



ZachXBT @zachxbt

Dec 7, 2023 · 9 tweets · [zachxbt/status/1732790450350703052](https://twitter.com/zachxbt/status/1732790450350703052)

1/ Throughout this year I have been monitoring someone who has withdrawn 11,200+ ETH (\$25M) from Tornado Cash and spent the majority of it on Magic The Gathering (MTG) trading cards.

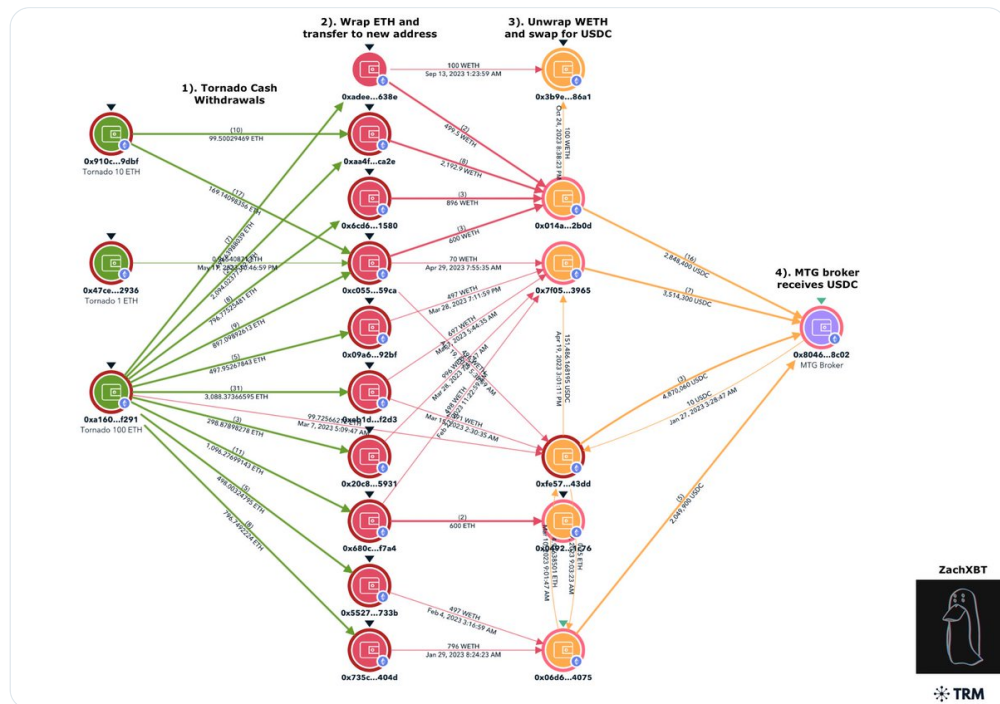
Here's my analysis of where the funds went and what the potential source of funds could be.

2/ This person has withdrawn 110 X 100 ETH from Tornado to 11 addresses.

After they would:

- 1) Wrap the ETH
- 2) Transfer WETH to new address
- 3) Unwrap the WETH
- 4) Transfer USDC to MTG broker

(this is a strategy used to trick KYT at exchanges)



3/ After USDC was sent to a MTG US based broker that accepts crypto

How did I find the broker used?

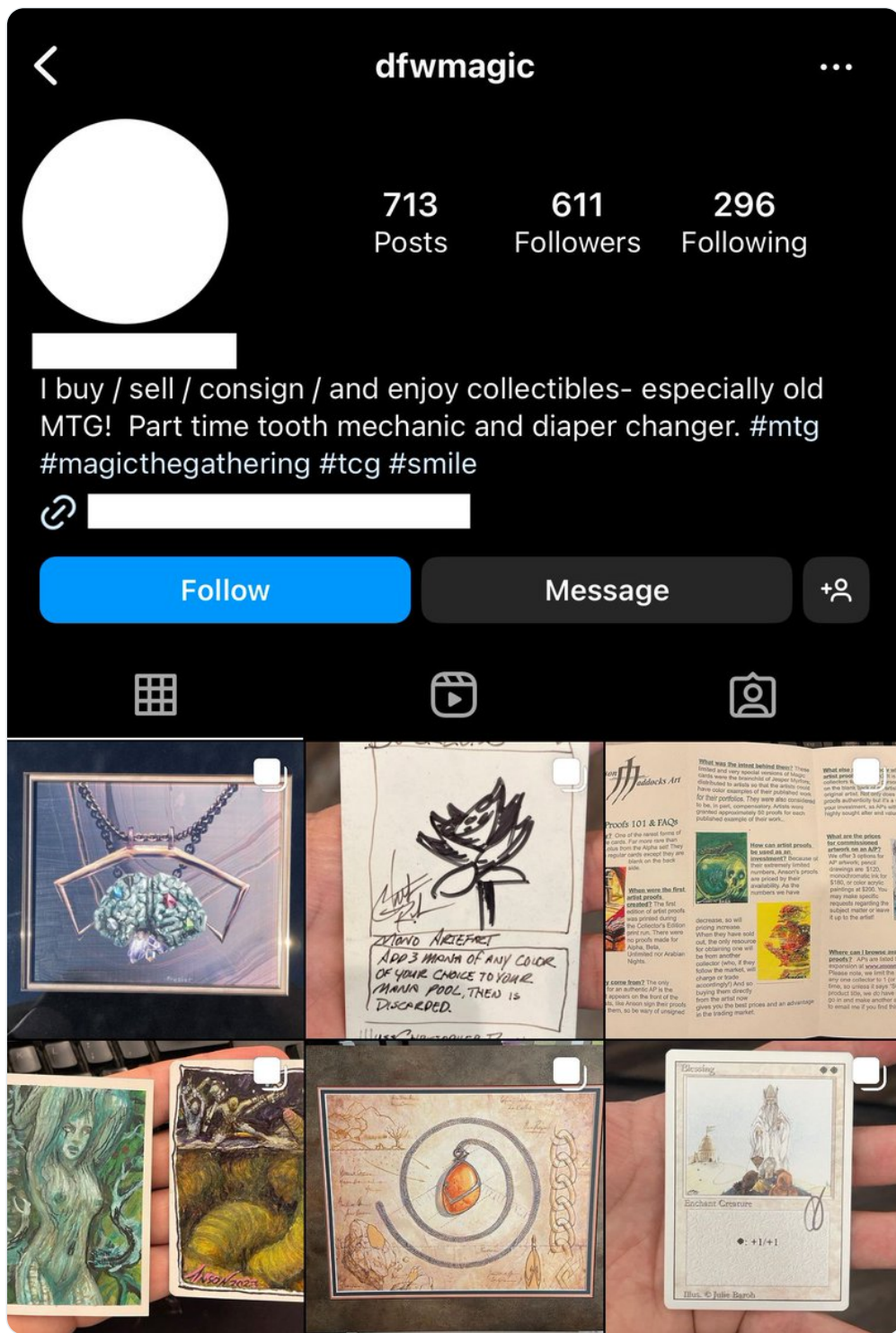
- 1) Instagram username was same as on OpenSea
- 2) Directly contacted a few MTG sellers the broker interacted w/ on-chain

Broker address

0x80462101b56cb4125c645ff299d3e20c1d908c02



The image shows a screenshot of a user profile on the OpenSea platform. At the top, the OpenSea logo is on the left, and navigation links for 'Drops', 'Stats', and 'Create' are on the right. The profile features a large, circular, lime-green avatar. Below the avatar, the username 'Dfwmagic' is displayed in a large, bold font. Underneath the name, the wallet address '0x8046...8c02' and the text 'Joined August 2021' are visible. A link labeled 'What's to know?' is positioned below the join date. At the bottom of the profile, there are five tabs: 'Collected 41', 'Offers made', 'Deals', 'Created', and 'Favorited'. The 'Collected 41' tab is highlighted with a dark background.



4/ After contacting MTG sellers were where things became interesting.

-buyer was spending millions on starter decks, alpha sets, sealed boxes

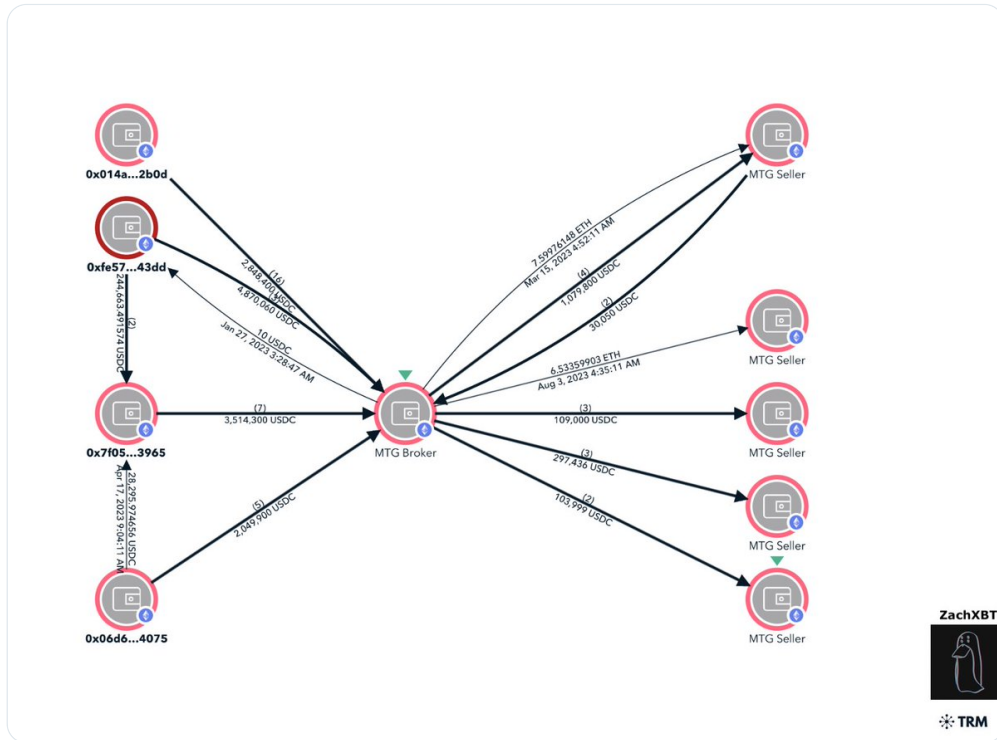
-buyer seemed to be overpaying by 5-10%

-buyer sent crypto up front and broker met up IRL with seller

-buyer was unknown to seller

-said the broker has limited crypto knowledge (likely does not know about Tornado)

seller names will be kept private for their safety



5/ The funds also go to various deposit addresses at Kraken, Bitpay, and Coinbase.

- 0x34e158883efc81c5d92fde785fba48db738711ee
- 0x3a43ac6baf1fa6bdbc966dbdfe26cf545131898e
- 0x85cb90db50608a950858e023509d6a7fa289e212
- 0xbfe6def287c402114d39d0156e17fda79efff4d2

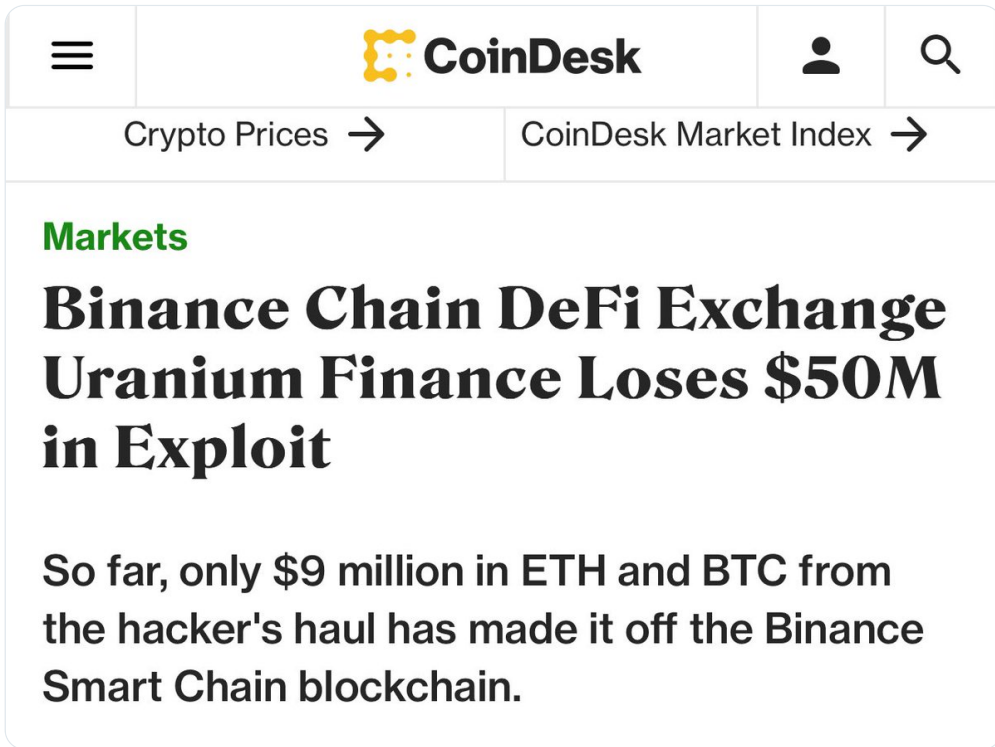
6/ Where do I think these funds could have originated from?

To start I began looking at the top Tornado depositors who were active throughout the past year using a Dune query created by @bax1337

- Anubis (12400 ETH)
- Cashio (11500 ETH)
- Uranium (11303 ETH)

Using timing and multi denomination reveal heuristics I arrived at the thesis that the funds potentially originated from the \$50M Uranium Finance hack that occurred in April 2021.

Anubis had previously potentially been solved however and Casino did not deposit enough ETH earlier in the year to match the withdrawals of this person.

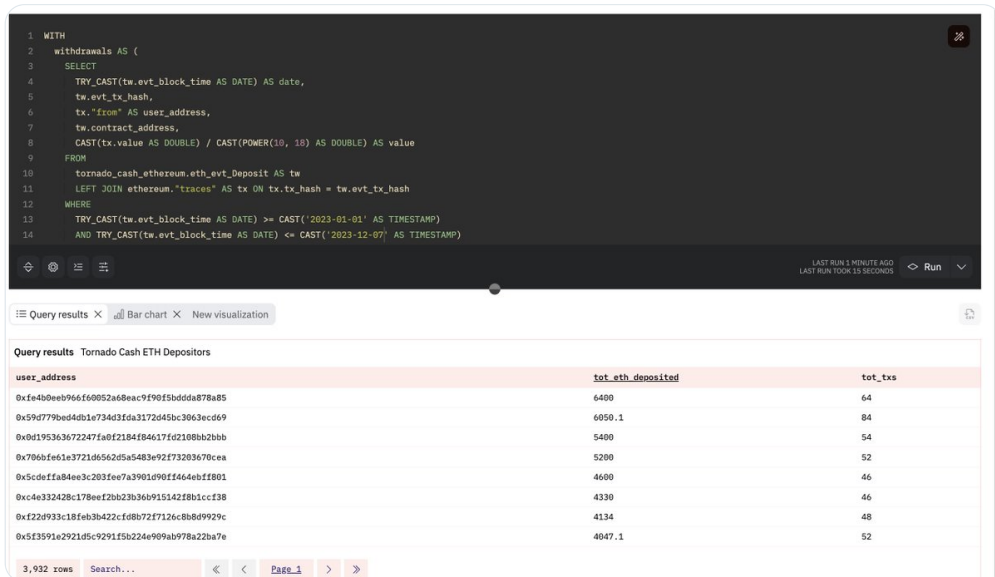


☰ **CoinDesk** 👤 🔍
 Crypto Prices → CoinDesk Market Index →

Markets

Binance Chain DeFi Exchange Uranium Finance Loses \$50M in Exploit

So far, only \$9 million in ETH and BTC from the hacker's haul has made it off the Binance Smart Chain blockchain.



```

1 WITH
2 withdrawals AS (
3   SELECT
4     TRY_CAST(tw.evt_block_time AS DATE) AS date,
5     tw.evt_tx_hash,
6     tx."from" AS user_address,
7     tw.contract_address,
8     CAST(tx.value AS DOUBLE) / CAST(POWER(10, 18) AS DOUBLE) AS value
9   FROM
10    tornado_cash_ethereum.eth_evt_Deposit AS tw
11   LEFT JOIN ethereum."traces" AS tx ON tx.tx_hash = tw.evt_tx_hash
12  WHERE
13    TRY_CAST(tw.evt_block_time AS DATE) >= CAST('2023-01-01' AS TIMESTAMPTZ)
14    AND TRY_CAST(tw.evt_block_time AS DATE) <= CAST('2023-12-07' AS TIMESTAMPTZ)
  
```

Query results Tornado Cash ETH Depositors

| user_address | tot_eth_deposited | tot_txs |
|--|-------------------|---------|
| 0x1e4b0eeb966f60952a68eac9f90f5ddda878a85 | 6400 | 64 |
| 0x59d779bed4db1e734d3fda3172045bc3063ec6d9 | 6050.1 | 84 |
| 0x0d195363672247fa0f2184f84617f02108bb2bbb | 5400 | 54 |
| 0x706bfe1e3721d6562d5a5483e92f73203670cea | 5200 | 52 |
| 0x5cdefa84ee3c2031ee7a3901d90f1464ebf1f801 | 4600 | 46 |
| 0xc4e332428c178ee22b23b60915142f8b1ccf38 | 4330 | 46 |
| 0xf22d933c18feb3b422cf88b72f7126c8b8d9929c | 4134 | 48 |
| 0x5f3591a2921d5c9291f5h224e909ab978a22ba7e | 4047.1 | 52 |

3,932 rows Search... Page 1

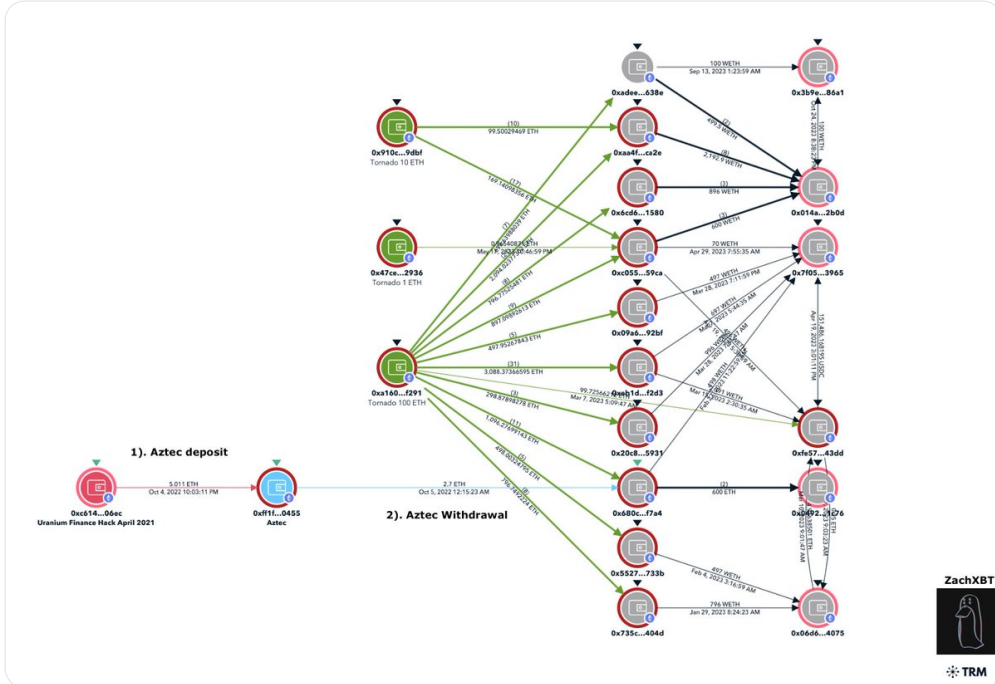
7/ Here's some of my rationale behind it being the Uranium hacker:

Oct 4, 2022 the Uranium hacker deposited 5.01 ETH total to Aztec (privacy tool) at 22:03 UTC

0xd332be2c39de1f4ecd4ef6ce23ae826906a8a144ebbf9cf2a74c7d320f563

Just 2 hours later at 00:15 UTC on Oct 5 this person received 2.7 ETH from Aztec

0x2b8745157bd13cb7aa76444af67e7deobfob288bff50886b599942a17e0e298c

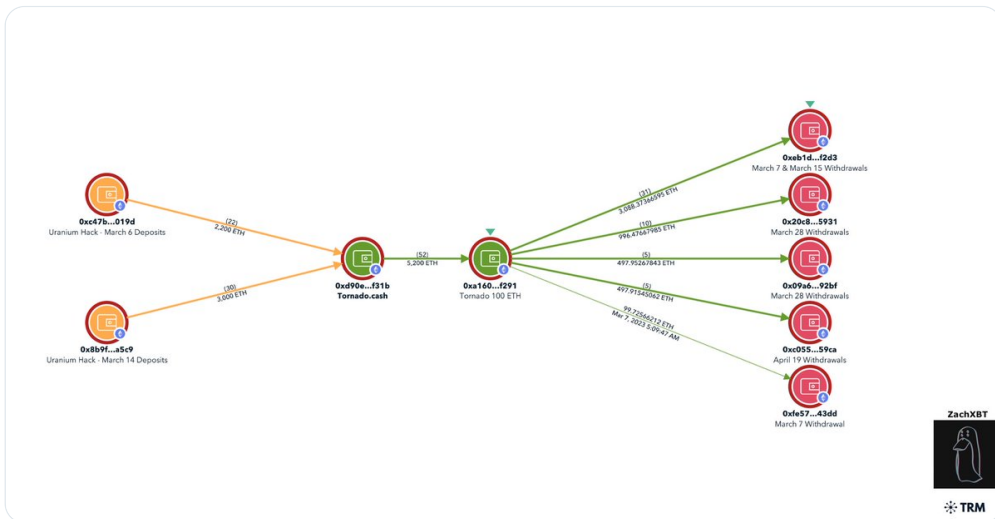


8/ In March 2023 the Uranium hacker deposited 52 X 100 ETH to Tornado & this person received 52 X 100 ETH

March 6 & 14: Uranium Hacker deposits 52 X 100 ETH to Tornado

March 7 & 15: Our person withdrew huge volumes from Tornado

After they finished the Uranium hacker deposits more in May



9/ While my analysis could be incorrect I find it very suspicious that this person:

- spends 8 figures on MTG
- is overpaying for MTG
- shields identity through broker who likely does not know what Tornado is

- receives \$13.2M from Tornado post OFAC while in the US
- uses WETH method to obfuscate source

...