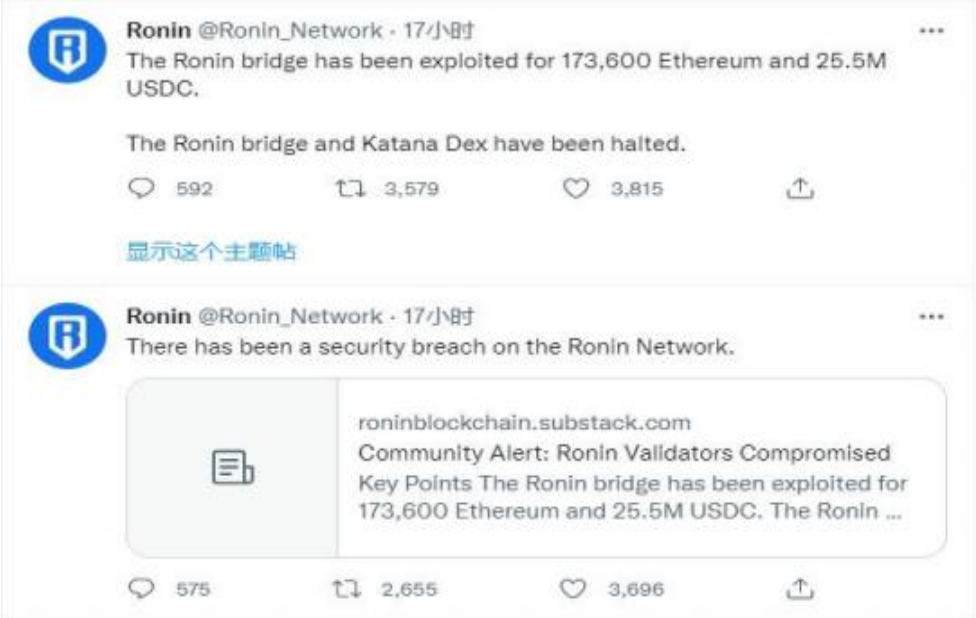
SharkTeam

# 620 million！hackers break the record again：Ronin Bridge attack incident analysis

2022-03-30

# 620 million！ hackers break the record again：Ronin Bridge attack incident analysis

On March 29, Ronin officially announced that the Ronin Bridge was hacked, and the hackers stole 173,600 ETH and 25.5M USDC, which amounted to about $625 million according to the price at the time.



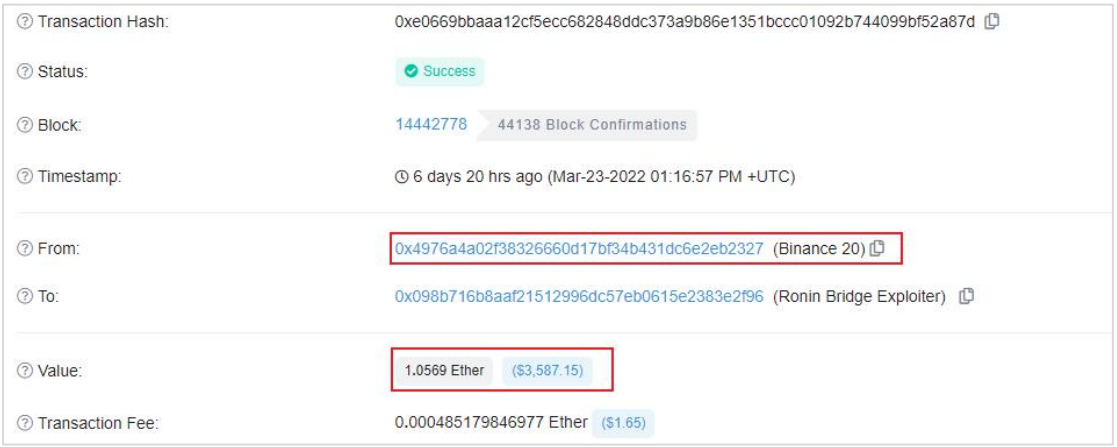

SharkTeam analyzed the attack technology for the first time, And summarized the security precautions. He hoped that the following blockchain projects would learn from this and build a security defense line for the blockchain industry.

## 1. Incident Analysis

Attacker address: 0x098b716b8aaf21512996dc57eb0615e2383e2f96

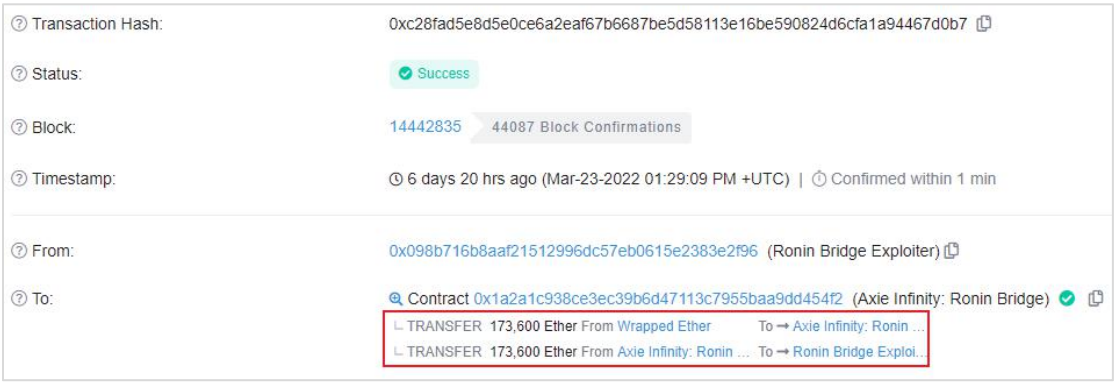
The transaction that launched the attack is as follows:


The funds for the attack came from Binance's wallet account, and the transaction was:
0xe0669bbaaa12cf5ecc682848ddc373a9b86e1351bccc01092b744099bf52a87d



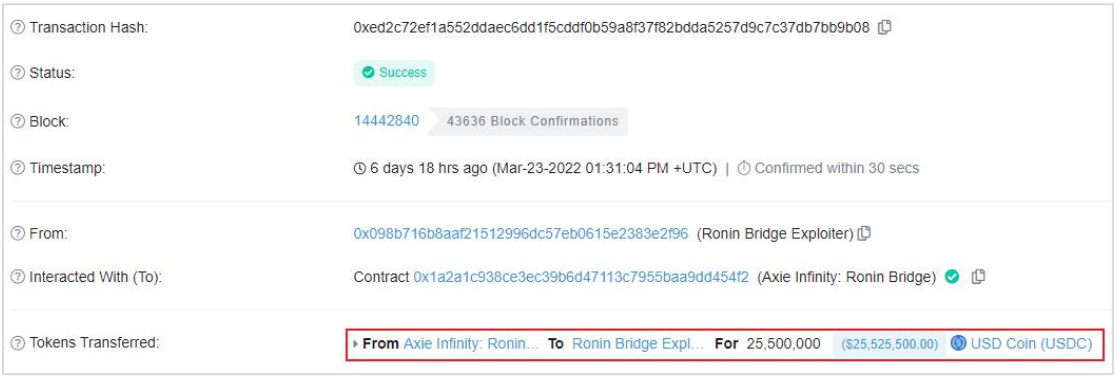

The attacker's account received a transfer from the Binance Wallet account Binance 20 with a transfer amount of 1.0569 Ether. The first attack transaction is as follows:

0xc28fad5e8d5e0ce6a2eaf67b6687be5d58113e16be590824d6cfa1a94467d0b7

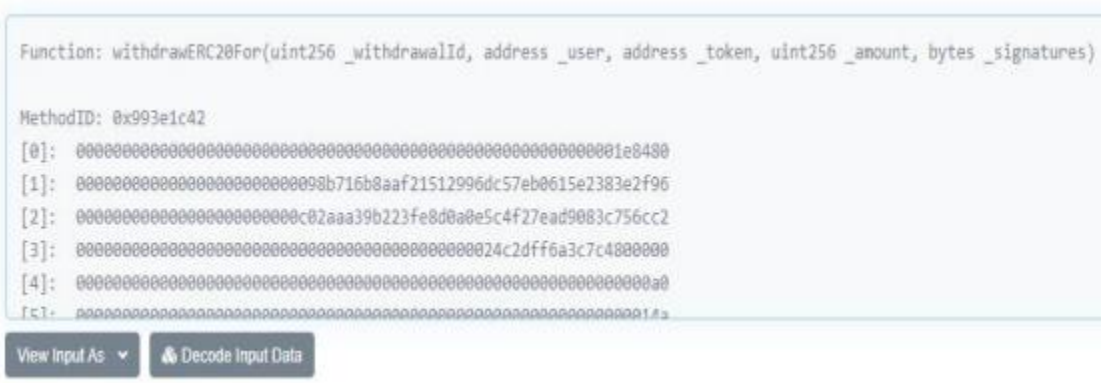



In this transaction, the attacker withdrew 172,600 Ether from the Ronin Bridge contract. The second attack transaction is as follows:

0xed2c72ef1a552ddaec6dd1f5cddf0b59a8f37f82bdda5257d9c7c37db7bb9b08



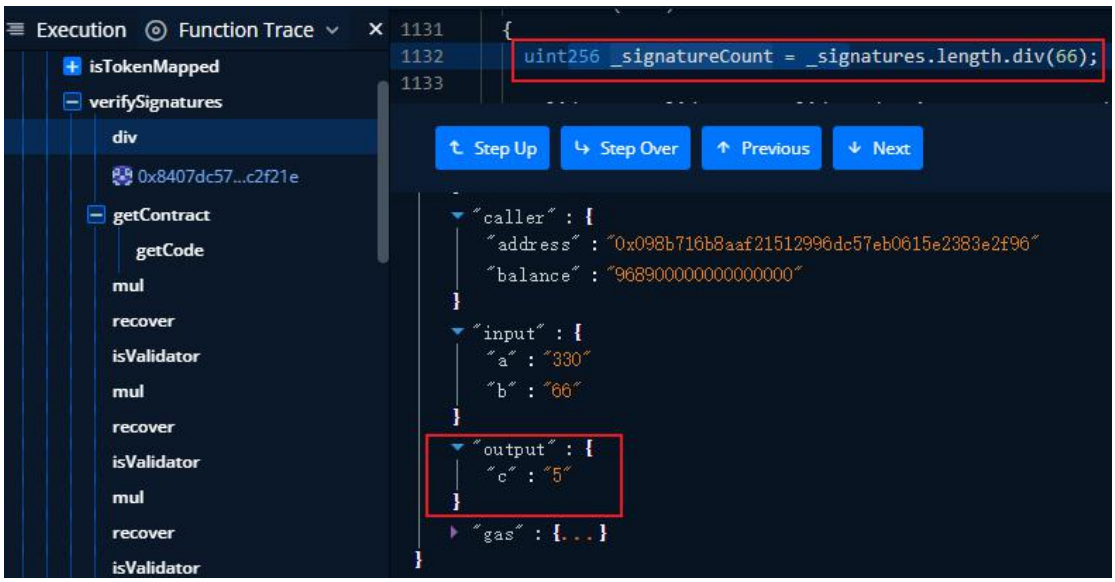

In this transaction, the attacker withdrew 25.5M USDC from the Ronin Bridge contract.Both of these attack transactions call the withdrawERC20For function in the Ronin Bridge contract:




We analyzed the withdrawERC20For function, which requires 5 signatures when withdrawing tokens:

```
1028  function withdrawERC20For(
1029    uint256 _withdrawalId,
1030    address _user,
1031    address _token,
1032    uint256 _amount,
1033    bytes memory _signatures
1034  )
1035    public
1036    whenNotPaused
1037    onlyMappedToken(_token, 20)
1038  {
1039    bytes32 _hash = keccak256(
1040      abi.encodePacked(
1041        "withdrawERC20",
1042        _withdrawalId,
1043        _user,
1044        _token,
1045        _amount
1046      )
1047    );
1048
1049    require(verifySignatures(_hash, _signatures));
1050
1051    if (_token == registry.getContract(registry.WETH_TOKEN())) {
1052      _withdrawETHFor(_user, _amount);
1053    } else {
1054      uint256 _gatewayBalance = IERC20(_token).balanceOf(address(this));
1055
1056      if (_gatewayBalance < _amount) {
1057        require(
1058          IERC20Mintable(_token).mint(address(this), _amount.sub(_gatewayBalance)),
1059          "MainchainGatewayManager: Minting ERC20 token to gateway failed"
1060        );
1061      }
1062
1063      require(IERC20(_token).transfer(_user, _amount), "Transfer failed");
1064    }
```

```
1128  function verifySignatures(
1129    bytes32 _hash,
1130    bytes memory _signatures
1131  )
1132    public
1133    view
1134    returns (bool)
1135  {
1136    uint256 _signatureCount = _signatures.length.div(66);
1137
1138    Validator _validator = Validator(registry.getContract(registry.VALIDATOR()));
1139    uint256 _validatorCount = 0;
1140    address _lastSigner = address(0);
1141
1142    for (uint256 i = 0; i < _signatureCount; i++) {
1143      address _signer = _hash.recover(_signatures, i.mul(66));
1144      if (_validator.isValidator(_signer)) {
1145        _validatorCount++;
1146      }
1147      // Prevent duplication of signatures
1148      require(_signer > _lastSigner);
1149      _lastSigner = _signer;
1150    }
1151
1152    return _validator.checkThreshold(_validatorCount);
1153  }
1154
```




The 5 signature accounts here are as follows:

0x11360eacdedd59bc433afad4fc8f0417d1fbebab

0x1a15a5e25811fe1349d636a5053a0e59d53961c9

0x70bb1fb41c8c42f6ddd53a708e2b82209495e455

0xb9e59d56fd1632fc250935182bdd5c59188b2302

0xf224beff587362a88d859e899d0d80c080e1e812

The attacker obviously successfully obtained the signatures of these five signer accounts, and the final transaction was successful.

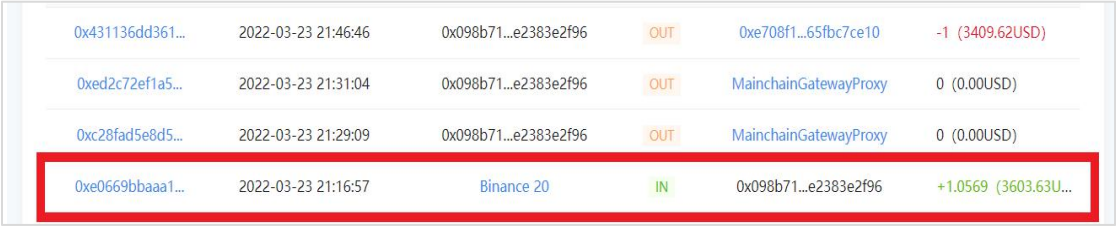
The attack occurred on March 23, 2022, and according to the official news

from Axie Infinity, the attack was discovered on March 29, after users reported that 5k Ether could not be withdrawn from Bridge.

## 2. Analysis of the cash flow

### 1. initial source of funding

The attackers obtained 1.0569 ETH of funds by withdrawing coins through the Binance exchange as the initial funds for this attack.



| | | | | | |
|---|---|---|---|---|---|
| 0x431136dd361... | 2022-03-23 21:46:46 | 0x098b71...e2383e2f96 | OUT | 0xe708f1...65fbc7ce10 | -1 (3409.62USD) |
| 0xed2c72ef1a5... | 2022-03-23 21:31:04 | 0x098b71...e2383e2f96 | OUT | MainchainGatewayProxy | 0 (0.00USD) |
| 0xc28fad5e8d5... | 2022-03-23 21:29:09 | 0x098b71...e2383e2f96 | OUT | MainchainGatewayProxy | 0 (0.00USD) |
| 0xe0669bbaaa1... | 2022-03-23 21:16:57 | Binance 20 | IN | 0x098b71...e2383e2f96 | +1.0569 (3603.63U... |

### 2. Funding link analysis

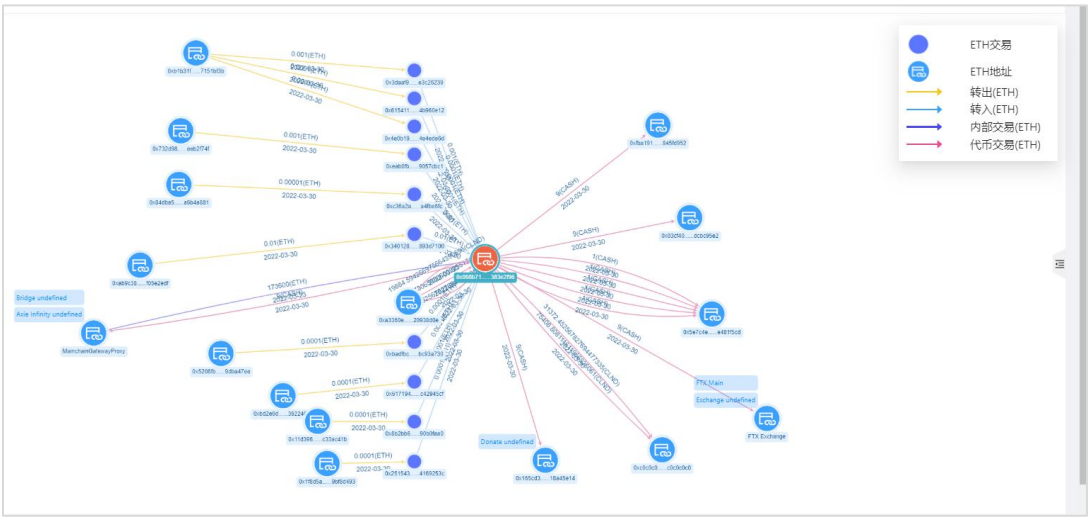
The attacker obtained 173,600 ETH and 25,500,000 USDC through the Ronin Bridge cross-chain bridge contract.

| | | | | | | |
|---|---|---|---|---|---|---|
| 0xc809c4632... | 2022-03-30 00:52:38 | 0xd45125...ddaad0c9c0 | IN | 0x098b71...e2383e2f96 | 788 | Sealenza |
| 0xe10472c87... | 2022-03-30 00:51:13 | 0xaf0c57...16a71ba59c | IN | 0x098b71...e2383e2f96 | 1 | Jupiter |
| 0x02ece0c70... | 2022-03-30 00:35:53 | 0xa9d25b...f23d41469f | IN | 0x098b71...e2383e2f96 | 5 | smith slappers |
| 0x04d7d0b9... | 2022-03-30 00:26:10 | 0x3238b5...944536ba19 | IN | 0x098b71...e2383e2f96 | 602 | Milady |
| 0x287dad48... | 2022-03-23 22:05:33 | 0x098b71...e2383e2f96 | OUT | 0x665660...d440155617 | 3500000 | USD Coin |
| 0xbb0c13809... | 2022-03-23 22:02:51 | 0x098b71...e2383e2f96 | OUT | 0xe708f1...65fbc7ce10 | 10000000 | USD Coin |
| 0x4e6d5f19c... | 2022-03-23 22:00:43 | 0x098b71...e2383e2f96 | OUT | 0x665660...d440155617 | 10000000 | USD Coin |
| 0x685e095d1... | 2022-03-23 21:56:44 | 0x098b71...e2383e2f96 | OUT | 0x665660...d440155617 | 1000000 | USD Coin |
| 0x55ae6a400... | 2022-03-23 21:54:53 | 0x098b71...e2383e2f96 | OUT | 0xe708f1...65fbc7ce10 | 1000000 | USD Coin |
| 0xed2c72ef1... | 2022-03-23 21:31:04 | MainchainGatewayProxy | IN | 0x098b71...e2383e2f96 | 25500000 | USD Coin |

共 50 条 < 1 2 3 > 跳至 页

The attacker transferred 25,500,000 USDC to 0xe708f address and 0x6656 address in five installments, and exchanged about 8564 ETH from this address.

The attacker then transferred 6,250 ETH to 5 addresses, and the other funds are still in the attacker's wallet address.




ChainAegis | ETH(Ethereu... | 搜索地址/交易/区块高度

| | | | | | |
|---|---|---|---|---|---|
| 0xbca767de1cd... | 2022-03-28 14:52:27 | 0x098b71...e2383e2f96 | OUT | 0x776b80...ff5867d0f3 | -750 (2559780.00U... |
| 0x47798dbe058... | 2022-03-28 10:36:18 | 0x098b71...e2383e2f96 | OUT | 0x9fae13...581751533f | -500 (1706520.00U... |
| 0x2a2942caeec... | 2022-03-28 10:33:07 | 0x098b71...e2383e2f96 | OUT | 0xdb3a63...807c39f5fa | -500 (1706520.00U... |
| 0xa442188adf1... | 2022-03-28 10:30:38 | 0x098b71...e2383e2f96 | OUT | 0x776b80...ff5867d0f3 | -500 (1706520.00U... |
| 0x67660f03925... | 2022-03-23 22:11:30 | 0xe708f1...65fbc7ce10 | IN | 0x098b71...e2383e2f96 | +3364.5375835279... |
| 0xb7bf311480c... | 2022-03-23 22:11:30 | 0x665660...d440155617 | IN | 0x098b71...e2383e2f96 | +1180.1426056027... |
| 0x287dad48bfe... | 2022-03-23 22:05:33 | 0x098b71...e2383e2f96 | OUT | FiatTokenProxy | 0 (0.00USD) |
| 0xbb0c1380942... | 2022-03-23 22:02:51 | 0x098b71...e2383e2f96 | OUT | FiatTokenProxy | 0 (0.00USD) |
| 0xeec0233a761... | 2022-03-23 22:02:51 | 0x665660...d440155617 | IN | 0x098b71...e2383e2f96 | +3390 (11570205.... |
| 0x4e6d5f19c52... | 2022-03-23 22:00:43 | 0x098b71...e2383e2f96 | OUT | FiatTokenProxy | 0 (0.00USD) |
| 0x5dfb733a952... | 2022-03-23 21:59:41 | 0xe708f1...65fbc7ce10 | IN | 0x098b71...e2383e2f96 | +330 (1126303.20... |
| 0xf1bdc548c01... | 2022-03-23 21:58:58 | 0x665660...d440155617 | IN | 0x098b71...e2383e2f96 | +300 (1023912.00... |
| 0x685e095d1f7... | 2022-03-23 21:56:44 | 0x098b71...e2383e2f96 | OUT | FiatTokenProxy | 0 (0.00USD) |
| 0x55ae6a400fb... | 2022-03-23 21:54:53 | 0x098b71...e2383e2f96 | OUT | FiatTokenProxy | 0 (0.00USD) |
| 0x655dd40d591... | 2022-03-23 21:49:41 | 0x098b71...e2383e2f96 | OUT | 0x665660...d440155617 | -1 (3413.04USD) |

### 3. Fund flow tracking

Hackers transferred some of the funds to Huobi and FTX, of which 3750 ETH was transferred to Huobi and 1250 ETH was transferred to FTX. Another 1 ETH was transferred to the Crypto.com address.

| | | | | | |
|---|---|---|---|---|---|
| 0xa50874ea03a... | 2022-03-30 08:13:40 | 0x3318f0...af934333c6 | IN | 0x036587...0dc25654f9 | 0 (0.00USD) |
| 0xdaa08bfd377... | 2022-03-29 15:41:54 | 0x036587...0dc25654f9 | OUT | FTX Exchange 2 | -123.981872521252... |
| 0xc6bdf5a1f26... | 2022-03-29 15:40:17 | 0x5d84a7...ee28f51555 | IN | 0x036587...0dc25654f9 | +123.98273110625... |
| 0x28f850bb661... | 2022-03-29 15:24:56 | 0x036587...0dc25654f9 | OUT | FTX Exchange 2 | -99.99916462 (341... |
| 0x8df13ffc5de... | 2022-03-29 15:24:18 | 0x5d84a7...ee28f51555 | IN | 0x036587...0dc25654f9 | +100 (341556.00U... |
| 0x00f1fd6a25b... | 2022-03-29 15:22:57 | 0x036587...0dc25654f9 | OUT | FTX Exchange 2 | -99.99916462 (341... |
| 0x2028f612276... | 2022-03-29 15:21:48 | 0x5d84a7...ee28f51555 | IN | 0x036587...0dc25654f9 | +100 (341556.00U... |
| 0x8c25a2f914e... | 2022-03-29 15:09:54 | 0x036587...0dc25654f9 | OUT | FTX Exchange 2 | -99.99916462 (341... |
| 0x569cad00723... | 2022-03-29 15:08:51 | 0x5d84a7...ee28f51555 | IN | 0x036587...0dc25654f9 | +100 (341556.00U... |
| 0x9a7f79825a1... | 2022-03-29 14:55:38 | 0x036587...0dc25654f9 | OUT | FTX Exchange 2 | -99.999141415 (34... |
| 0x5e337d5dbd2... | 2022-03-29 14:54:52 | 0x5d84a7...ee28f51555 | IN | 0x036587...0dc25654f9 | +100 (341556.00U... |

**Remaining funds:**

| Adress | amount of funds (ETH) |
|---|---|
| 0x5b5082214D62585D686850Ab8D9E3f6b6a5c58FF | 1234 |
| 0xa9BFdC186c6Bcf058Fbb5Bf62046D7bC74E96Ce2 | 15 |
| 0x098b716b8aaf21512996dc57eb0615e2383e2f96 (Attacker address) | 175914 |

ChainAegis on-chain risk monitoring platform has started real-time account movement monitoring for the above addresses.

## 3. Safety suggestion

SharkTeam reminds you that please be vigilant when setting foot in blockchain projects. Try to choose more stable, More secure, public chains, and projects that have been audited for several rounds, In initiating a transaction. Never put your assets at risk and become a hacker's ATM.

SharkTeam, a leading blockchain security service team, offers smart contract audit services for developers. To satisfy the demands of different clients, the smart contract audit services provide both manual auditing and automated

auditing. It implements almost 200 auditing contents that cover four aspects: high-level language layer, virtual machine layer, blockchain layer, and business logic layer, ensuring that smart contracts are completely guaranteed and Safety.

Website: https://www.sharkteam.org/

Telegram: https://t.me/sharkteamorg

Twitter：https://twitter.com/sharkteamorg

SharkTeam

In Math，We Trust！

https://sharkteam.org

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg