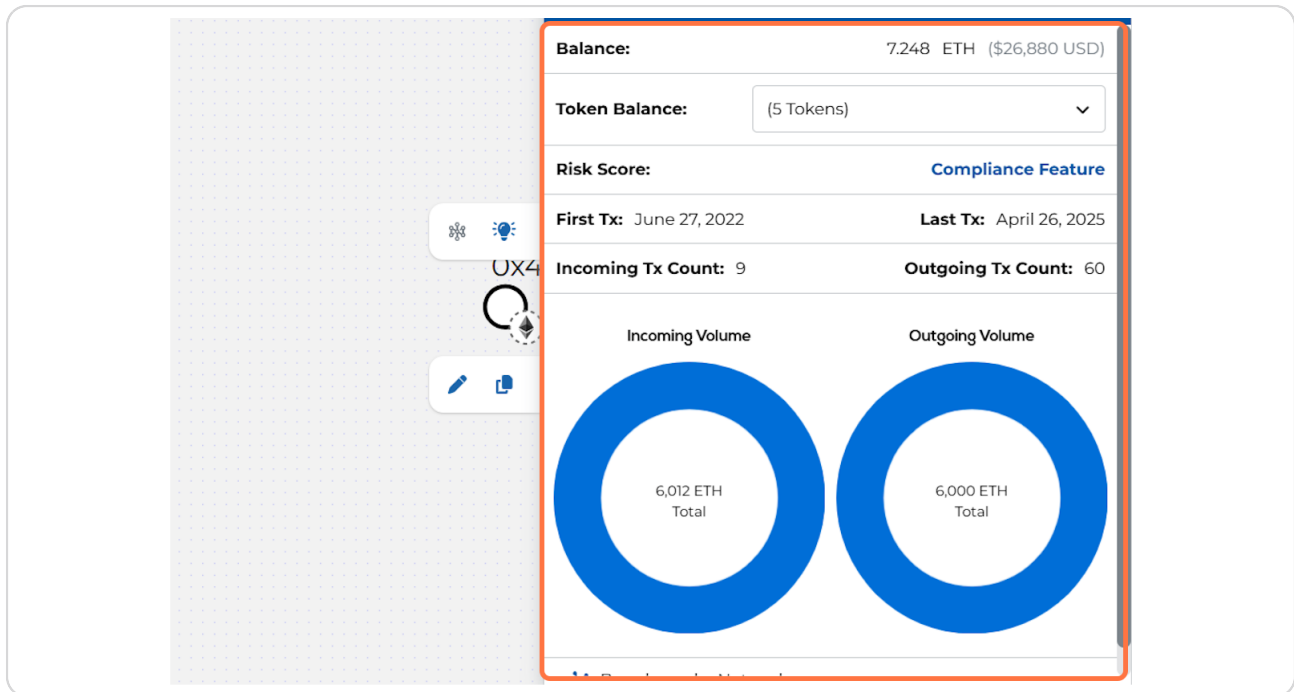
“This is the Lazarus-linked wallet we’re investigating. Breadcrumbs visualizes it as a central node, ready for path analysis.”



STEP 9

View wallet ETH balance after Tornado transfer

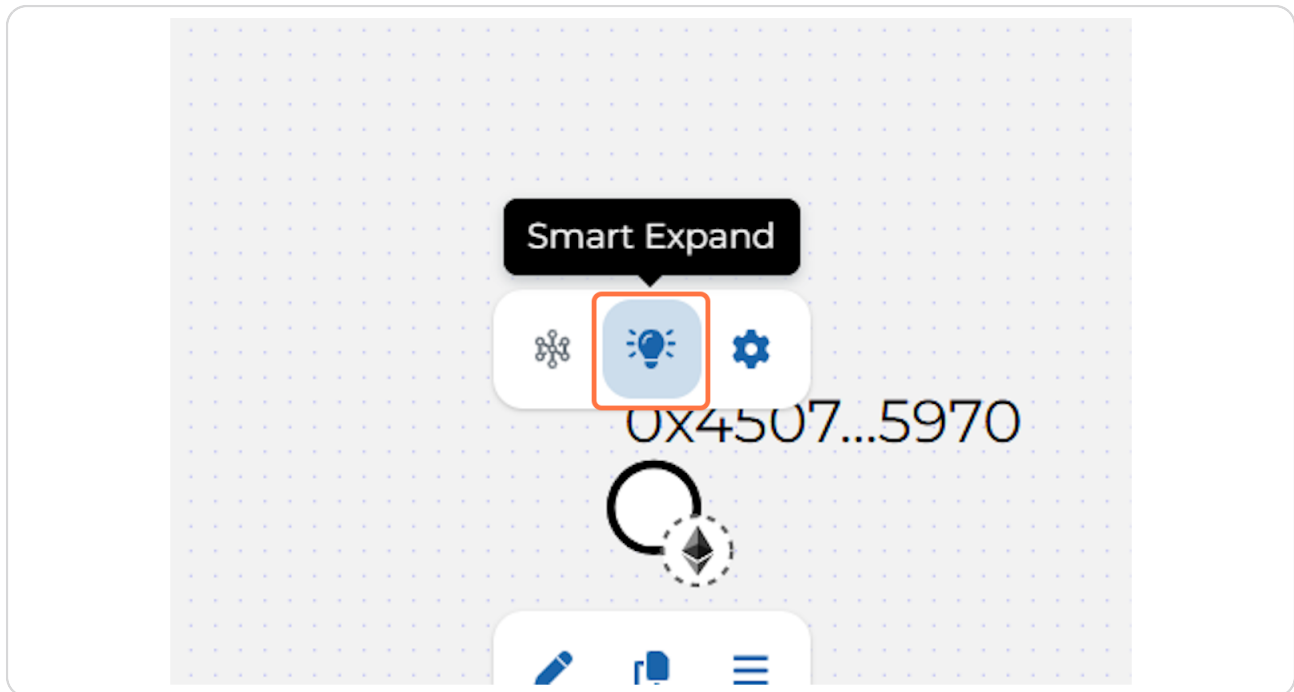
After sending 100 ETH to Tornado Cash, this wallet's balance decreased accordingly. This helps confirm the funds were actually moved and not spoofed



STEP 10

Expand outgoing flow to Tornado Cash

Expand the wallet's outgoing edges. We see a 100 ETH transfer to Tornado Cash Router — confirming the start of the laundering path.



STEP 11

Add Tornado Cash node to the graph

We click on the Tornado Cash node to display its connections. This mixer receives funds from many sources and fragments them for anonymity.

SMART EXPAND ⓘ
Helps trace your funds through an address.

Transaction Relationship

Ethereum data last updated **9 minutes ago** at block **#22991913**

Node Visualizer

Transactions (69)

Filter 0 No filter selected Export to CS

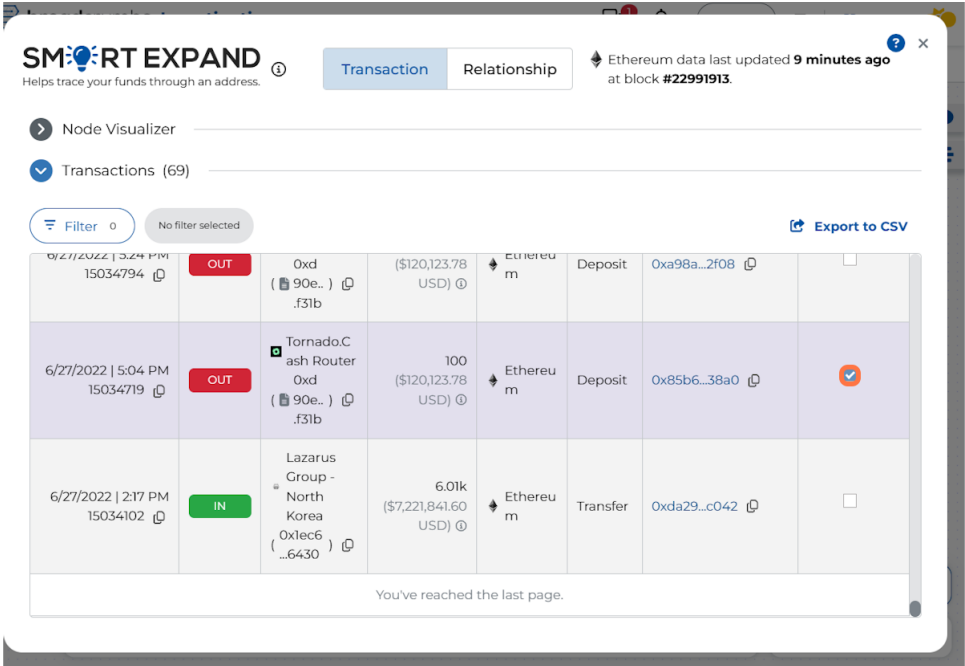
6/27/2022 3:24 PM 15034794 ⓘ	OUT	Oxd (90e..) ⓘ .f31b ⓘ	(\$120,123.78 USD) ⓘ	Ethereu m ⓘ	Deposit	Oxa98a...2f08 ⓘ	☐
6/27/2022 5:04 PM 15034719 ⓘ	OUT	Tornado.C ash Router Oxd (90e..) ⓘ .f31b ⓘ	100 (\$120,123.78 USD) ⓘ	Ethereu m ⓘ	Deposit	Ox85b6...38a0 ⓘ	☐
6/27/2022 2:17 PM 15034102 ⓘ	IN	Lazarus Group - North Korea Oxlec6 (...6430) ⓘ	6.01k (\$7,221,841.60 USD) ⓘ	Ethereu m ⓘ	Transfer	Oxda29...c042 ⓘ	☐

You've reached the last page.

STEP 12

View outgoing fragmentation from Tornado Cash

Once funds enter Tornado Cash, they are fragmented into smaller transfers to many wallets. This obfuscates the destination and breaks the trace.



The screenshot displays the SMART EXPAND web application interface. At the top, the logo "SMART EXPAND" is visible with the tagline "Helps trace your funds through an address." Below the logo, there are two tabs: "Transaction" (selected) and "Relationship". A notification states "Ethereum data last updated 9 minutes ago at block #22991913." The main content area shows a list of transactions. The first transaction is dated 6/21/2022 at 5:04 PM, with a value of 100 ETH (\$120,123.78 USD), categorized as a "Deposit" to a Tornado.Cash Router. The second transaction is dated 6/21/2022 at 2:17 PM, with a value of 6.01k ETH (\$7,221,841.60 USD), categorized as a "Transfer" from Lazarus Group - North Korea. The interface includes a "Filter" button, a "No filter selected" indicator, and an "Export to CSV" link. A message at the bottom indicates "You've reached the last page."

Date	Time	Address	Value	Unit	Type	Destination	Action
6/21/2022	5:04 PM	0xd...f31b	100	ETH (\$120,123.78 USD)	Deposit	0xa98a...2f08	<input type="checkbox"/>
6/21/2022	5:04 PM	0xd...f31b	100	ETH (\$120,123.78 USD)	Deposit	0x85b6...38a0	<input checked="" type="checkbox"/>
6/21/2022	2:17 PM	0x1ec6...6430	6.01k	ETH (\$7,221,841.60 USD)	Transfer	0xda29...c042	<input type="checkbox"/>

STEP 13

Check Tornado Cash inflows

We look at the IN tab on Tornado Cash to confirm this wallet was a real depositor. This step shows multiple wallets sending in similar amounts – common in laundering patterns

The screenshot shows the SMART EXPAND interface with the 'Transaction' tab selected. The 'IN' tab is active, displaying a list of transactions. A transaction from 'Lazarus Group - North Korea' is highlighted with a red box. The transaction details are as follows:

Date	Type	From	Amount	Asset	To	Check
6/27/2022 5:04 PM 15034794	OUT	0xd...90e...f31b	(\$120,123.78 USD)	Ethereum	Deposit	<input type="checkbox"/>
6/27/2022 5:04 PM 15034719	OUT	Tornado.Cash Router 0xd...90e...f31b	100 (\$120,123.78 USD)	Ethereum	Deposit	<input checked="" type="checkbox"/>
6/27/2022 2:17 PM 15034102	IN	Lazarus Group - North Korea 0x1ec6...6430	6.01k (\$7,221,841.60 USD)	Ethereum	Transfer	<input type="checkbox"/>

The interface also includes a 'Filter' button, a 'No filter selected' status, and an 'Export to CSV' link. A message at the bottom states 'You've reached the last page.'

STEP 14

Verify anonymity of outputs

The OUT tab shows hundreds of small ETH transfers to unrelated wallets. These outputs are anonymized and impossible to follow without advanced forensic access — proving the effectiveness of mixing

SMART EXPAND

Helps trace your funds through an address.

Transaction

Relationship

Ethereum data last updated 9 minutes ago at block #22991913.

> Node Visualizer

> Transactions (69)

Filter 0

No filter selected

Export to CSV

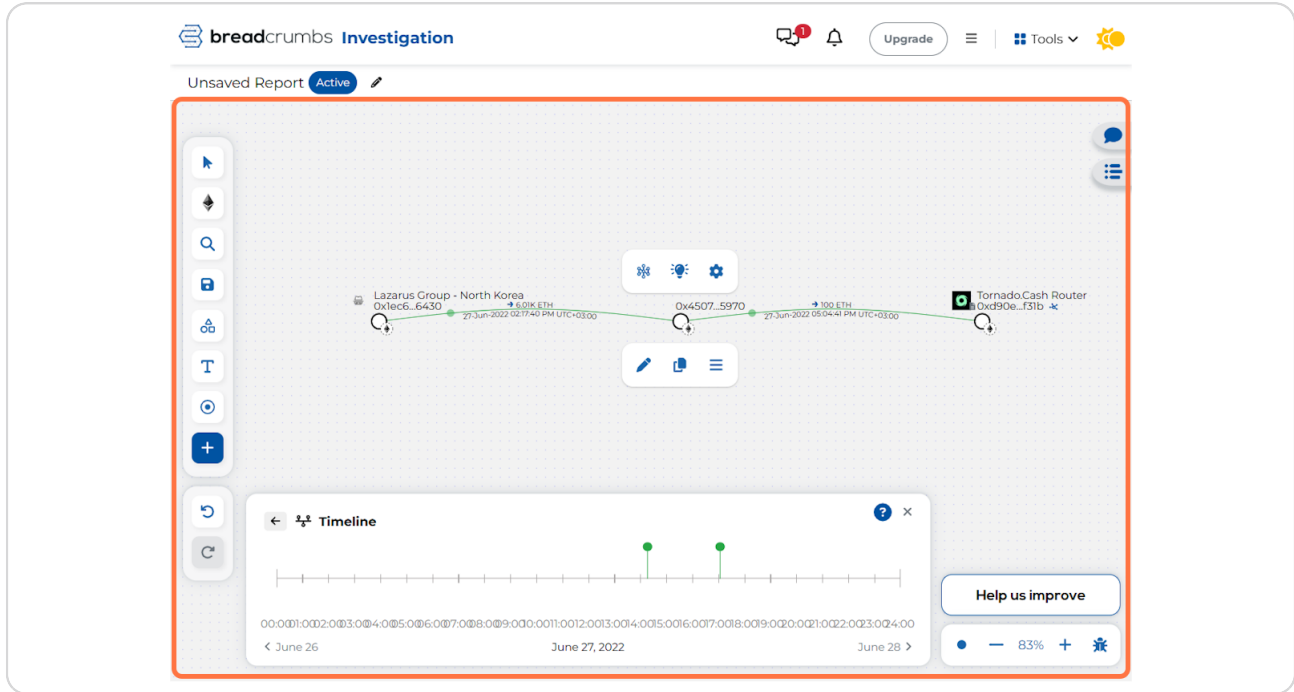
6/27/2022 5:24 PM 15034794	OUT	Oxd (90e.) .f31b	(\$120,123.78 USD)	Ethereu m	Deposit	Oxa98a...2f08	
6/27/2022 5:04 PM 15034719	OUT	Tornado.C ash Router Oxd (90e.) .f31b	100 (\$120,123.78 USD)	Ethereu m	Deposit	Ox85b6...38a0	<input checked="" type="checkbox"/>
6/27/2022 2:17 PM 15034102	IN	Lazarus Group - North Korea Ox1ec6 (...6430)	6.01k (\$7,221,841.60 USD)	Ethereu m	Transfer	Oxda29...c042	<input checked="" type="checkbox"/>

You've reached the last page.

STEP 15

Analysis Summary: Lazarus to Tornado

This investigation shows that a Lazarus Group-linked wallet received 6,010 ETH and fragmented it via Tornado Cash. This pattern is commonly used in laundering and obfuscating large-scale illicit funds.



STEP 16

Investigation completed by Shad Shaho

- **GitHub:** github.com/ShadSF
- **Telegram:** @shad1134
- **Project:** On-chain trace of Lazarus Group funds into Tornado Cash

Tango

Never miss a step again. Visit [Tango.ai](https://tango.ai)