Following Poly Network Attack: Beosin KYT/AML Keeps Tracing Stolen Funds and Unveils Hackers' Tactic

According to Beosin EagleEye security risk monitoring platform, on July 2, the Poly Network cross-chain bridge was suspected of being attacked due to a potential compromise of private keys or a multi-signature service attack. The hacker has exploited forged proofs to initiate withdrawal operations on the cross-chain bridge contracts across multiple chains.

It is not the first time that Poly Network got attacked. As early as August 10, 2021, Beosin EagleEye showed that Poly Network was attacked and nearly 600 million dollars in funds were stolen from the three chains of Ethereum, BSC, and Polygon.

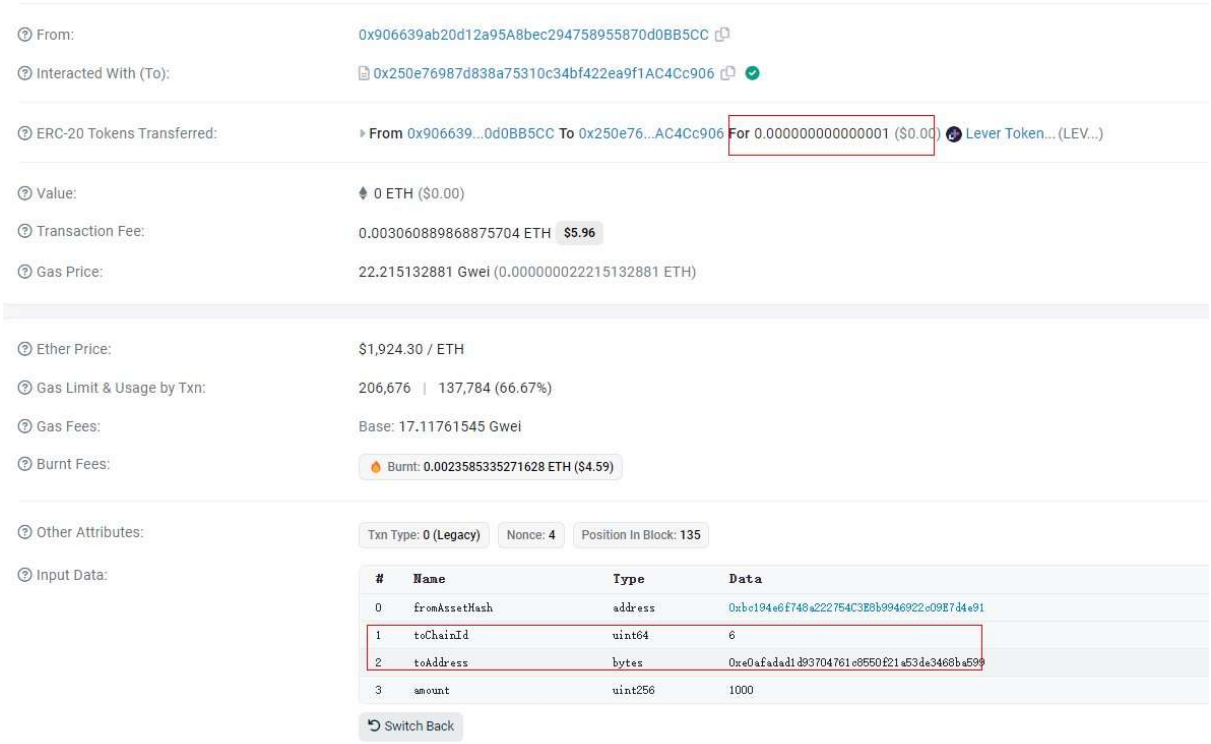
This incident of the year also became the security incident with the largest amount of loss in 2021. Two years ago, the attacker used the logic flaw in the EthCrossChainManager contract to call the putCurEpochConPubKeyBytes function in the EthCrossChainData contract to change the Keeper to the hacker address and then used the address to sign the transaction of withdrawing tokens, thereby withdrawing a large number of tokens in the LockProxy contract. However, under the pressure of many parties, the attacker finally chose to return the stolen assets.

This time, how did the hacker attack Poly Network and deal with the stolen funds? The details are as follows.

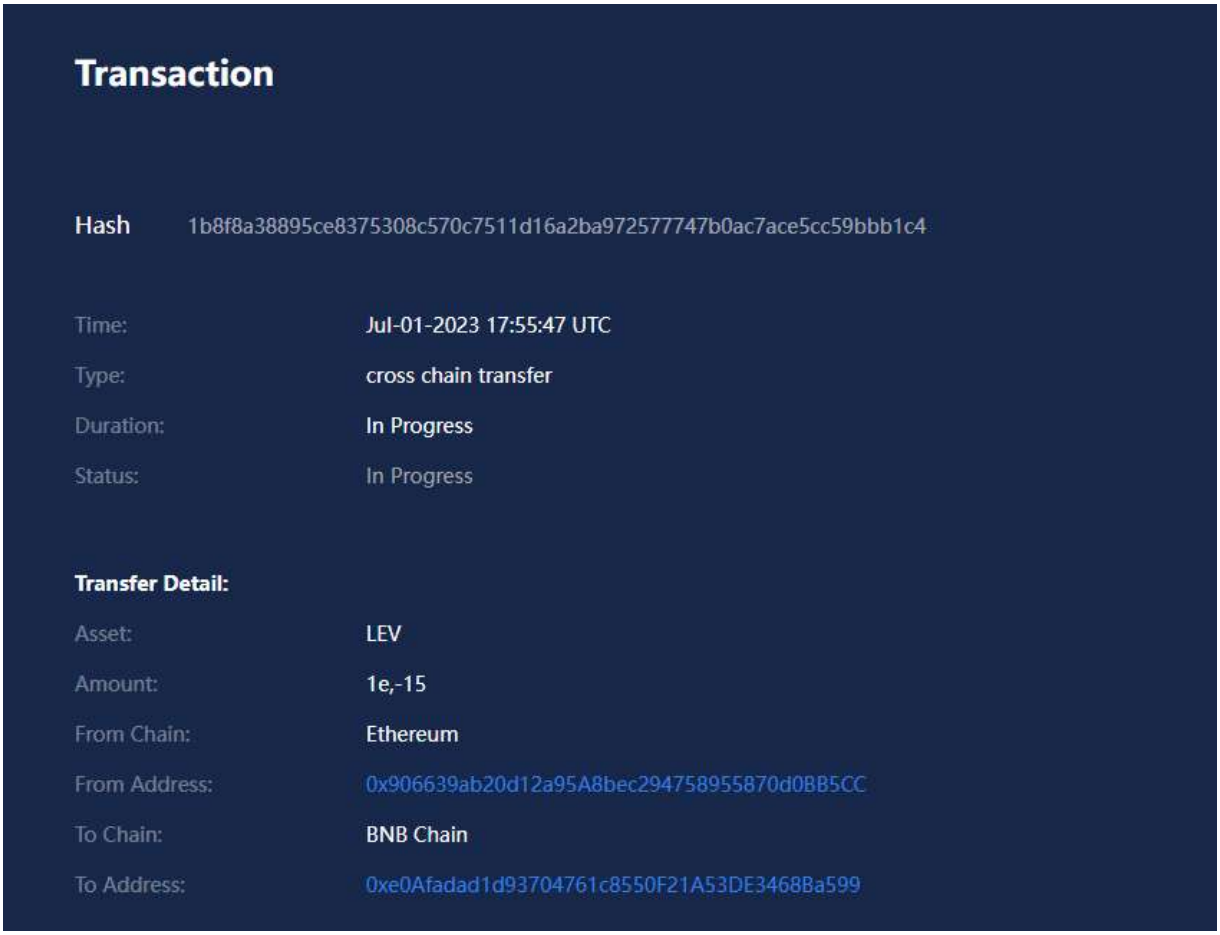
Attack Analysis

Take the attack address 0x906639ab20d12a95a8bec294758955870d0bb5cc as an example:

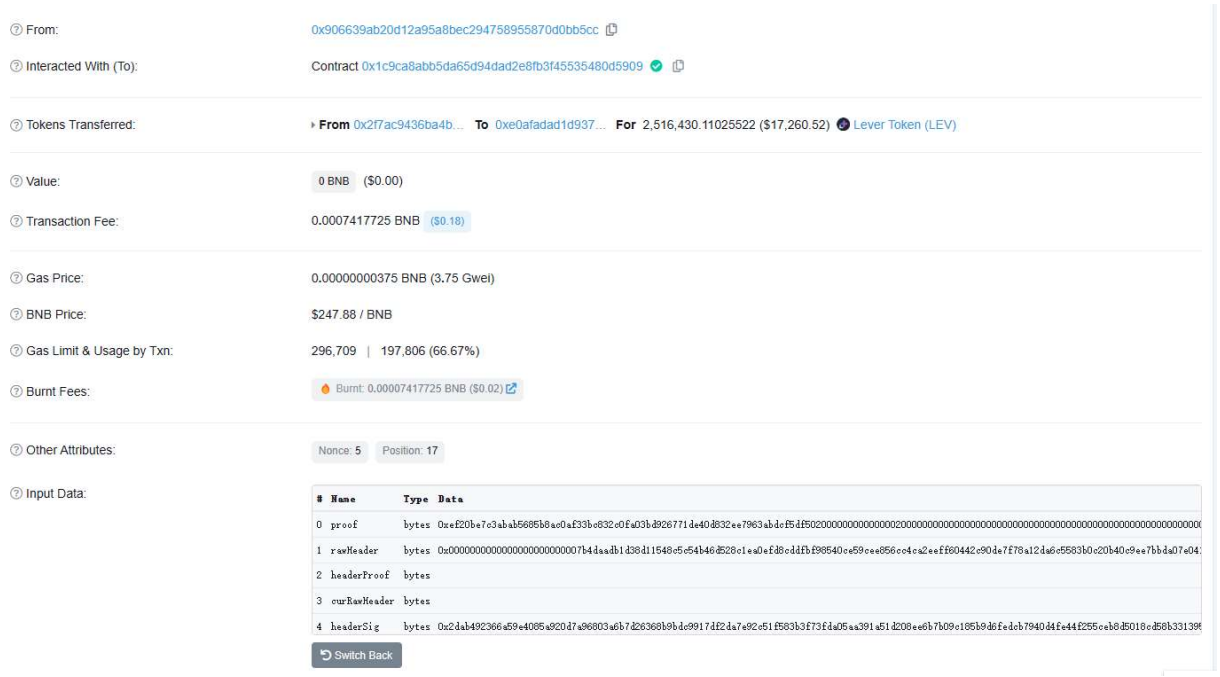
Firstly, the attacker called the lock function on the LockProxy cross-chain bridge contract to lock a small amount of Lever Token.



The toChainId 6 corresponds to the BNB chain, which can be viewed at https://explorer.poly.network. If a transaction is visible on the Poly Network explorer, it indicates that it has been validated through the relay chain.



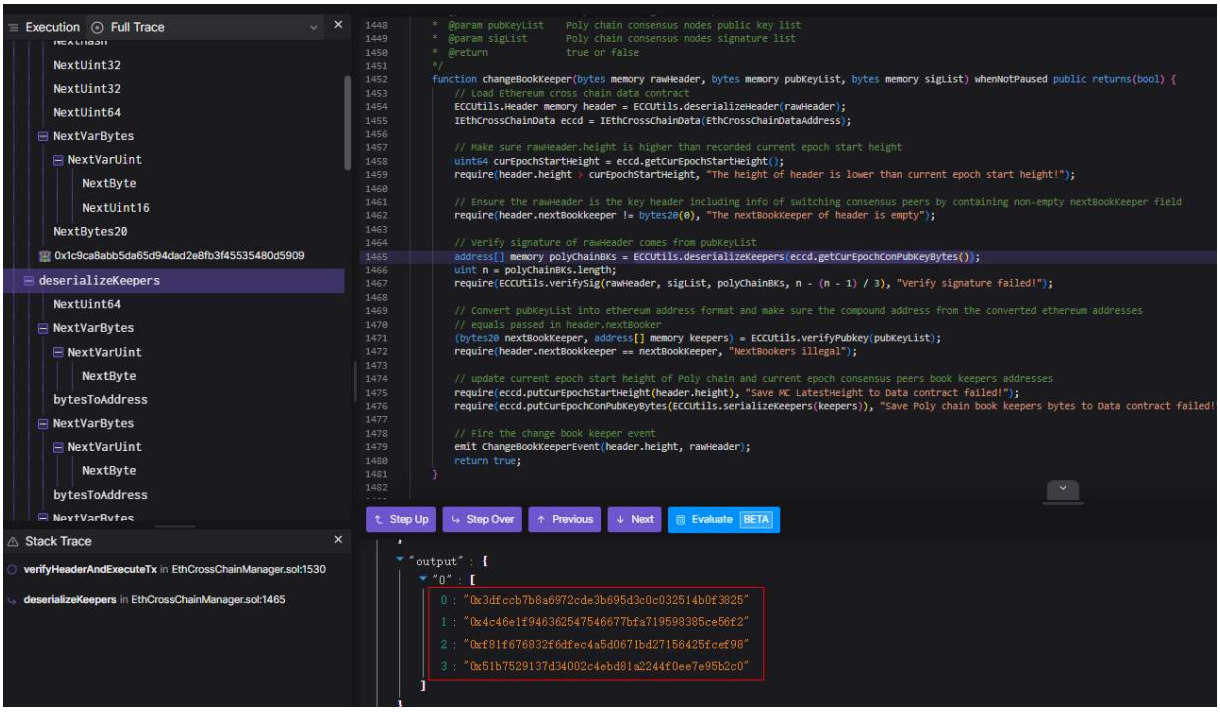
Switching to the BNB chain, the attacker used the verifyHeaderAndExecuteTx function to initiate withdrawal operations, but the quantity involved does not match the original lock amount.



However, upon querying the relay chain network, no record of this transaction was found.

There is now reason to suspect that either the signatures have been leaked or the keepers have been modified.

Keepers are responsible for signing user withdrawals, so controlling a keeper would allow the attacker to initiate withdrawals with forged signatures. The attack on Poly Network in 2021 was caused by hackers using the attack to modify the keeper.



Upon analyzing the attacker's use of the verifyHeaderAndExecuteTx function for withdrawal operations, it was found that the keepers have not been modified.

Now, there is reason to believe that three keepers (0x4c46e1f946362547546677bfa719598385ce56f2, 0x51b7529137d34002c4ebd81a2244f0ee7e95b2c0, 0x3dfccb7b8a6972cde3b695d3c0c032514b0f3825) may have suffered private key compromise or a multi-signature service attack.

At the same time, according to Beosin KYT/AML, **the hackers called the contract of Poly Network through a batch of addresses and used the loopholes in the two functions of UnlockEvent and verifyHeaderAndExecuteTx in the contract to attack the project party and transfer funds to your deposit address.**

The fund flow

On the Ethereum

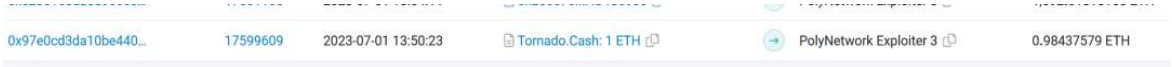
The addresses calling the attacked contract obtained gas fees through a common address.

0xf64d5843d96634dfe...	Transfer	17144348	2023-04-28 11:32:59	0x0dFEb4...8Cb9701C	OUT	0x58c999...953e5201	0.2 ETH	0.0007039
0x3d823911011f0f99e...	Transfer	17144155	2023-04-28 10:53:23	0x0dFEb4...8Cb9701C	OUT	0x080C23...48575f6E	0.2 ETH	0.00068272
0xea19dae4f164539bd...	Transfer	17144118	2023-04-28 10:45:59	0x0dFEb4...8Cb9701C	OUT	0x8c43d3...797d8968	0.2 ETH	0.00103371
0x9672ab880619f163...	Transfer	17143814	2023-04-28 9:44:35	0x0dFEb4...8Cb9701C	OUT	0xB03BAE...f85bFe9A	0.2 ETH	0.00069639
0xc18eec9ad15d3d62...	Transfer	17143711	2023-04-28 9:23:35	0x0dFEb4...8Cb9701C	OUT	0x0Cb079...2c337905	0.2 ETH	0.00112659
0x6f761e7ac4a644090...	Transfer	17143644	2023-04-28 9:10:11	0x0dFEb4...8Cb9701C	OUT	0x1c1B69...5231081A	0.2 ETH	0.00069091
0x60ca19097c27252b...	Transfer	17143605	2023-04-28 9:02:23	0x0dFEb4...8Cb9701C	OUT	0x29A232...f2E3353B	0.2 ETH	0.00074891
0x6ac8fa4a853933cdf...	Transfer	17143549	2023-04-28 8:51:11	0x0dFEb4...8Cb9701C	OUT	0xa59118...2e5fB049	0.2 ETH	0.0006676
0x7c54d6adcf8a8f916...	Transfer	17143518	2023-04-28 8:44:59	0x0dFEb4...8Cb9701C	SELF	0x0dFEb4...8Cb9701C	0 ETH	0.00076047
0xf47a1fc85eabaf408...	Transfer	17143518	2023-04-28 8:44:59	0x0dFEb4...8Cb9701C	OUT	0x906639...0d0BB5CC	0.2 ETH	0.00076026
0x2e58724fb6beccf88...	Transfer	17143372	2023-04-28 8:15:11	0x0dFEb4...8Cb9701C	OUT	0xa052A3...A9a0dDf1	0.2 ETH	0.00066785
0xccb5c63af8c3a42a8...	Transfer	17143290	2023-04-28 7:58:23	0x0dFEb4...8Cb9701C	OUT	0x879ab1...D8180261	0.2 ETH	0.0007663
0x69923ea025e76845...	Transfer	17143252	2023-04-28 7:50:47	FixedFloat	IN	0x0dFEb4...8Cb9701C	6.7569414 ETH	0.000735

Transactions to distribute fees

The address(0x0dfeb429166e629204aca66467484cd88cb9701c) to distribute fees obtained the fee through an exchange called FixedFloat.
There are three sources of fees in total for the hackers' consolidated address.

1. A fee comes from Tornado.Cash

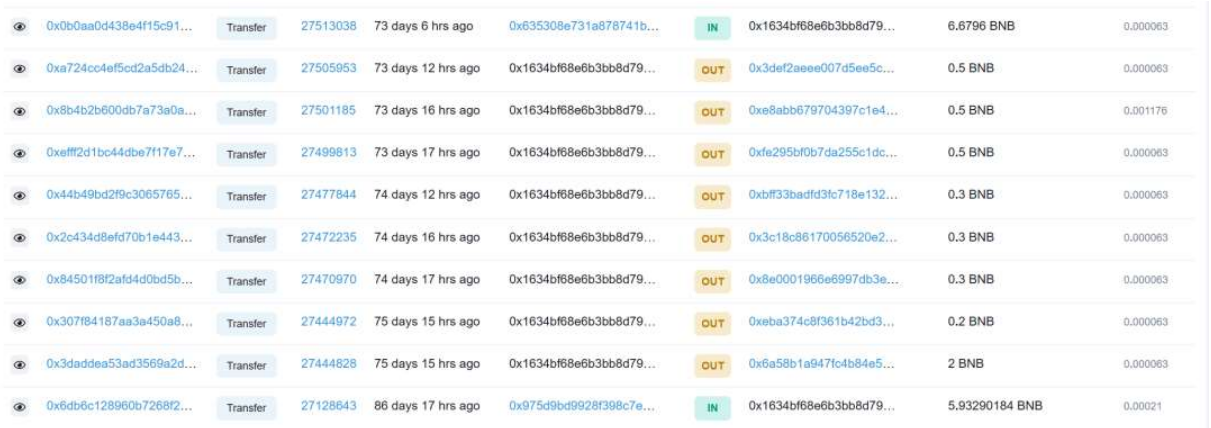


The fee for the consolidated address 0xe0afadad1d93704761c8550f21a53de3468ba599

2. Through Bybit, it flows into the address through a layer of transit.
The address to transfer fees: 0x4FbC021742A4664D1cf8e9d2730b8519B9Dcc523
transaction
hash0xb8b0626b86ed336c9c0fff56b20761438535aa06461dcca9cdc39dc10ec1c620

3. Use the stolen assets to swap for ETH as fees
There are two hacker addresses that swap the stolen USDT/USDC into ETH in DEX, and then use it as fees for subsequent addresses. The following are the initial fee transfer and hashes of the two addresses.
Hacker address 1: 0xdddE20a5F569DFB11F5c405751367E939ebC5886
Fee transfer address: 0xD475747a4937a66Cc7D4a2c7eA7F6e827D0f7390
Transaction hash:
0x853b75b1b8a7f56c51fcba9b996af8d132b784cfa0da7162c20a48a5994d8a06
Hacker address 2: 0x8E0001966e6997db3e45c5F75D4C89a610255b2E
Transaction hash:
0x0f3cf1fe16052223e091e87c2a6f7a9a94e53a565dfac7b83eb0b9b79458ad8f

On the BSC chain



The address(0x1634Bf68e6b3Bb8D79388EfB3d1A5215506FBbEd) to distribute fees

The address to distribute fees obtained fees and distributes them through Kucoin and ChangeNow exchanges.

1. Kucoin
Transaction hash:
0x0b0aa0d438e4f15c919e55148c87890ae0d089d036cadbdc6b87afa9e19f747b

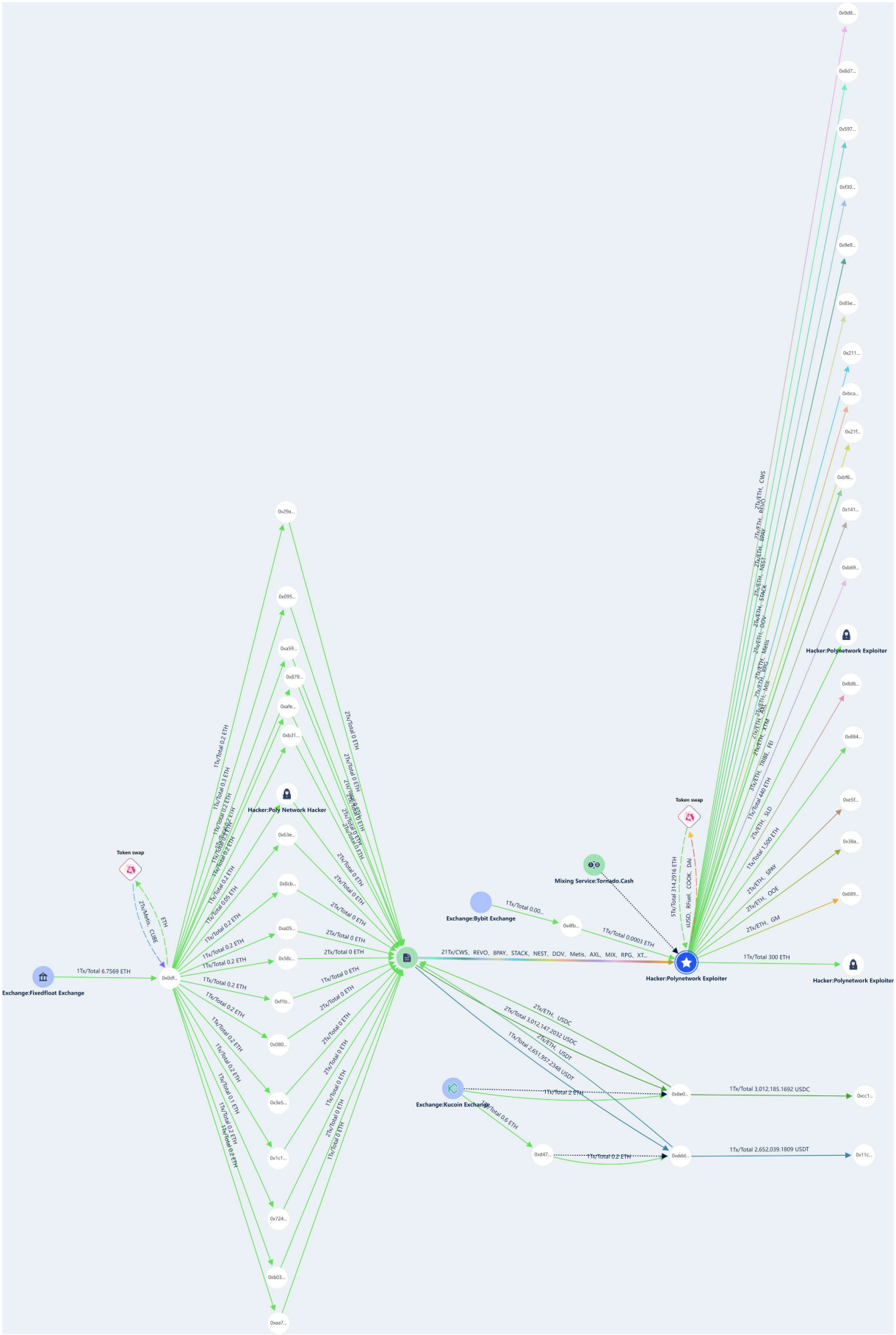
2、 ChangeNow
Transaction hash:
0x6db6c128960b7268f2bf8c199b2c0c017b3bee29bbefac0bf5d31c63b6373075
There is no fee for the consolidated addresses.
On the Polygon chain

The address(0x09F92eDce2E46C399BFE7881a7619598AF8436d5) to distribute fees
The address calling the attacked contract obtained fees through a common address.
This address gets the transaction fee through the FixedFloat exchange.
Transaction hash:
0xc7a25eb840718028c0d8f402d1293dcb479755d77609a7dfb616c10e90176dec
The source of the hacker's consolidated addresses' fees is
0x09F92eDce2E46C399BFE7881a7619598AF8436d5。

Beosin KYT/AML keeps tracing the flow of funds

On the Ethereum

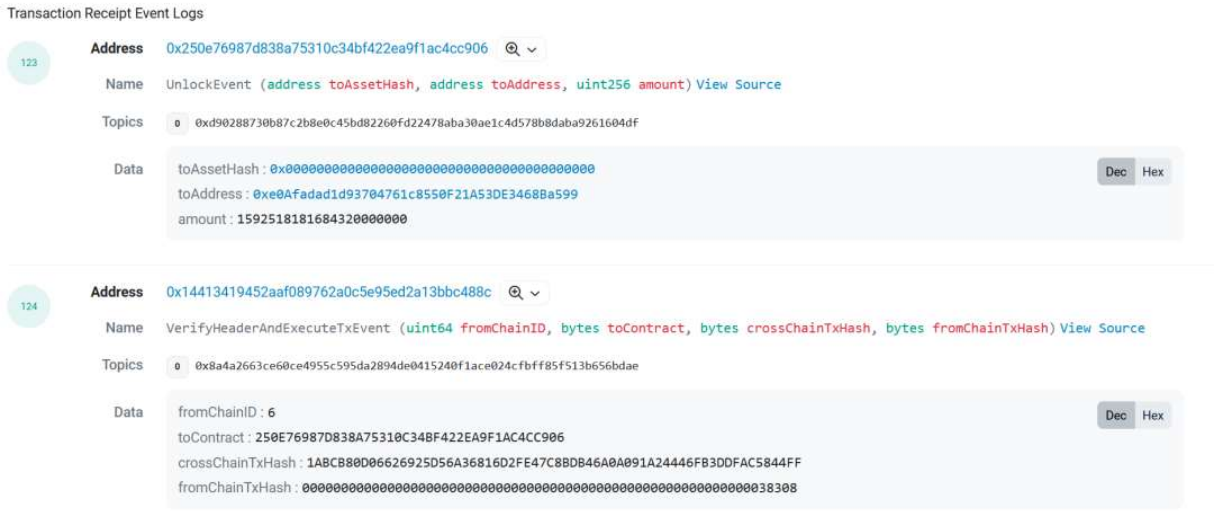
Beosin KYT/AML tracked and found that the stolen funds on the ETH chain are as follows:



First, the hacker called the attacked contract through a batch of addresses to exploit the vulnerability, using a total of 20 addresses.

The fees of these 20 addresses all came from the address 0x0dfeb429166e629204aca66467484cd88cb9701c, and the fees of this address were transferred in through Fixedfloat.

The hacker called LOCK in the Poly Network contract, locked the funds, and then called the two functions of UnlockEvent and verifyHeaderAndExecuteTx to attack the project. The case is as follows:



It can be seen that in the UnlockEvent, the variable toAddress has become the hacker consolidated address, and the amount has also been modified to the amount of stolen funds (1,592.51818168432 ETH here).

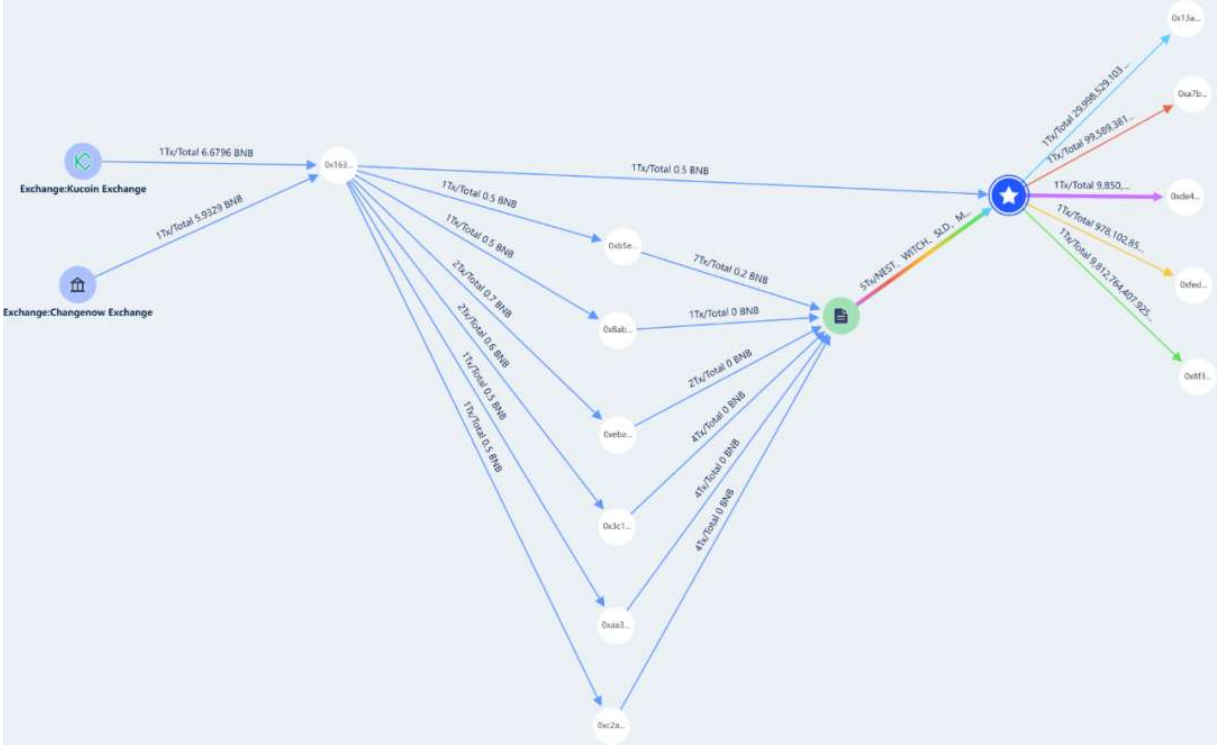
From here, we can see that the Proof item in the input data has been replaced with the content containing the hacker consolidated address.The fee of the hacker's address involved in the case is mainly obtained from five ways:

1. Transfer to ETH through Tronado.cash
2. Transfer to ETH through Bybit exchange
3. Transfer to ETH through KuCoin Exchange
4. Transfer to ETH through the FixedFloat exchange
5. Using stolen ETH

Hackers began to attack on July 1, 2023. Up to now, only some virtual currencies have been exchanged for ETH through Dex and ETH and some other virtual currencies have been transferred to other addresses.

On the BSC chain

The flow on the BSC chain is similar to that on the Ethereum. The hacker continued to use some of the same addresses for the stealing operation, and used the contract bugs to transfer the assets to the hacker's addresses.



First, the hacker called the attacked contract through a batch of addresses to exploit the vulnerability, using more than 30 addresses.

The fees of these addresses all came from the address 0x1634Bf68e6b3Bb8D79388EfB3d1A5215506FBbEd and the fee of this address was transferred through the Kucoin and ChangeNow platforms.

Then, by using the same vulnerability to attack the contract, the stolen funds were transferred to the hacker address, and then part of the funds were transferred to multiple consolidated addresses.

On the Polygon chain

The flow on the Polygon is similar to that on the Ethereum and BSC. Hackers continued to use some of the same addresses to carry out the stealing operations, and used contract bugs to transfer assets to the hacker's addresses.

First, the hacker called the attacked contract through a batch of addresses to exploit the vulnerability. The hacker only used one address 0x09F92eDce2E46C399BFE7881a7619598AF8436d5 and the fee was transferred through Fixedfloat.

Then, by using the same vulnerability to attack the contract, the stolen funds were transferred to the collection address, and then part of the funds were transferred to multiple consolidated addresses.

Currently, the Beosin security team is working with Poly Network to deal with this security incident and the latest progress will be shared with you as soon as possible.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, Korea, Japan, and other 10+ countries. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-one" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts and protected more than $500 billion funds of our clients.

Contact

If you need any blockchain security services, welcome to contact us:
Official Website Beosin EagleEye Twitter Telegram Login | InCareer