Written by an anonymous guy and prepared by Mr.B: *https://twitter.com/bbbb*

BZX Hacked Uranium Finance?
Tracking with Tornado Cash

Uranium Finance Exploits Research

We have researched some strong **indirect** evidence that some core team member(s) behind BZX protocol can be related to both 2 exploits of the Uranium Finance project. The core members of this team are US citizens:

Kyle Kistner
https://twitter.com/betheb0x
Tom Bean
https://twitter.com/tcbean

Some general info about them:
https://cointelegraph.com/top-people-in-crypto-and-blockchain/kyle-kistner
https://www.plexusrs.com/tom-bean-kyle-kistner-bzx-network-interview/

Their project Bzx protocol was exploited 3 times.
https://cointelegraph.com/news/the-unluckiest-defi-protocol-a-personal-take-on-bzx-s-tumultuous-year

Some general info about them:
https://cointelegraph.com/top-people-in-crypto-and-blockchain/kyle-kistner
https://www.plexusrs.com/tom-bean-kyle-kistner-bzx-network-interview/

It is hard to imagine that even one of those well-known people in crypto space can be involved in those hacks, what to say about both of them, but we have researched 5 indirect facts that point to them with some level of probability.

Fact 1. Possible relation of Bzx team member(s) to the first Uranium Finance exploiter via a chain of funds transfers on blockchain.

The first Uranium Finance exploit case description is here:
https://uraniumfinance.medium.com/uranium-post-mortem-v2-compensations-aac4b0706d7d

The exploiter stole 1m+ usd and sent this funds from bsc network to ethereum network. So it does not look like a white hat attack with the initial intention to return funds.
The Uranium team said that the hacker contacted them and they made a deal that he can take the remaining stolen funds, if he returns 500 eth.

The initial hacker's address is this one
https://bscscan.com/address/0x36ad9ee78bfb730955993d2aa77ecccf95e3313e

He sent funds to his ethereum address:
https://etherscan.io/address/0xaa9da5e217e0a18e2ec8ef16c1c2334bfbd03cc6

Some of these cross-chain transfers are the following:
https://bscscan.com/tx/0x89fea1784be2bc240b934d1d41e337dbe1111ad7a08dbdb3569bf1130687acdc
https://bscscan.com/tx/0x4312f8435cb273834779addf52ad72a1a7111adbeb098d991e5f9d915c6b6ac3
https://bscscan.com/tx/0x9116fddb1022f56c40f11e47f1332580add9414765d4390510e54402e6288102

Ethereum network.
The address, which received stolen funds is this one:
https://etherscan.io/address/0xaa9da5e217e0a18e2ec8ef16c1c2334bfbd03cc6

It also received 10 eth from the address below after returning 500 eth to the Uranium Finance team.
https://etherscan.io/address/0x36ad9ee78bfb730955993d2aa77ecccf95e3313e

https://etherscan.io/tx/0xd6afdad93143305cbed0ea6bedda007ccaa4d7634f9263dc34252a0aeceb0f90

This address 0x36ad9ee78bfb730955993d2aa77ecccf95e3313e received its first eth from
https://etherscan.io/address/0x821352e950db90decb228da89aaff3b532f4d652

https://etherscan.io/tx/0x49c096b4c1b8adb32286b8630729851e36584b0080e00ab1f98132925b7abb6d

This address 0x821352e950db90decb228da89aaff3b532f4d652 received its first eth from
https://etherscan.io/address/0x52ad87832400485de7e7dc965d8ad890f4e82699

https://etherscan.io/tx/0x60c406b949fa7478970fd3efda6f2f6a7f171311fa0721c9d2903c75f7bec61f

So https://etherscan.io/address/0x52ad87832400485de7e7dc965d8ad890f4e82699 is connected to the address, which received stolen funds:
https://etherscan.io/address/0xaa9da5e217e0a18e2ec8ef16c1c2334bfbd03cc6

And it is likely there is one person behind them.

Also 0x52Ad87832400485DE7E7dC965D8Ad890f4e82699 did a small cross-chain transfer of 0.0476 eth from bsc to ethereum network with eth anyswap tokens (which were also used by the exploiter)
https://bscscan.com/tx/0x04f09f6acd6ceaaf2e015844ae5dc7f3d2fe9cfe7f632a1644bc5ce447f7c633 at Apr-09-2021 12:54:24 AM +UTC
A very small amount of 0.0476 eth was transferred, which is not comparable with the amount of funds operated by this address.

The exploiter did a 4+ minutes pause between his transactions exactly at the time of that transfer by 0x52Ad87832400485DE7E7dC965D8Ad890f4e82699.

Apr-08-2021 12:53:14 AM +UTC
https://bscscan.com/tx/0x71b331535c018cb17f29571c265e2d14d929eaba0cedc8e365d218ee1b35dc27

Apr-08-2021 12:57:53 AM +UTC
https://bscscan.com/tx/0x8776da8f32ced03a66f2d2e51c2a76198010f958fc90845977e24b85e3f1e1f0

At other moments transactions were executed every minute.

Also notice, that 0x52Ad87832400485DE7E7dC965D8Ad890f4e82699 received 737,153.086036 ($302,974.34) **bzrx** tokens from binance hot wallet.
https://bscscan.com/tx/0x57f0165432ab5fa213df10e268118bc057c3c77e2d016bf8f3556652789e7c67

And sent them to the address
https://bscscan.com/address/0xb7cfb4dd07a7b183bac63170118c2361dcf3e742

https://bscscan.com/tx/0x61c0e74ad1a65988a08839053271358a906ba6cd9c387c8923a7ba4cc158803f

0x52Ad87832400485DE7E7dC965D8Ad890f4e82699 also sent around 5m busd to another related address
https://bscscan.com/address/0xb7cfb4dd07a7b183bac63170118c2361dcf3e742

https://bscscan.com/tx/0x832a52f8211a6ae8c617bbc4b80e4ae6b83a4fe2484ae245d66e110a9bf1cf8e

https://bscscan.com/tx/0x3dfbdd63a7f6a55d1adedc1ee4a3d50ed3245317c712575874554b69645fb56c

Just remember this address 0xb7cfb4dd07a7b183bac63170118c2361dcf3e742 for future reference.

0x52Ad87832400485DE7E7dC965D8Ad890f4e82699 has interaction with the address 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9 via a chain of funds transfers. This

address 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9 belongs to the Bzx team (explained below).
https://etherscan.io/address/0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9

Transactions chain:

1)

0x52Ad87832400485DE7E7dC965D8Ad890f4e82699 - 0xdC63983db369BE1596F5F511bd903B716509801a

https://etherscan.io/tx/0x1db2797b1bbb602ea21c35fbbdeff903b2de65de8532ec2a4963b35802d86a6e 933 eth

https://etherscan.io/tx/0x2edfae1195985580a09bbe82ccbe8776dbcc8f4aecb62b948e86a895e4454177 37,900 dai

0xdC63983db369BE1596F5F511bd903B716509801a - 0xDa495C2Ab0a91623564126778D5AB20fA87C1DFc

https://etherscan.io/tx/0x310bb2d8d5c314966fc773e6c838383ae4489beeea9851e47e33fba665006f7c 31.30 eth

https://etherscan.io/tx/0x50817b76e0151ce5937122356ed639c7935a2536acbf98bb2e95e68d27348421 61 eth

https://etherscan.io/tx/0x4e4276cc781e611fbd7d218870c9f91f5e6904a8e73d62d921229c51294146fc 1.17 eth
and 3 more transactions.

0xDa495C2Ab0a91623564126778D5AB20fA87C1DFc - 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9

https://etherscan.io/tx/0x8eb6865c92a7c65cf421ae0b494aa740cddc3b972f26a85860c13d213b5056c9 3,454,275.61 usdc
https://etherscan.io/tx/0x05c62c47053a1f38ec9953e5ef142b31ed7f9afdfb7d580e1f0c3d1ceae9b512 504.40 eth

2)

0x52Ad87832400485DE7E7dC965D8Ad890f4e82699 - 0x813413997503e41173f210c908cdb3528835cd42

https://etherscan.io/tx/0xe22876e166c19916aafeeff50601209e15abc1bfc15f2cbf738d00ea1eaec9d4 10.7 cream

https://etherscan.io/tx/0xa7386d6ec8f53ebfc3c686bc00423d84fbb3ff8f315a200ddd56428772e43786 13.8 cream

https://etherscan.io/tx/0xed6d81791328d7deae1fd077c7f14a76d0c6efe3762a3fe1094fc6452e287f22 13,000 usdc

0x813413997503e41173f210c908cdb3528835cd42 - 0xDa495C2Ab0a91623564126778D5AB20fA87C1DFc

https://etherscan.io/tx/0xb43f3174d9ee929cde5dc648f6e4660f872c67f7916420300563f1ed5f403fb5 16.54 cream

https://etherscan.io/tx/0xdb1a863e0d331d3b3b418ff21d2905f19257f2805c220f7154dc08a640b9812e 1075 eth

https://etherscan.io/tx/0x4f23ae03840f9f8829a60230e5149721f2afc336765a0c2fe2090ab110dc2792 3000 cream

https://etherscan.io/tx/0x0829ba6cdab7cee783f43d25c9632501fb5eb560a49b81304b246cb1142d081d 1,075 eth
and 12 more transactions.

0xDa495C2Ab0a91623564126778D5AB20fA87C1DFc - 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9

https://etherscan.io/tx/0x8eb6865c92a7c65cf421ae0b494aa740cddc3b972f26a85860c13d213b5056c9 3,454,275.61 usdc
https://etherscan.io/tx/0x05c62c47053a1f38ec9953e5ef142b31ed7f9afdfb7d580e1f0c3d1ceae9b512 504.40 eth

Why does the address 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9 belong to the bzx core team because?

It received vbzx vesting tokens
https://etherscan.io/tx/0x493ea9e764ea11dc805cb0fa9ddba6c4330ddcb9e163c51ca01cd00378eb963d 103,000,000 ($10,190,447.16)

It also received bxz tokens from Bzx team vesting contract deployer address
https://etherscan.io/tx/0x99e23d1be5313846328cd1fee774cb128b0d5db9e4b8f3c297d5e3386a43fded 4,665,489 bzrx ($1,916,956.22)

So the first Uranium Finance exploiter is connected with the bzx team address via a short chain of funds transfers.

Fact 2. Possible relation of Bzx team member(s) to the first Uranium Finance exploiter via Tornado Cash transactions.

Bzx team related address 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9 received its first eth in these transactions:
https://etherscan.io/tx/0xafd24ef6d216a484df64cf3fedb3f3e2e0892f8cecf4390125e1547605934d12 Apr-16-2021 11:34:04 PM +UTC
https://etherscan.io/tx/0x75d4ab8bdb5c3bc22c86541859231e776112d91304db0a3bff68c61f3ce63cf6 Apr-16-2021 11:58:16 PM +UTC

The address which sent those initial eth is this one:
https://etherscan.io/address/0x243fbe211592e5244ca1f7f941f2f3dd0a854fbd

A few minutes after receiving initial eth 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9 transferred bzx tokens, so the owner of the address, which sent eth and the owner of 0x83b9e8A7FD1373022172Ba571cd4E1f6463998C9 are likely the same person.

https://etherscan.io/tx/0x6d6baed27d0342e83137f7979ba9f8ecb555ee29ef66236c301bbb0cf49f460e Apr-17-2021 12:01:23 AM +UTC

0x243fbe211592e5244ca1f7f941f2f3dd0a854fbd has only 9 incoming transactions.
One transaction is from Aztec service and 8 transactions are from Tornado Cash:
https://etherscan.io/address/0x243fbe211592e5244ca1f7f941f2f3dd0a854fbd#internaltx

Split of Tornado Cash transactions is this ones:
4 transactions of 10 eth.
4 transactions of 1 eth.

The first transaction is this one
https://etherscan.io/tx/0x0e8e47bcc0596ab66289c2fbae7a3fe7a802c72f4ce3426aac6210cd8dd08980 Time: Apr-10-2021 08:03:08 AM +UTC

The first Uranium Finance Exploiter sent the remaining funds to Tornado Cash after returning 500 eth to the Uranium Finance team. Review the list of transactions here: https://etherscan.io/address/0xaa9da5e217e0a18e2ec8ef16c1c2334bfbd03cc6

Split of its Tornado Cash transactions:
1 transaction of 100 eth.
8 transactions of 10 eth.
4 transactions of 1 eth.

The first transaction is this one:
https://etherscan.io/tx/0xfeb35153742ecccd7a34a141255649be29112828fbbb0971ed0af9e3f69bad45 Apr-10-2021 01:03:12 AM +UTC

The last transaction is this one:
https://etherscan.io/tx/0xe8a6622f20ce3534a2fdb2ea2d5dbd40e079d2a1f9350b2381b7a8c58b15c651 Apr-10-2021 01:45:02 AM +UTC

The first Uranium Finance Exploiter address also did a deposit to Aztec service:
https://etherscan.io/tx/0x82acceeddb0a597f54a3d0a477ab96084e9f3cc5fd852c6b685d219ac69f41f7

So it is likely that 0x243fbe211592e5244ca1f7f941f2f3dd0a854fbd is the address, which received funds, sent by the exploiter via Tornado Cash, because of very rare combination of tornado cash withdrawals (4x1 eth and 4x10 eth), matching time frame (first withdrawal was 6-7 hours after depositing funds to Tornado Cash) and also both those addresses interacted with Aztec service.

Fact 3. Possible relation of the first Uranium Finance exploiter to the second Uranium Finance exploiter via Tornado Cash transaction.

0x243fbe211592e5244ca1f7f941f2f3dd0a854fbd was inactive during 8 days after the last transaction
https://etherscan.io/tx/0xc9ce208773e2cea79d8a40669cc5a1938dd0818c7218dd83ce2c1fa4f12bb536 Apr-18-2021 09:59:27 AM +UTC

The only transaction after that date till now was depositing 1 eth to Tornado Cash
https://etherscan.io/tx/0x52a3adf6d763b5c47b79baf962f609897acc73b7090ec812723700fc604eee55 Apr-26-2021 06:17:54 AM +UTC

The second exploiter of Uranium Finance received 1 eth from Tornado Cash on ethereum network in 1 day after 0x243fbe211592e5244ca1f7f941f2f3dd0a854fbd deposited 1 eth to Tornado Cash and then the second exploiter sent this funds to bsc network.

https://etherscan.io/tx/0xc9e276852d873edb60432234daeb2c21a4b3b6b3b7b788606c0be0f772860cba Apr-27-2021 03:32:56 AM +UTC

Fact 4. Possible relation of the first Uranium Finance exploiter to the second Uranium Finance exploiter via depositing funds to Ellipsis Finance.

There is a pattern for the first exploiter and its related addresses on bsc to deposit funds to Ellipsis Finance even for a short period of time, when they do not have any trading positions. Actually this was the very first action, which the first exploiter did after he received funds on bsc network:
https://bscscan.com/tx/0x8c0bc46d2693b65b9402c3a908a20dfb764b183a7c0e77e90daadd5156f7fe6b

The list of such deposits for the first Uranium Finance exploiter and its related addresses:
https://bscscan.com/token/0xaf4de8e872131ae328ce21d909c74705d3aaf452?a=0x36ad9ee78bfb730955993d2aa77ecccf95e3313e
https://bscscan.com/token/0xaf4de8e872131ae328ce21d909c74705d3aaf452?a=0xb7cfb4dd07a7b183bac63170118c2361dcf3e742
https://bscscan.com/token/0xaf4de8e872131ae328ce21d909c74705d3aaf452?a=0x52Ad87832400485DE7E7dC965D8Ad890f4e82699

The second Uranium Finance exploiter also deposited 17.3m of stolen funds to Ellipsis Finance, which it is his biggest allocation of the stolen funds:
https://bscscan.com/tx/0x4ca316eb7d62616bca3b81174f19ff58fe3dd1b122cba49c0b58ccb52167c549

Fact 5. Possible relation of Bzx team member(s) to the second Uranium Finance exploiter via the initial announcement of the incident details.

One of the first people (or even the very first one), who tweeted about which lines of code caused the vulnerability was Kyle Kistne, Bzx co-founder.
https://twitter.com/BeTheb0x/status/1387288334649622528

His tweet was quoted by many sources:
https://thedefiant.io/upstart-amm-uranium-finance-suffers-50m-hack-second-attack-in-a-month/
https://cryptobriefing.com/bsc-protocol-uranium-finance-hacked-50-million/
etc

2 questions here.

1. How did he find the source of the issue so fast?
2. Why is there a black background behind the code lines and the code text is gray on his screenshots? Did he open Uranium Finance contracts in some local IDE software instead of just making screenshots of the source code on github https://github.com (usually white background or a dark mode, but the text color is different) or on bscscan https://bscscan.com (gray background)? If yes and it is really his IDE software, why did he launch Uranium Finance contracts there and when? This is an example how screenshots should look like instead, if just “an average person, passing by” tweets about the incident: https://twitter.com/FrankResearcher/status/1387347025742557186/photo/1

P.S.There is a transaction when the first exploiter related address 0x52ad87832400485de7e7dc965d8ad890f4e82699 interacted with the Integral Protocol contract for the amount of 804,616.87 usdc.
https://etherscan.io/tx/0xe28f771b4c9a0afe8dcd0a96059506382e28315194dde743ec25a68613d72bfd

Tom Bean and Kyle Kistner are both on Integral Resistance’s discord:
https://discord.gg/mGeMwCEgMt

If all the facts above are not a series of coincidences, it is not clear enough if both of Bzx core team members are involved in Uranium Finance exploits or just one of them.