SharkTeam

Web3 Security Threat' Trend Report 2022 Q2

July 25th 2022

Table of contents

1. Overview of Web3 Security Situation.. 3

2. Incident type analysis...3

2.1 Contract Vulnerability Exploitation.. 4

2.2 Flash Loan Attack..5

2.3 Phishing Attack... 6

2.4 Rugpulls.. 6

3. Typical Case Analysis... 7

3.1 Transaction Replay + Management Vulnerability - Analysis of 20 Million OP Stolen Incident.. 7

3.2 Beanstalk Farms Attack Principle and Fund Flow Analysis - Flash Loan + Proposal Attack...11

3.3 Jay Chou's NFT was stolen by a phishing site on April Fool's Day19

4. Crypto Wars..22

5. Summary.. 29

1. Overview of Web3 Security Situation

The Web3 ecosystem lost more than **$2 billion** in the first half of 2022.The **$1.55 billion** overall loss for 2021 has been exceeded by losses in the first half of 2022.

The most common attacks in Q2 2022 are contract exploits, flash loans and phishing attacks.

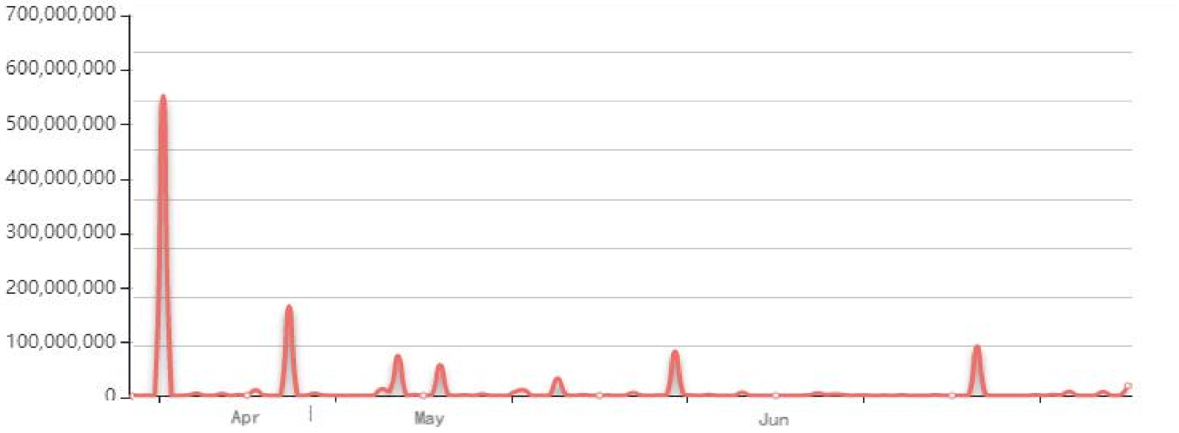
With the development of the Web3 ecosystem, governments have also promulgated a series of policies. The most influential of these are the executive order on the regulatory framework for cryptocurrencies signed by the Biden administration in the United States, and the European Union's MiCA Act.

In general, the 2022 Web3 ecosystem is challenged by the ongoing bear market and constant hacking.

2. Incident type analysis

The Web3 ecosystem revealed **49** security incidents in Q2 2022,

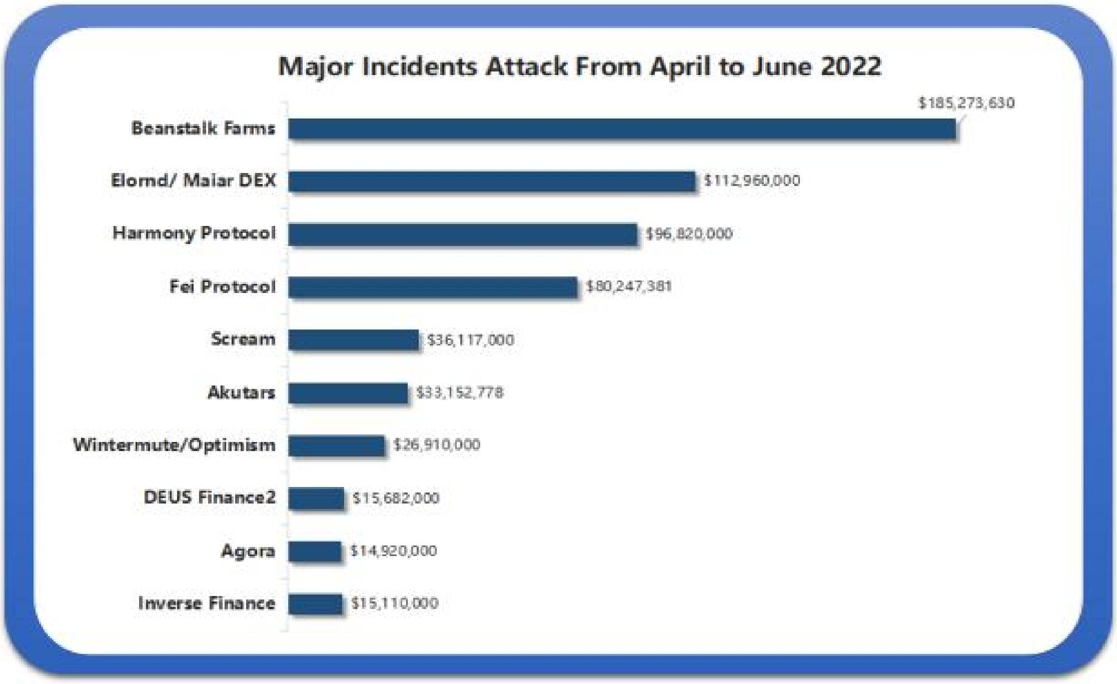
with a loss of about **$721,163,820** overall.



SharkTeam reported 49 major attacks in the Web 3 domain during the second quarter of 2022, with a total loss of about US$721.16 million. Among them, there were 3 attacks with losses of US$100 million or more, 12 attacks with losses of US$10 million or more, and 28 attacks with losses of US$1 million or more. The events with the highest losses were

Beanstalk Farmss Elrond and Harmony, at $182 million, $113 million and $100 million, respectively.

2.1 Contract Vulnerability Exploitation

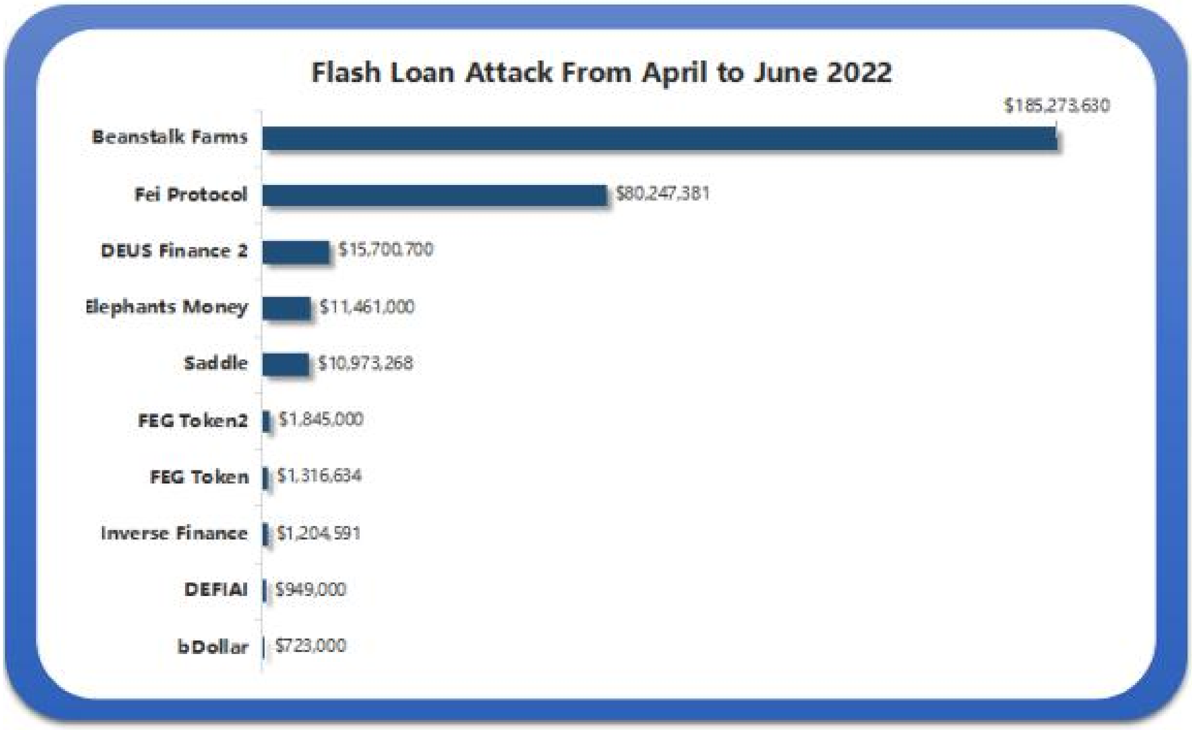


Contract vulnerability exploitation cover a range of hacker attack techniques. Basically, hackers attack using vulnerabilities in project code or infrastructure. For example, it may be that the multi-signature key has been leaked, or the minting function, reentrancy problem, or a defect in the oracle itself. While there has been a decreasing trend in attacks exploiting contract vulnerabilities this quarter, this type of attack tends to be more damaging.

40 attacks and more than $530 million in losses were caused through contract exploits in 2022 Q2. Compared with 2022 Q1, the loss amount decreased by about 56.7%. But surprisingly, the number of attacks did not drop, in fact increased from 32 to 40. The main reason for this discrepancy was the attack on the Ronin network, which caused a loss of $624 million. However, even without the Ronin attack, the average funds lost per attack dropped from 18.9 million to 13.4 million.

2.2 Flash Loan Attack

Flashloan is one of the main pain points for Web3 security, with 28 attacks involving flash loans during the quarter, totaling $310,002,694 in losses. Compared to Q1, both the number of attacks and attack losses have grown tremendously. The number of attacks increased from 15 in Q1 to **28** in Q2, an increase of 46.4%, and the amount of lost funds increased by more than 2000% from $13,978,452 in Q1 to **$310,002,694** in Q2.



The highest loss for the quarter was the $185 million security incident against Beanstalk Farms, followed by the $80.24 million flash loan attack against the Fei protocol. Compared to 2022 Q1, the biggest flash loan incident was the $3 million attack on Deus Finance. However, flash loan attacks in Q2 were still more damaging than in Q1. Using Q1 and Q2 as a benchmark, we can forecast a loss of nearly $678 million, an 81% increase from the previous year. Also, flash loan attacks are rarely "just" flash loan attacks, they often involve oracles, liquidity, and more contract exploits.

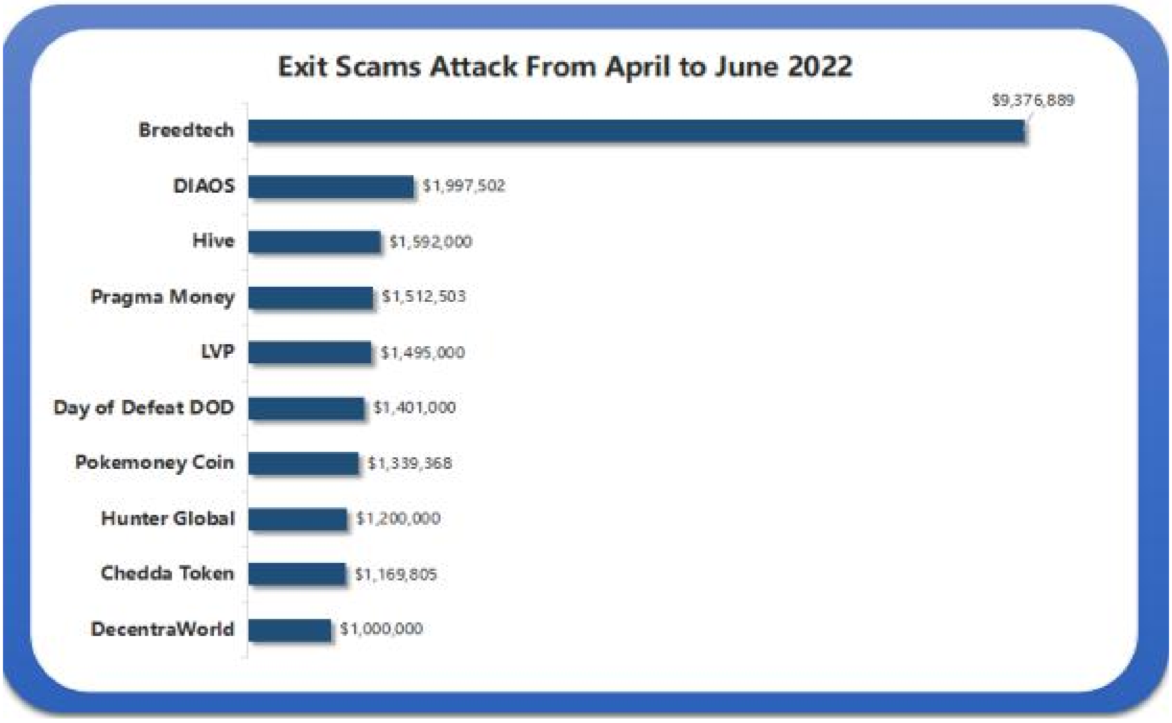
2.3 Phishing Attack

Phishing attacks are becoming more frequently in Q2 2022 as well. In Q1, there were just 106 attacks, and in the second, there were nearly 300 attacks.

Additionally, the great majority of phishing efforts have been carried out via Discord. On the one hand, this shows that it is the preferred cryptocurrency/NFT social scene. But on the other hand, related reports also pointed out its long-standing security problems.

Although the number of phishing attacks increased in Q2, losses caused by phishing attacks decreased by 14.7% from the previous quarter to $37.72 million. The main reason for this comes down to the current cryptocurrency bear market, This makes it harder for inexperienced investors to be fooled by all kinds of fraudulent information.

2.4 Rugpulls



Rugpulls are still serious, with 91 occurrences during the quarter resulting in losses of $39,421,648. While this was an 18% increase from the first quarter, this category of attacks declined in Q2 compared to 2021. This is probably the effect of a prolonged bear market.

Investors are more cautious about how they use the assets in their hands, After several major events in Q2, like the demise of Terra, Three Arrows Capital, and Celsius's insolvency problems.

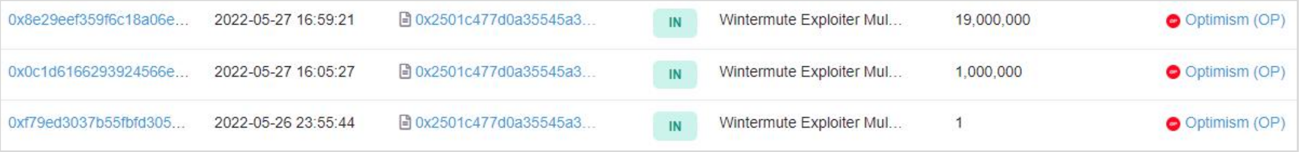
The above types of security incidents are more common in Q2, whether we will usher in a better and more secure encryption market, and whether the decline in some risk indicators will continue, it remains to be seen, the security of the Web3 ecosystem will depend on investment The degree of security awareness of the operator, whether the project team has a better security mechanism, and whether the market resumes a more complete supervision mechanism.

3. Typical Case Analysis

3.1 Transaction Replay + Management Vulnerability - Analysis of 20 Million OP Stolen Incident

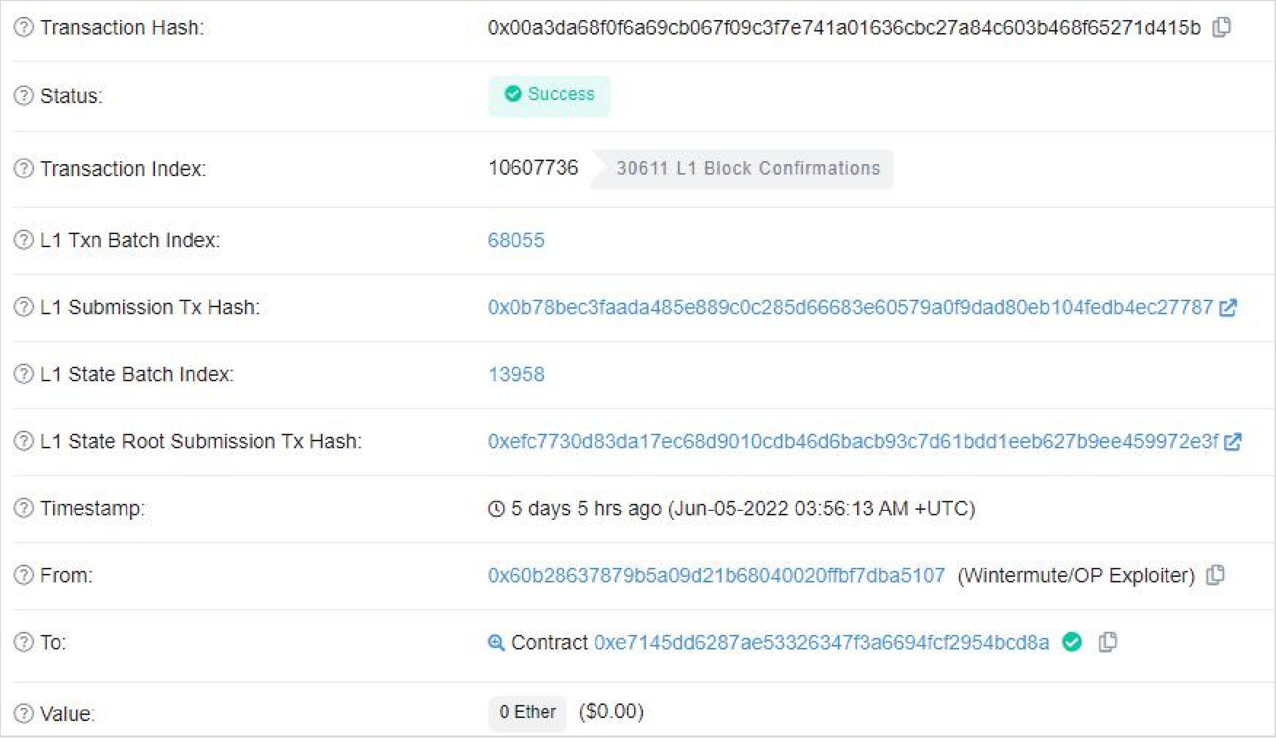
Hackers stole 20 million Optimism tokens on June 9, 2022, according to Optimism and cryptocurrency market maker Wintermute. Wintermute was awarded 20 million OP tokens from the Optimism Foundation on June 9th.

he Optimism Foundation transferred 20 million OP tokens to Wintermute's multi-signature contract address in two phases on May 27th, and transferred 1 OP token on May 26th through a multi-signature contract. The following are the three transactions:



0x8e29eef359f6c18a06e...	2022-05-27 16:59:21	0x2501c477d0a35545a3...	IN	Wintermute Exploiter Mul...	19,000,000	Optimism (OP)
0x0c1d6166293924566e...	2022-05-27 16:05:27	0x2501c477d0a35545a3...	IN	Wintermute Exploiter Mul...	1,000,000	Optimism (OP)
0xf79ed3037b55fbfd305...	2022-05-26 23:55:44	0x2501c477d0a35545a3...	IN	Wintermute Exploiter Mul...	1	Optimism (OP)

According to the transaction time and the number of OP tokens in the transaction, we analyzed that on the 26th, the Optimism Foundation transferred 1 OP token to the Wintermute multi-signature contract address as a test. OP tokens are sent to the Wintermute multi-signature contract address in two consecutive transactions. The receiving address is the multi-signature contract address that Wintermute has deployed on Ethereum/L1, so Wintermute only verifies whether the token has been received, but does not verify the ownership of the address on Optimism/L2, which is not on Optimism/L2 at this time. There is no actual deployment of multi-signature contracts, which gives hackers an opportunity. First, let's take a look at the 0x4f3a contract deployment transaction on Optimism/L2: txHash is 0x00a3da68f0f6a69cb067f09c3f7e741a01636cbc27a84c603b468f65271d415b



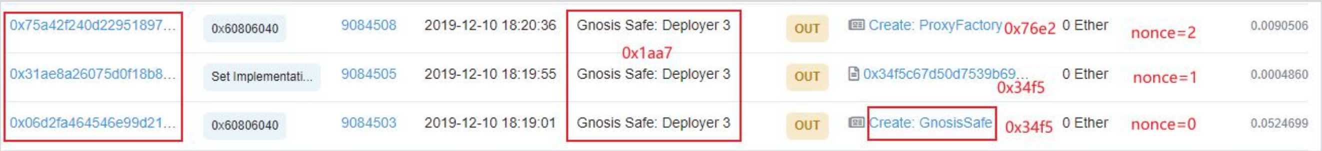
Transaction Hash:	0x00a3da68f0f6a69cb067f09c3f7e741a01636cbc27a84c603b468f65271d415b
Status:	Success
Transaction Index:	10607736 30611 L1 Block Confirmations
L1 Txn Batch Index:	68055
L1 Submission Tx Hash:	0x0b78bec3faada485e889c0c285d66683e60579a0f9dad80eb104fedb4ec27787
L1 State Batch Index:	13958
L1 State Root Submission Tx Hash:	0xefc7730d83da17ec68d9010cdb46d6bacb93c7d61bdd1eeb627b9ee459972e3f
Timestamp:	5 days 5 hrs ago (Jun-05-2022 03:56:13 AM +UTC)
From:	0x60b28637879b5a09d21b68040020ffbf7dba5107 (Wintermute/OP Exploiter)
To:	Contract 0xe7145dd6287ae53326347f3a6694fcf2954bcd8a
Value:	0 Ether ($0.00)

Note that the deployment time of the contract is June 5, and Wintermute/OP Exploiter is an address of the hacker, abbreviated as 0x60b2.

How does this transaction accurately generate the 0x4f3a contract address?

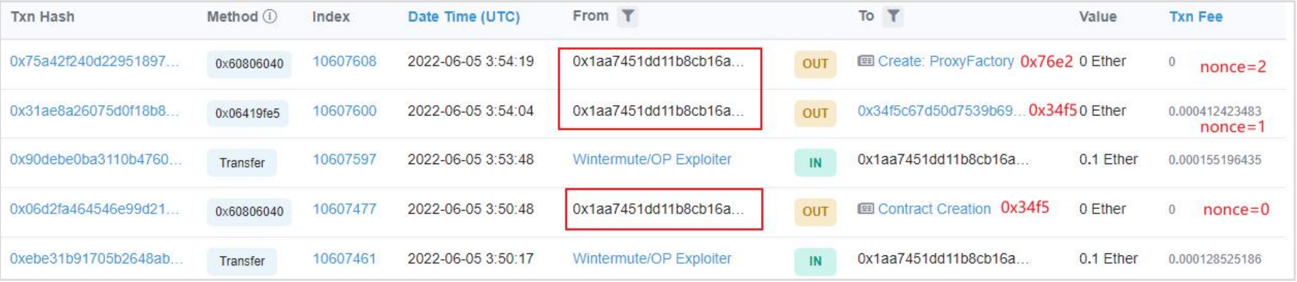
The hacker replayed 3 transactions, especially the one created by the last Gnosis Safe: Proxy Factory 1.1.1 contract, as follows:

(1) Transactions on Ethereum/L1 are as follows:



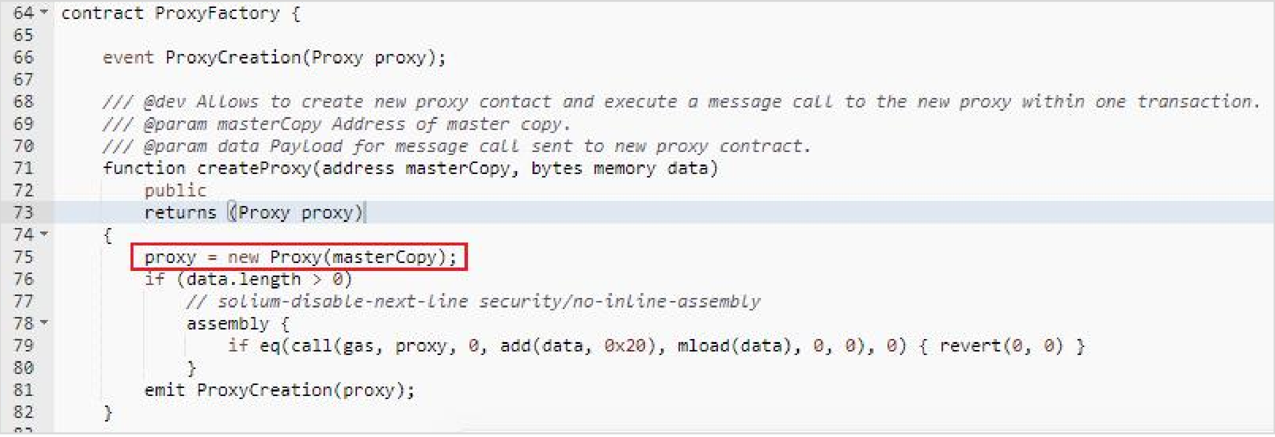
0x75a42f240d22951897...	0x60806040	9084508	2019-12-10 18:20:36	Gnosis Safe: Deployer 3 0x1aa7	OUT	Create: ProxyFactory	0x76e2 0 Ether	nonce=2	0.0090506
0x31ae8a26075d0f18b8...	Set Implementati...	9084505	2019-12-10 18:19:55	Gnosis Safe: Deployer 3	OUT	0x34f5c67d50d7539b69...	0x34f5 0 Ether	nonce=1	0.0004860
0x06d2fa464546e99d21...	0x60806040	9084503	2019-12-10 18:19:01	Gnosis Safe: Deployer 3	OUT	Create: GnosisSafe	0x34f5 0 Ether	nonce=0	0.0524699

(2) Transactions on Optimism/L2:



Txn Hash	Method	Index	Date Time (UTC)	From		To	Value	Txn Fee
0x75a42f240d22951897...	0x60806040	10607608	2022-06-05 3:54:19	0x1aa7451dd11b8cb16a...	OUT	Create: ProxyFactory 0x76e2	0 Ether	0 nonce=2
0x31ae8a26075d0f18b8...	0x06419fe5	10607600	2022-06-05 3:54:04	0x1aa7451dd11b8cb16a...	OUT	0x34f5c67d50d7539b69... 0x34f5	0 Ether	0.000412423483 nonce=1
0x90debe0ba3110b4760...	Transfer	10607597	2022-06-05 3:53:48	Wintermute/OP Exploiter	IN	0x1aa7451dd11b8cb16a...	0.1 Ether	0.000155196435
0x06d2fa464546e99d21...	0x60806040	10607477	2022-06-05 3:50:48	0x1aa7451dd11b8cb16a...	OUT	Contract Creation 0x34f5	0 Ether	0 nonce=0
0xebe31b91705b2648ab...	Transfer	10607461	2022-06-05 3:50:17	Wintermute/OP Exploiter	IN	0x1aa7451dd11b8cb16a...	0.1 Ether	0.000128525186

By replaying the transaction, the hacker created the same Gnosis Safe: Proxy Factory 1.1.1 contract on Optimism/L2 as on Ethereum/L1 (the address is the same as the contract code), and the function of creating the proxy contract is as follows:

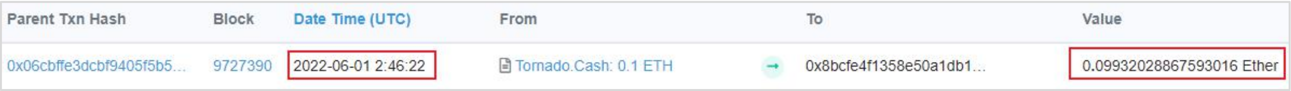


```
contract ProxyFactory {

    event ProxyCreation(Proxy proxy);

    /// @dev Allows to create new proxy contact and execute a message call to the new proxy within one transaction.
    /// @param masterCopy Address of master copy.
    /// @param data Payload for message call sent to new proxy contract.
    function createProxy(address masterCopy, bytes memory data)
        public
        returns (Proxy proxy)
    {
        proxy = new Proxy(masterCopy);
        if (data.length > 0)
            // solium-disable-next-line security/no-inline-assembly
            assembly {
                if eq(call(gas, proxy, 0, add(data, 0x20), mload(data), 0, 0), 0) { revert(0, 0) }
            }
        emit ProxyCreation(proxy);
    }
```

Gnosis Safe: The Proxy Factory 1.1.1 contract uses the 0.5 version of Solidity, and the create command is used instead of create2 when using new to create a contract. Use the create command to create a contract. The contract address is calculated by msg.sender and nonce. On Ethereum/L1, the msg.sender that created the multi-signature contract 0x4f3a is the address of Gnosis Safe: Proxy Factory 1.1.1. Hackers replay the transaction in Optimism/L2 to create the main contract of Gnosis Safe: Proxy Factory 1.1.1. The purpose is to ensure that the msg.sender of the contract 0x4f3a created on Optimism/L2 is consistent with that on Ethereum/L1, then the hacker can easily call the createProxy function through the smart contract (contract 0xe714) to create a contract with the address 0x4f3a. Additionally, the deployment of contract 0xe714 was completed on June 1 in the following transaction:

txHash: 0x69ee67800307ef7cb30ffa42d9f052290e81b3df6d3b7c29303007e33cd1c240

The address where the transaction was initiated is 0x8bcfe4f1358e50a1db10025d731c8b3b17f04dbb (abbreviated as 0x8bcf), which is also the address held by the hacker. At the same time, this transaction is also the first transaction initiated by 0x8bcf, and the funds come from Tornado:



Parent Txn Hash	Block	Date Time (UTC)	From		To	Value
0x06cbffe3dcbf9405f5b5...	9727390	2022-06-01 2:46:22	Tornado.Cash: 0.1 ETH	→	0x8bcfe4f1358e50a1db1...	0.09932028867593016 Ether

In terms of time, the whole process

(1) On May 27th, the Optimism address 0x2501 transferred 20 million OP to the 0x4f3a address on Optimism/L2. The 0x4f3a address was the multi-signature contract address of Wintermute on Ethereum/L1, but it was not deployed on Optimism/L2 at this time. contract;

(2) On June 1, the hacker address 0x8bcf deployed the contract 0xe714.

(3) On June 5th, the hacker created the Gnosis Safe: Proxy Factory 1.1.1 contract by replaying the transaction on Ethereum/L1 with the same address as on Ethereum/L1; then the address 0x60b2 deployed the multi-signature contract through the contract 0xe714 0x4f3a, the ownership of the contract belongs to the hacker, so the 20 million OP transferred in on May 27 was stolen by the hacker.

(4) On June 5, after receiving 20 million OP, the multi-signature contract 0x4f3a transferred 1 million OP to the hacker address 0x60b2, and then exchanged 1 million OP for 720.7 Ether.

(5) On June 9, the contract 0x4f3a transferred 1 million OPs to the account address 0xd8da, and the other 18 million OPs were still in the contract 0x4f3a.

Security Suggestion : The main reason of this security incident is a combination of factors such as transaction replay, vulnerabilities in the old version of Solidity, and transaction signature verification on the main chain and side chain, not because of loopholes in the contract code of the project party.

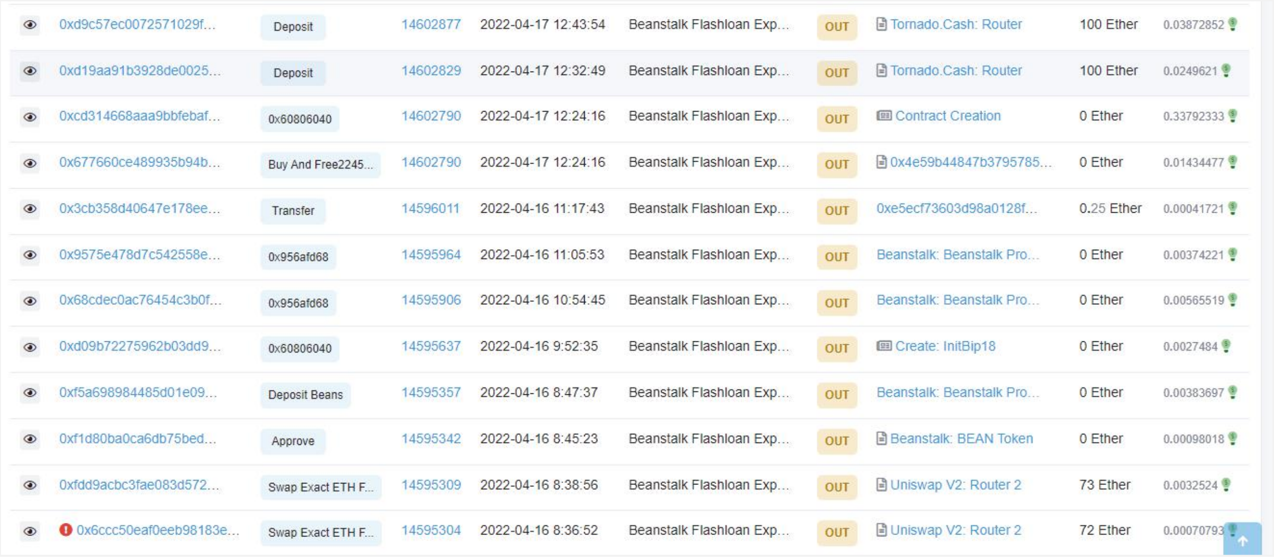
In addition, in response to this incident, the project party did not respond in a timely manner, and the contract management was not strict, etc., which also gave hackers an opportunity; from the perspective of the attack timeline and attack preparation, it is not ruled out that there is a possibility that there is collusion within the OP to commit crimes.

3.2 Beanstalk Farms Attack Principle and Fund Flow Analysis - Flash Loan + Proposal Attack

The algorithmic stablecoin project Beanstalk Farms was hacked on April 17, 2022, and more than $80 million was stolen, including 24,830 ETH and 36 million BEAN.

- Attacker address: 0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4
- Attack contract address: 0x728ad672409da288ca5b9aa85d1a55b803ba97d7
- Attacked contract address: 0xC1E088fC1323b20BCBee9bd1B9fC9546db5624C5
- Key attack transaction: 0xcd314668aaa9bbfebaf1a0bd2b6553d01dd58899c508d4729fa7311dc5d33ad7

The following transactions are included in the attack process:



0xd9c57ec0072571029f...	Deposit	14602877	2022-04-17 12:43:54	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.03872852
0xd19aa91b3928de0025...	Deposit	14602829	2022-04-17 12:32:49	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.0249621
0xcd314668aaa9bbfebaf...	0x60806040	14602790	2022-04-17 12:24:16	Beanstalk Flashloan Exp...	OUT	Contract Creation	0 Ether	0.33792333
0x677660ce489935b94b...	Buy And Free2245...	14602790	2022-04-17 12:24:16	Beanstalk Flashloan Exp...	OUT	0x4e59b44847b3795785...	0 Ether	0.01434477
0x3cb358d40647e178ee...	Transfer	14596011	2022-04-16 11:17:43	Beanstalk Flashloan Exp...	OUT	0xe5ecf73603d98a0128f...	0.25 Ether	0.00041721
0x9575e478d7c542558e...	0x956afd68	14595964	2022-04-16 11:05:53	Beanstalk Flashloan Exp...	OUT	Beanstalk: Beanstalk Pro...	0 Ether	0.00374221
0x68cdec0ac76454c3b0f...	0x956afd68	14595906	2022-04-16 10:54:45	Beanstalk Flashloan Exp...	OUT	Beanstalk: Beanstalk Pro...	0 Ether	0.00565519
0xd09b72275962b03dd9...	0x60806040	14595637	2022-04-16 9:52:35	Beanstalk Flashloan Exp...	OUT	Create: InitBip18	0 Ether	0.0027484
0xf5a698984485d01e09...	Deposit Beans	14595357	2022-04-16 8:47:37	Beanstalk Flashloan Exp...	OUT	Beanstalk: Beanstalk Pro...	0 Ether	0.00383697
0xf1d80ba0ca6db75bed...	Approve	14595342	2022-04-16 8:45:23	Beanstalk Flashloan Exp...	OUT	Beanstalk: BEAN Token	0 Ether	0.00098018
0xfdd9acbc3fae083d572...	Swap Exact ETH F...	14595309	2022-04-16 8:38:56	Beanstalk Flashloan Exp...	OUT	Uniswap V2: Router 2	73 Ether	0.0032524
❗ 0x6ccc50eaf0eeb98183e...	Swap Exact ETH F...	14595304	2022-04-16 8:36:52	Beanstalk Flashloan Exp...	OUT	Uniswap V2: Router 2	72 Ether	0.00070793

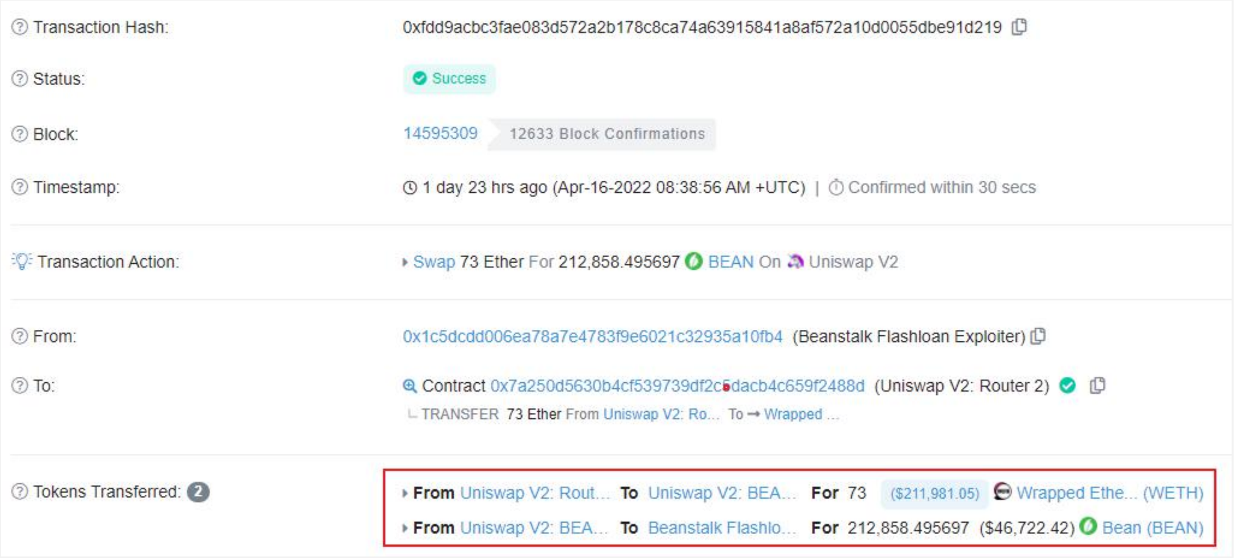
The following is the analysis of the attack process:

1. Token exchange.

The attackers exchanged 73 ETH for 212k BEAN via UniswapV2.

Transaction:

0xfdd9acbc3fae083d572a2b178c8ca74a63915841a8af572a10d0055dbe91d219

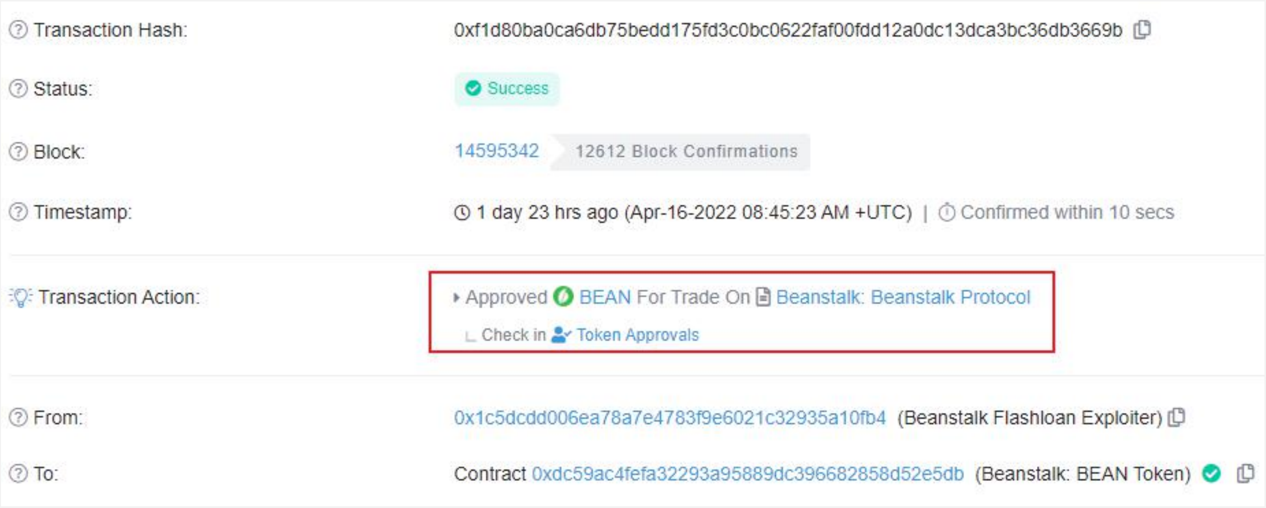


Transaction Hash:	0xfdd9acbc3fae083d572a2b178c8ca74a63915841a8af572a10d0055dbe91d219
Status:	Success
Block:	14595309 12633 Block Confirmations
Timestamp:	1 day 23 hrs ago (Apr-16-2022 08:38:56 AM +UTC) | Confirmed within 30 secs
Transaction Action:	Swap 73 Ether For 212,858.495697 BEAN On Uniswap V2
From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
To:	Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (Uniswap V2: Router 2) TRANSFER 73 Ether From Uniswap V2: Ro... To → Wrapped ...
Tokens Transferred: 2	From Uniswap V2: Rout... To Uniswap V2: BEA... For 73 ($211,981.05) Wrapped Ethe... (WETH) From Uniswap V2: BEA... To Beanstalk Flashlo... For 212,858.495697 ($46,722.42) Bean (BEAN)

2. Authorization

BEAN is delegated to the Beanstalk Protocol contract by the attacker.

Transaction:0xf1d80ba0ca6db75bedd175fd3c0bc0622faf00fdd12a0dc13dca3bc36db3669b



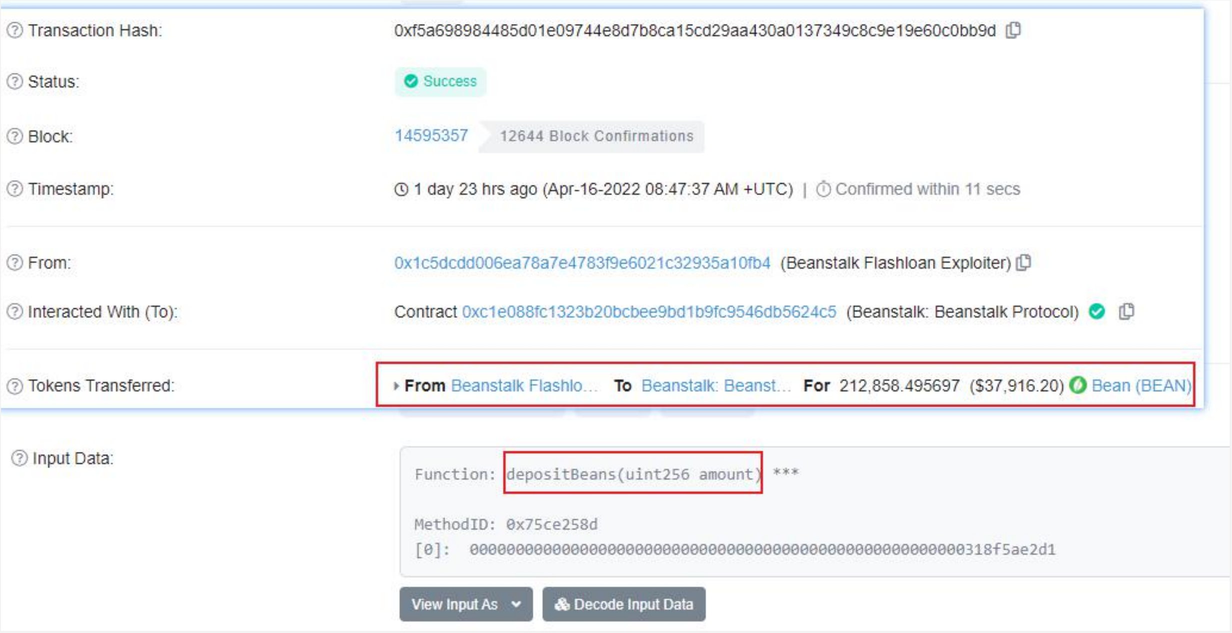
Transaction Hash:	0xf1d80ba0ca6db75bedd175fd3c0bc0622faf00fdd12a0dc13dca3bc36db3669b
Status:	Success
Block:	14595342 12612 Block Confirmations
Timestamp:	1 day 23 hrs ago (Apr-16-2022 08:45:23 AM +UTC) | Confirmed within 10 secs
Transaction Action:	Approved BEAN For Trade On Beanstalk: Beanstalk Protocol Check in Token Approvals
From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
To:	Contract 0xdc59ac4fefa32293a95889dc396682858d52e5db (Beanstalk: BEAN Token)

3. Deposit

To prepare for the attack, the attacker deposits the BEAN into the Beanstalk Protocol contract.

Transaction:

0xf5a698984485d01e09744e8d7b8ca15cd29aa430a0137349c8c9e19e60c0bb9d



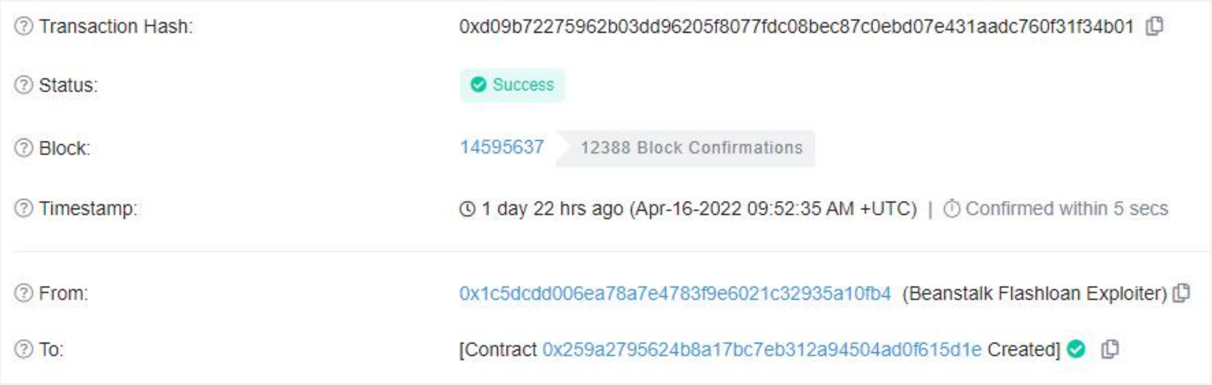
Transaction Hash:	0xf5a698984485d01e09744e8d7b8ca15cd29aa430a0137349c8c9e19e60c0bb9d
Status:	Success
Block:	14595357 12644 Block Confirmations
Timestamp:	1 day 23 hrs ago (Apr-16-2022 08:47:37 AM +UTC) | Confirmed within 11 secs
From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
Interacted With (To):	Contract 0xc1e088fc1323b20bcbee9bd1b9fc9546db5624c5 (Beanstalk: Beanstalk Protocol)
Tokens Transferred:	From Beanstalk Flashlo... To Beanstalk: Beanst... For 212,858.495697 ($37,916.20) Bean (BEAN)
Input Data:	

```
Function: depositBeans(uint256 amount) ***

MethodID: 0x75ce258d
[0]:  000000000000000000000000000000000000000000000000000000318f5ae2d1
```

4. Create InitBip18 proposal contract

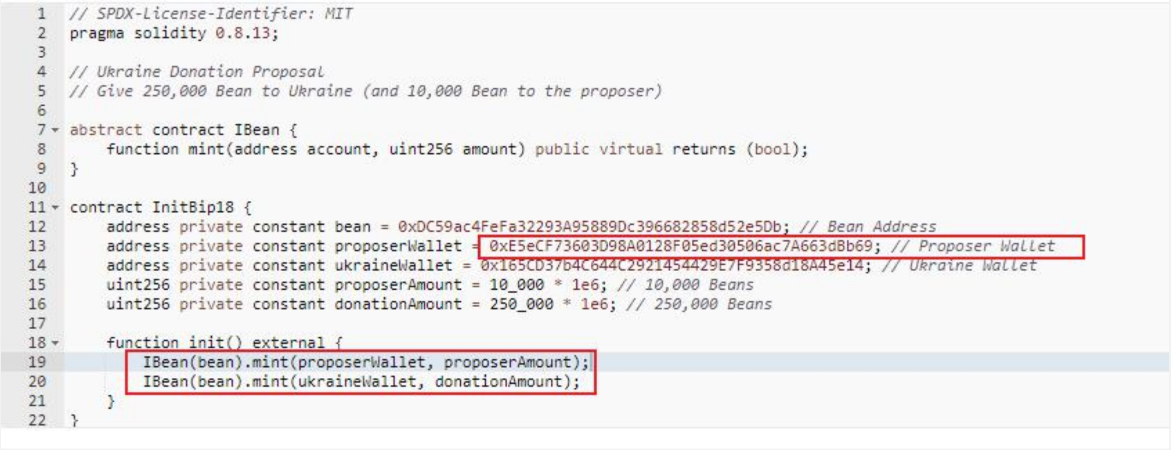
Transaction:

0xd09b72275962b03dd96205f8077fdc08bec87c0ebd07e431aadc760f31f34b01



Transaction Hash:	0xd09b72275962b03dd96205f8077fdc08bec87c0ebd07e431aadc760f31f34b01
Status:	Success
Block:	14595637 12388 Block Confirmations
Timestamp:	1 day 22 hrs ago (Apr-16-2022 09:52:35 AM +UTC) | Confirmed within 5 secs
From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
To:	[Contract 0x259a2795624b8a17bc7eb312a94504ad0f615d1e Created]

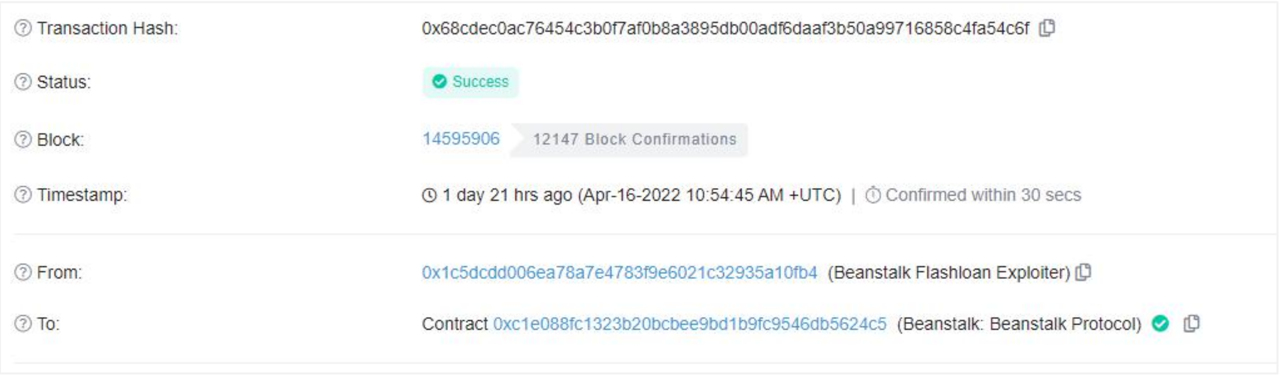
InitBip18 proposal contract address: 0x259a2795624b8a17bc7eb312a94504ad0f615d1e



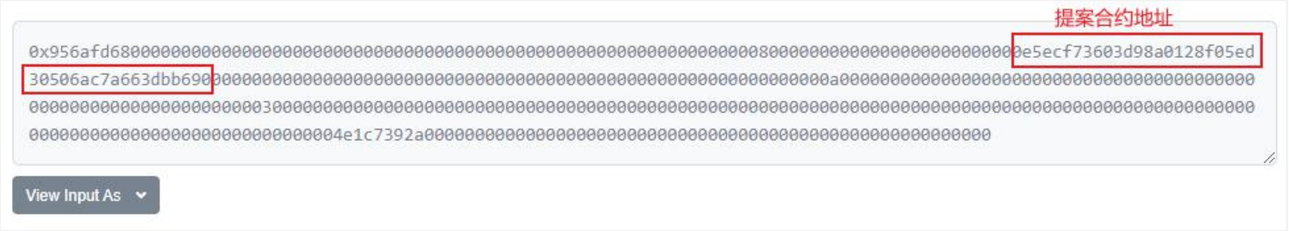
```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.13;

// Ukraine Donation Proposal
// Give 250,000 Bean to Ukraine (and 10,000 Bean to the proposer)

abstract contract IBean {
    function mint(address account, uint256 amount) public virtual returns (bool);
}

contract InitBip18 {
    address private constant bean = 0xDC59ac4FeFa32293A95889Dc396682858d52e5Db; // Bean Address
    address private constant proposerWallet = 0xE5eCF73603D98A0128F05ed30506ac7A663dBb69; // Proposer Wallet
    address private constant ukraineWallet = 0x165CD37b4C644C2921454429E7F9358d18A45e14; // Ukraine Wallet
    uint256 private constant proposerAmount = 10_000 * 1e6; // 10,000 Beans
    uint256 private constant donationAmount = 250_000 * 1e6; // 250,000 Beans

    function init() external {
        IBean(bean).mint(proposerWallet, proposerAmount);
        IBean(bean).mint(ukraineWallet, donationAmount);
    }
}
```

5. Initiate Proposal Transaction

Transaction: 0x68cdec0ac76454c3b0f7af0b8a3895db00adf6daaf3b50a99716858c4fa54c6f



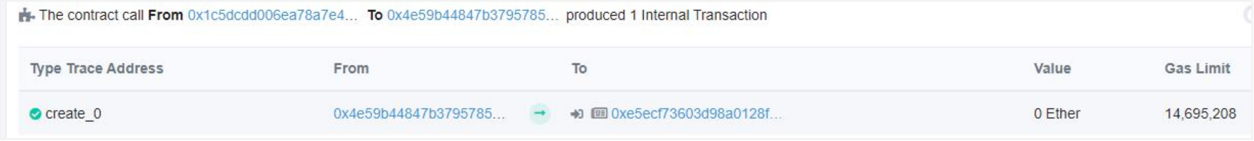
ⓘ Transaction Hash:	0x68cdec0ac76454c3b0f7af0b8a3895db00adf6daaf3b50a99716858c4fa54c6f
ⓘ Status:	✓ Success
ⓘ Block:	14595906 12147 Block Confirmations
ⓘ Timestamp:	1 day 21 hrs ago (Apr-16-2022 10:54:45 AM +UTC) | Confirmed within 30 secs
ⓘ From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
ⓘ To:	Contract 0xc1e088fc1323b20bcbee9bd1b9fc9546db5624c5 (Beanstalk: Beanstalk Protocol) ✓



提案合约地址

```
0x956afd680000000000000000000000000000000000000000000000000000000000000080000000000000000000000000e5ecf73603d98a0128f05ed
30506ac7a663dbb6900000000000000000000000000000000000000000000000000000000000000a00000000000000000000000000000000000000000
0000000000000000000000030000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000004e1c7392a00000000000000000000000000000000000000000000000000000000
```

The proposal contract address here is 0xe5ecf73603d98a0128f05ed30506ac7a663dbb69 (contract 0xe5ec for short), which is the Proposer Wallet in the InitBip18 proposal contract. The contract was created in transaction 0x677660ce489935b94bf5ac32c494669a71ee76913ffabe623e82a7de8226b460.

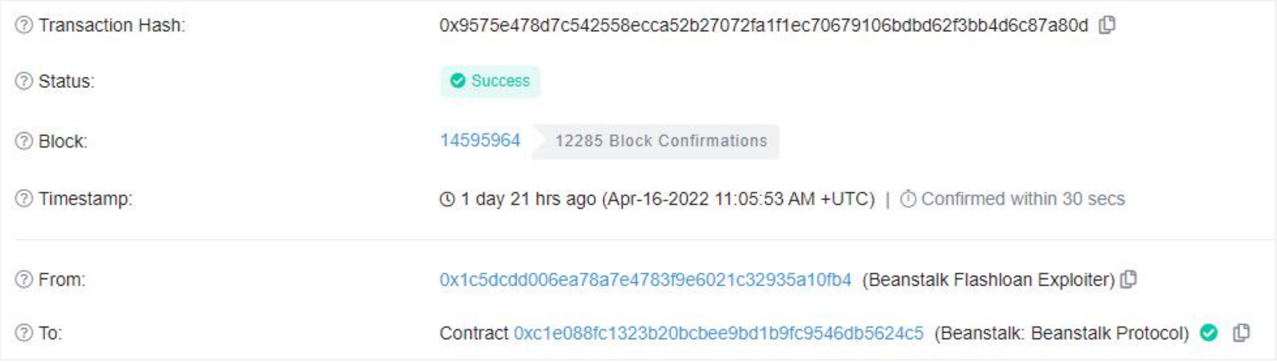


The contract call **From** 0x1c5dcdd006ea78a7e4... **To** 0x4e59b44847b3795785... produced 1 Internal Transaction

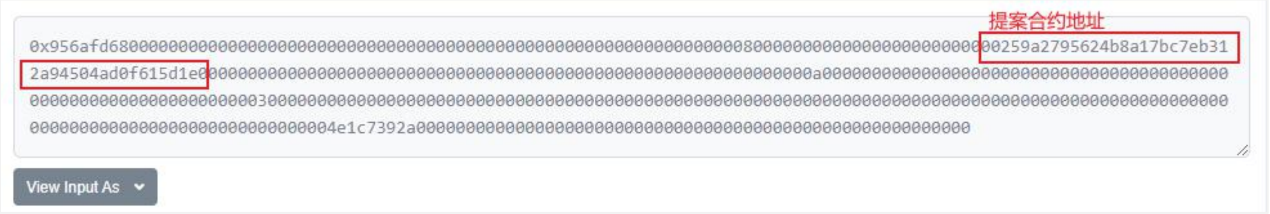
Type Trace Address	From	To	Value	Gas Limit
✓ create_0	0x4e59b44847b3795785... →	0xe5ecf73603d98a0128f...	0 Ether	14,695,208

Transaction:

0x9575e478d7c542558ecca52b27072fa1f1ec70679106bdbd62f3bb4d6c87a80d



ⓘ Transaction Hash:	0x9575e478d7c542558ecca52b27072fa1f1ec70679106bdbd62f3bb4d6c87a80d
ⓘ Status:	✓ Success
ⓘ Block:	14595964 12285 Block Confirmations
ⓘ Timestamp:	1 day 21 hrs ago (Apr-16-2022 11:05:53 AM +UTC) | Confirmed within 30 secs
ⓘ From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
ⓘ To:	Contract 0xc1e088fc1323b20bcbee9bd1b9fc9546db5624c5 (Beanstalk: Beanstalk Protocol) ✓



提案合约地址

```
0x956afd6800000000000000000000000000000000000000000000000000000000000000800000000000000000000000000259a2795624b8a17bc7eb31
2a94504ad0f615d1e00000000000000000000000000000000000000000000000000000000000000a00000000000000000000000000000000000000000
0000000000000000000000030000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000004e1c7392a00000000000000000000000000000000000000000000000000000000
```

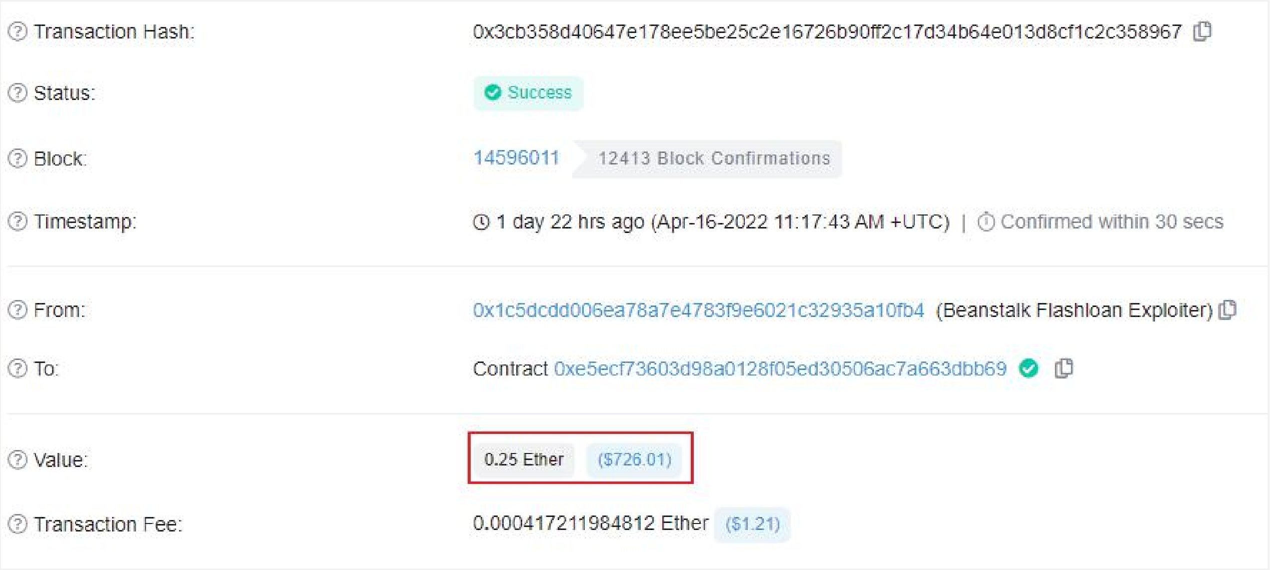
The proposal contract address here is the InitBip18 proposal contract in the previous step.

6. Transfer

The attacker transfers 0.25 ETH to the contract 0xe5ec.

Transaction:

0x3cb358d40647e178ee5be25c2e16726b90ff2c17d34b64e013d8cf1c2c358967



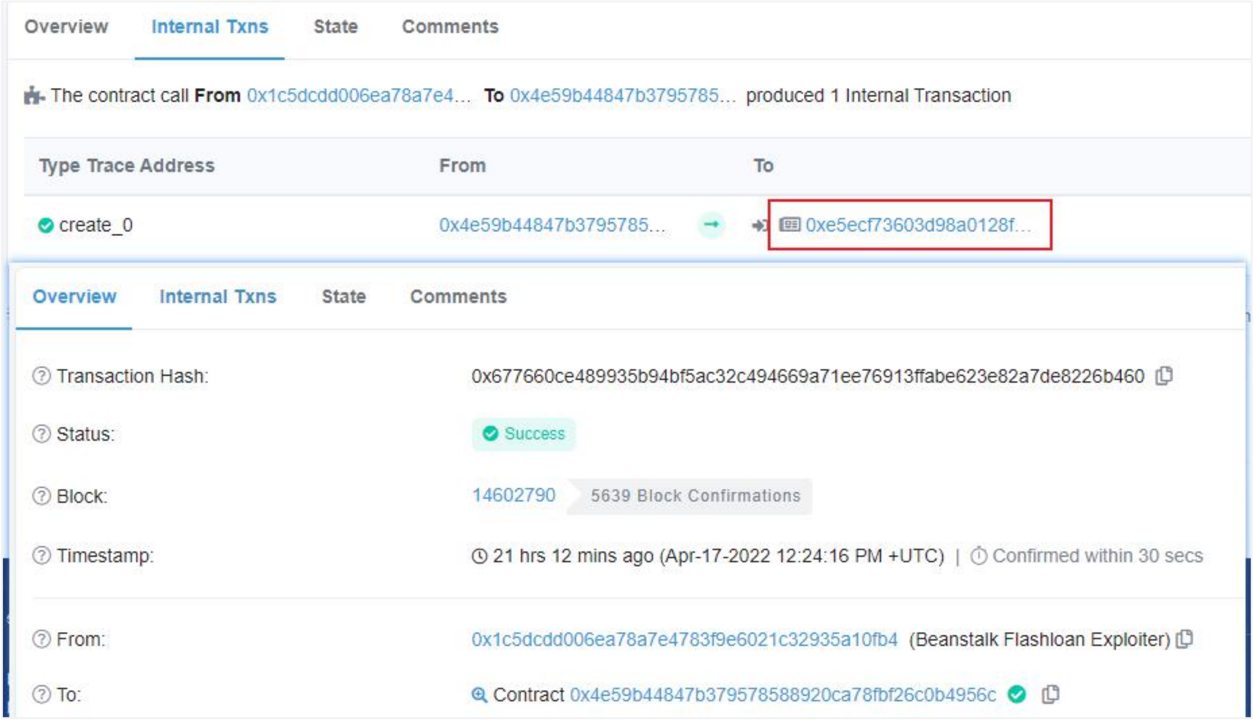
Transaction Hash:	0x3cb358d40647e178ee5be25c2e16726b90ff2c17d34b64e013d8cf1c2c358967
Status:	Success
Block:	14596011 12413 Block Confirmations
Timestamp:	1 day 22 hrs ago (Apr-16-2022 11:17:43 AM +UTC) | Confirmed within 30 secs
From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
To:	Contract 0xe5ecf73603d98a0128f05ed30506ac7a663dbb69
Value:	0.25 Ether ($726.01)
Transaction Fee:	0.000417211984812 Ether ($1.21)

7. Create the proposal contract 0xe5ec

Transaction:

0x677660ce489935b94bf5ac32c494669a71ee76913ffabe623e82a7de8226b460

The proposal contract 0xe5ec is created within the transaction.



The contract call **From** 0x1c5dcdd006ea78a7e4... **To** 0x4e59b44847b3795785... produced 1 Internal Transaction

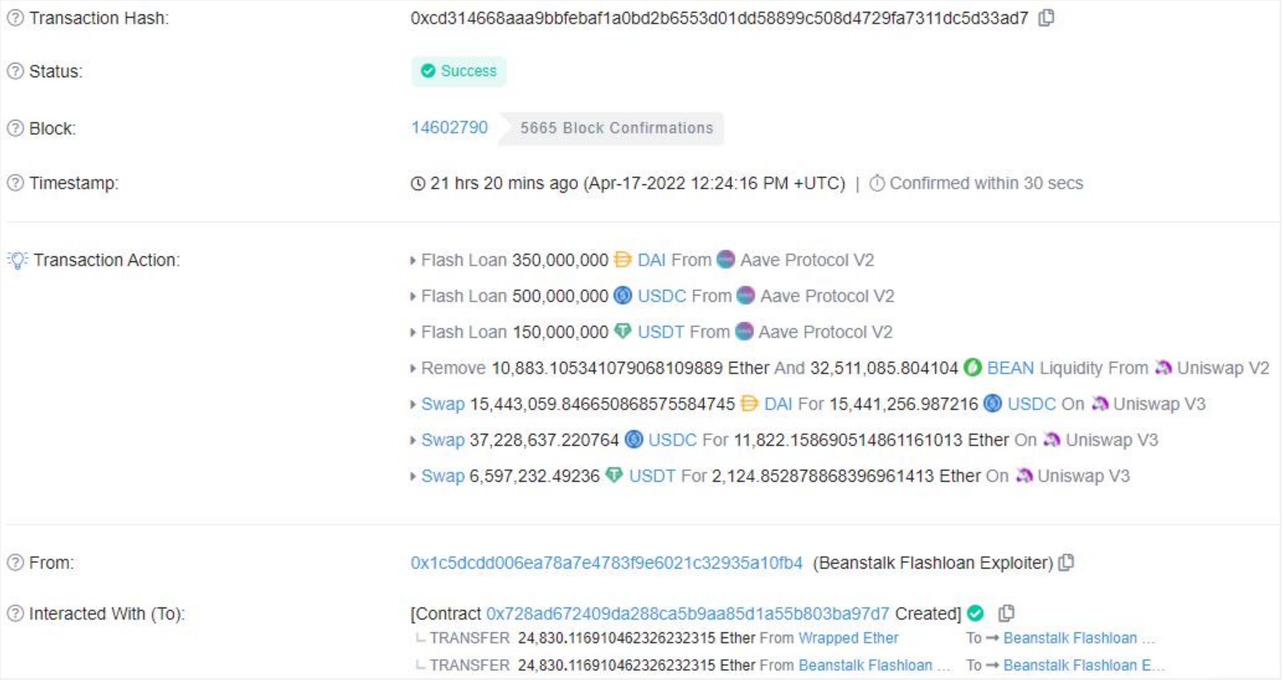
Type Trace Address	From	To
create_0	0x4e59b44847b3795785...	0xe5ecf73603d98a0128f...

Transaction Hash:	0x677660ce489935b94bf5ac32c494669a71ee76913ffabe623e82a7de8226b460
Status:	Success
Block:	14602790 5639 Block Confirmations
Timestamp:	21 hrs 12 mins ago (Apr-17-2022 12:24:16 PM +UTC) | Confirmed within 30 secs
From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
To:	Contract 0x4e59b44847b379578588920ca78fbf26c0b4956c

8. Attack

Transaction:

0xcd314668aaa9bbfebaf1a0bd2b6553d01dd58899c508d4729fa7311dc5d33ad7



Transaction Hash:	0xcd314668aaa9bbfebaf1a0bd2b6553d01dd58899c508d4729fa7311dc5d33ad7
Status:	✓ Success
Block:	14602790 5665 Block Confirmations
Timestamp:	21 hrs 20 mins ago (Apr-17-2022 12:24:16 PM +UTC) | Confirmed within 30 secs
Transaction Action:	▸ Flash Loan 350,000,000 DAI From Aave Protocol V2 ▸ Flash Loan 500,000,000 USDC From Aave Protocol V2 ▸ Flash Loan 150,000,000 USDT From Aave Protocol V2 ▸ Remove 10,883.105341079068109889 Ether And 32,511,085.804104 BEAN Liquidity From Uniswap V2 ▸ Swap 15,443,059.846650868575584745 DAI For 15,441,256.987216 USDC On Uniswap V3 ▸ Swap 37,228,637.220764 USDC For 11,822.158690514861161013 Ether On Uniswap V3 ▸ Swap 6,597,232.49236 USDT For 2,124.852878868396961413 Ether On Uniswap V3
From:	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4 (Beanstalk Flashloan Exploiter)
Interacted With (To):	[Contract 0x728ad672409da288ca5b9aa85d1a55b803ba97d7 Created] ✓ └ TRANSFER 24,830.116910462326232315 Ether From Wrapped Ether To → Beanstalk Flashloan ... └ TRANSFER 24,830.116910462326232315 Ether From Beanstalk Flashloan ... To → Beanstalk Flashloan E...

The attack details are as follows:

(1) Borrow 350M DAI, 500M USDC and 150M USDT from Aave platform through flash loan, 32.1M BEAN from Uniswap platform, and 11.6M LUSD from SushiSwap platform.

(2) Invest all the borrowed DAI, USDC and USDT into the Curve DAI/USDC/USDT liquidity pool, and mint 979,691,328 liquidity tokens 3Crv.

(3) Convert 15M 3Crv to 15,251,318 LUSD, add 964,691,328 3Crv to obtain 795,425,740 BEAN3CRV-f, add 32,100,950 BEAN and 26,894,383 LUSD to obtain 58,924,887 BEAN3CRV-f

(4) Vote for the proposal to pass and execute using all of the BEAN3CRV-f proposals obtained previously. Then got 36,084,584 BEAN, 0.5407 UNI-V2, 874,663,982 NEAN3CRV-f and 60,562,844 BEANLUSD-f

(5) Remove liquidity to get 1,007,734,729 3Crv and 28,149,504 LUSD

(6) Repay 11,678,100 LUSD and 32,197,543 BEAN of SushiSwap Flash Loan, including commission fees.

(7) Convert the remaining 16,471,404 LUSD into 16,184,690 3Crv.

(8) Remove the liquidity 3Crv and get 522,487,380 USDC, 365,758,059 DAI and

156,732,232 USDT.

(9) Repay the flash loan and commission fees by depositing 350,315,000 DAI, 500,450,000 USDC, and 150,135,000 USDT to the Aave platform.

(10) Remove the liquidity of 0.5407 UNI-V2, get 10,883 WETH and 32,511,085 BEAN and return the flash loan amount and commission fees.

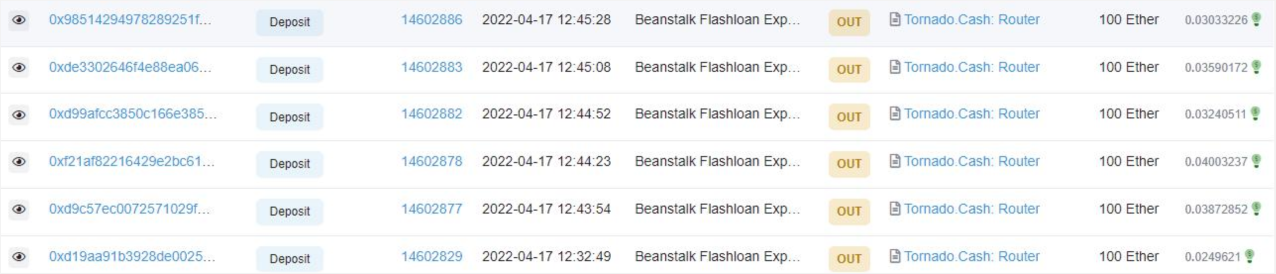
(11) Donated 250k USDC to Ukraine Crypto Donation

(12) Convert the remaining Tokens to WETH

(13) Complete the attack by withdrawing the 24,830 WETH obtained and converting it to the attacker's address.

9. Coin Mixing

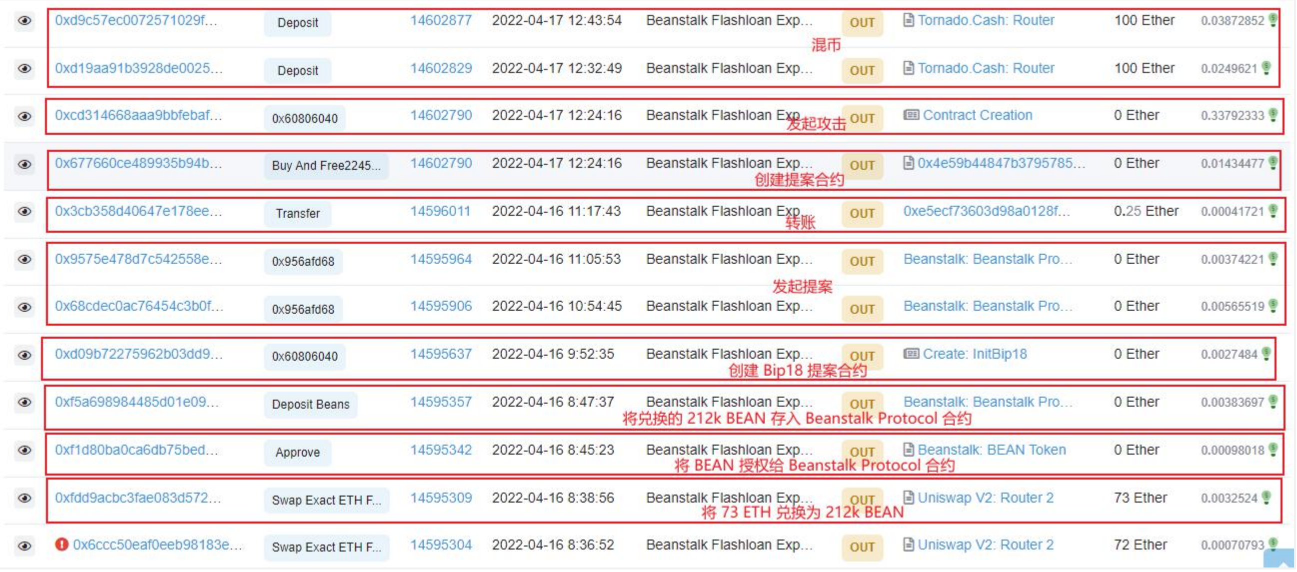
In order to implement coin mixing, the attacker deposits the obtained ETH into the coin mixing platform Tornash.Cash in batches.



0x98514294978289251f...	Deposit	14602886	2022-04-17 12:45:28	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.03033226
0xde3302646f4e88ea06...	Deposit	14602883	2022-04-17 12:45:08	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.03590172
0xd99afcc3850c166e385...	Deposit	14602882	2022-04-17 12:44:52	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.03240511
0xf21af82216429e2bc61...	Deposit	14602878	2022-04-17 12:44:23	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.04003237
0xd9c57ec0072571029f...	Deposit	14602877	2022-04-17 12:43:54	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.03872852
0xd19aa91b3928de0025...	Deposit	14602829	2022-04-17 12:32:49	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.0249621

10 Summary

The following is a review of the attack process:

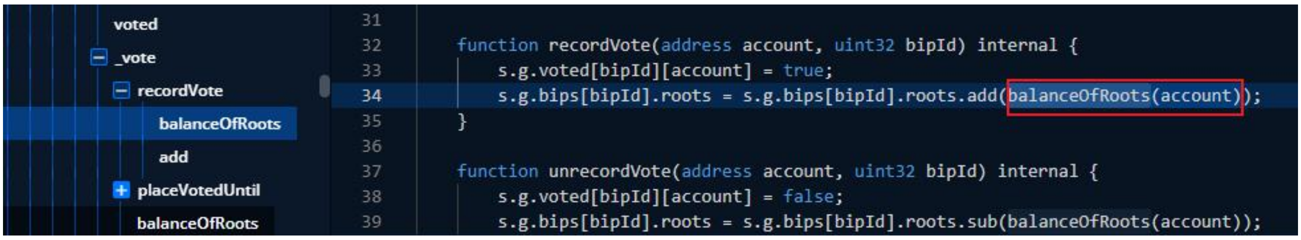


混币
发起攻击
创建提案合约
转账
发起提案
创建 Bip18 提案合约
将兑换的 212k BEAN 存入 Beanstalk Protocol 合约
将 BEAN 授权给 Beanstalk Protocol 合约
将 73 ETH 兑换为 212k BEAN

0xd9c57ec0072571029f...	Deposit	14602877	2022-04-17 12:43:54	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.03872852
0xd19aa91b3928de0025...	Deposit	14602829	2022-04-17 12:32:49	Beanstalk Flashloan Exp...	OUT	Tornado.Cash: Router	100 Ether	0.0249621
0xcd314668aaa9bbfebaf...	0x60806040	14602790	2022-04-17 12:24:16	Beanstalk Flashloan Exp	OUT	Contract Creation	0 Ether	0.33792333
0x677660ce489935b94b...	Buy And Free2245...	14602790	2022-04-17 12:24:16	Beanstalk Flashloan Exp...	OUT	0x4e59b44847b3795785...	0 Ether	0.01434477
0x3cb358d40647e178ee...	Transfer	14596011	2022-04-16 11:17:43	Beanstalk Flashloan Exp	OUT	0xe5ecf73603d98a0128f...	0.25 Ether	0.00041721
0x9575e478d7c542558e...	0x956afd68	14595964	2022-04-16 11:05:53	Beanstalk Flashloan Exp...	OUT	Beanstalk: Beanstalk Pro...	0 Ether	0.00374221
0x68cdec0ac76454c3b0f...	0x956afd68	14595906	2022-04-16 10:54:45	Beanstalk Flashloan Exp...	OUT	Beanstalk: Beanstalk Pro...	0 Ether	0.00565519
0xd09b72275962b03dd9...	0x60806040	14595637	2022-04-16 9:52:35	Beanstalk Flashloan Exp...	OUT	Create: InitBip18	0 Ether	0.0027484
0xf5a698984485d01e09...	Deposit Beans	14595357	2022-04-16 8:47:37	Beanstalk Flashloan Exp...	OUT	Beanstalk: Beanstalk Pro...	0 Ether	0.00383697
0xf1d80ba0ca6db75bed...	Approve	14595342	2022-04-16 8:45:23	Beanstalk Flashloan Exp...	OUT	Beanstalk: BEAN Token	0 Ether	0.00098018
0xfdd9acbc3fae083d572...	Swap Exact ETH F...	14595309	2022-04-16 8:38:56	Beanstalk Flashloan Exp...	OUT	Uniswap V2: Router 2	73 Ether	0.0032524
0x6ccc50eaf0eeb98183e...	Swap Exact ETH F...	14595304	2022-04-16 8:36:52	Beanstalk Flashloan Exp...	OUT	Uniswap V2: Router 2	72 Ether	0.00070793

In terms of time, the attackers made adequate preparations on the 16th, and launched an attack on the 17th after a full day. This is because voting does not start until 1 day after the proposal.

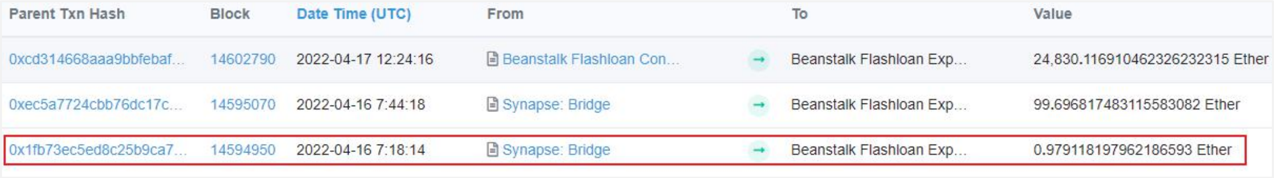
Furthermore, from the perspective of the entire attack process, the attacker analyzed the entire transaction and found that the number of votes in the voting contract was calculated based on the BEAN3CRV-f token holdings in the account during the entire attack process.



```
    function recordVote(address account, uint32 bipId) internal {
        s.g.voted[bipId][account] = true;
        s.g.bips[bipId].roots = s.g.bips[bipId].roots.add(balanceOfRoots(account));
    }

    function unrecordVote(address account, uint32 bipId) internal {
        s.g.voted[bipId][account] = false;
        s.g.bips[bipId].roots = s.g.bips[bipId].roots.sub(balanceOfRoots(account));
```

The attacker took advantage of this vulnerability to obtain a large number of tokens through flash loans, put these tokens into the mining pool, and temporarily obtained a large number of BEAN3CRV-f tokens, As a result, the attacker has an absolute advantage in the number of votes, Attacker can decided his own proposal by himself without others' votes. Finally, a large number of Tokens were stolen.

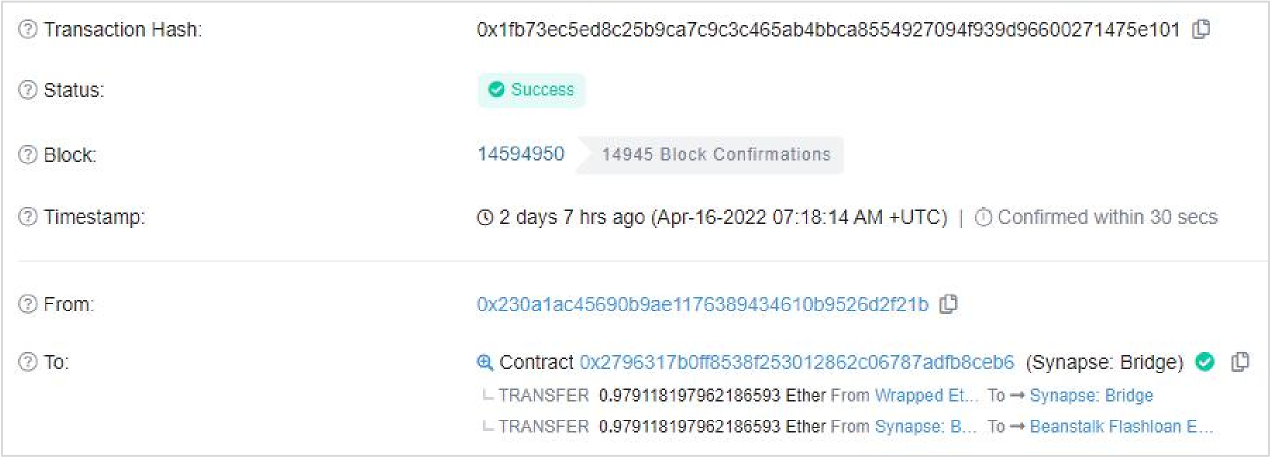
In addition, the internal transaction analysis of the attacker's address is as follows:



Parent Txn Hash	Block	Date Time (UTC)	From		To	Value
0xcd314668aaa9bbfebaf...	14602790	2022-04-17 12:24:16	Beanstalk Flashloan Con...	→	Beanstalk Flashloan Exp...	24,830.116910462326232315 Ether
0xec5a7724cbb76dc17c...	14595070	2022-04-16 7:44:18	Synapse: Bridge	→	Beanstalk Flashloan Exp...	99.696817483115583082 Ether
0x1fb73ec5ed8c25b9ca7...	14594950	2022-04-16 7:18:14	Synapse: Bridge	→	Beanstalk Flashloan Exp...	0.979118197962186593 Ether

We found that the start-up funds for the attacker's address to launch the attack came from the Synapse Bridge, as follows:

Transaction: 0x1fb73ec5ed8c25b9ca7c9c3c465ab4bbca8554927094f939d96600271475e101



Transaction Hash:	0x1fb73ec5ed8c25b9ca7c9c3c465ab4bbca8554927094f939d96600271475e101
Status:	Success
Block:	14594950 14945 Block Confirmations
Timestamp:	2 days 7 hrs ago (Apr-16-2022 07:18:14 AM +UTC) | Confirmed within 30 secs
From:	0x230a1ac45690b9ae1176389434610b9526d2f21b
To:	Contract 0x2796317b0ff8538f253012862c06787adfb8ceb6 (Synapse: Bridge) ✓ TRANSFER 0.979118197962186593 Ether From Wrapped Et... To → Synapse: Bridge TRANSFER 0.979118197962186593 Ether From Synapse: B... To → Beanstalk Flashloan E...

The main reason for this security incident is that the number of votes is obtained from the account's tokens, and the account's tokens can be obtained in one transaction through flash loans, and in a large amount. SharkTeam would like to remind you that:

(1) Separate voting and execution to ensure that voting and execution do not be in the same block time, i.e., voting and execution cannot be in the same transaction at the same time, thus avoiding the risks associated with flash loans.

(2) To avoid the impact of flash loans, increase authority, prohibit contract voting, and can only vote through the EOA account

(3) To prevent the implementation of malicious proposals as much as possible.The project party and community members should pay attention to all proposals, and should respond to and notify the risky proposals in a timely manner

(4) Multiple comprehensive contract audits can be undertaken prior to the project's start to ensure that the contract is safe.

3.3 Jay Chou's NFT was stolen by a phishing site on April Fool's Day

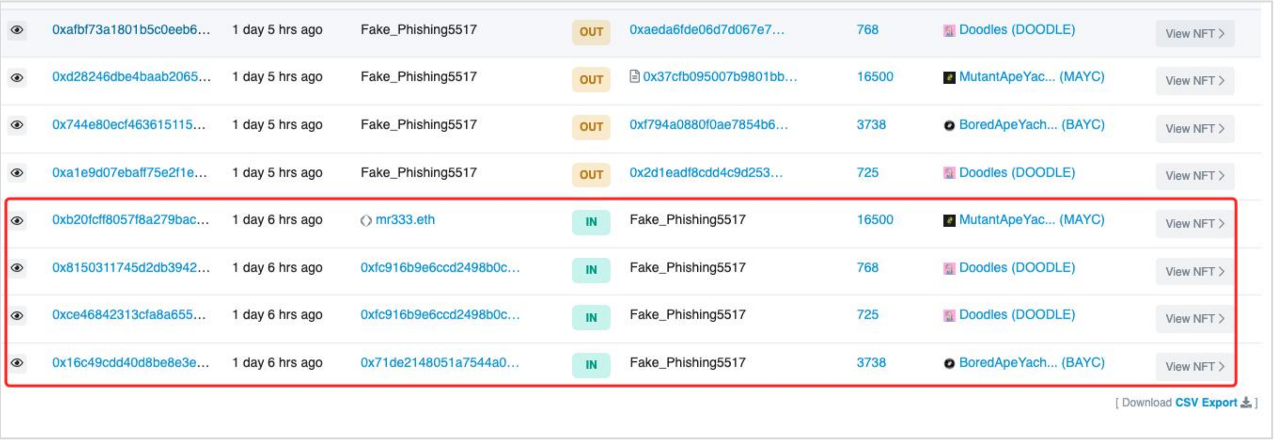
On April 1, 2022, April Fool's Day, Jay Chou posted on Instagram that the BAYC#3738 NFT he held (the NFT was presented by Huang Licheng in January this year) has been stolen! Also stolen was MAYC #16500 Doodles #768 Doodles #725, worth 169.6 ETH, more than 3 million.

Attacker address: 0xe34f004bdef6f069b92dc299587d6c8a731072da

1) Jay Chou was phished. He should have signed and authorized (approve)

the wallet address starting with 0x71de2 through a phishing website, and granted the NFT permission to the attacker's address (0xe34f00). At this time, Jay Chou did not realize that he was of NFTs are already at risk.

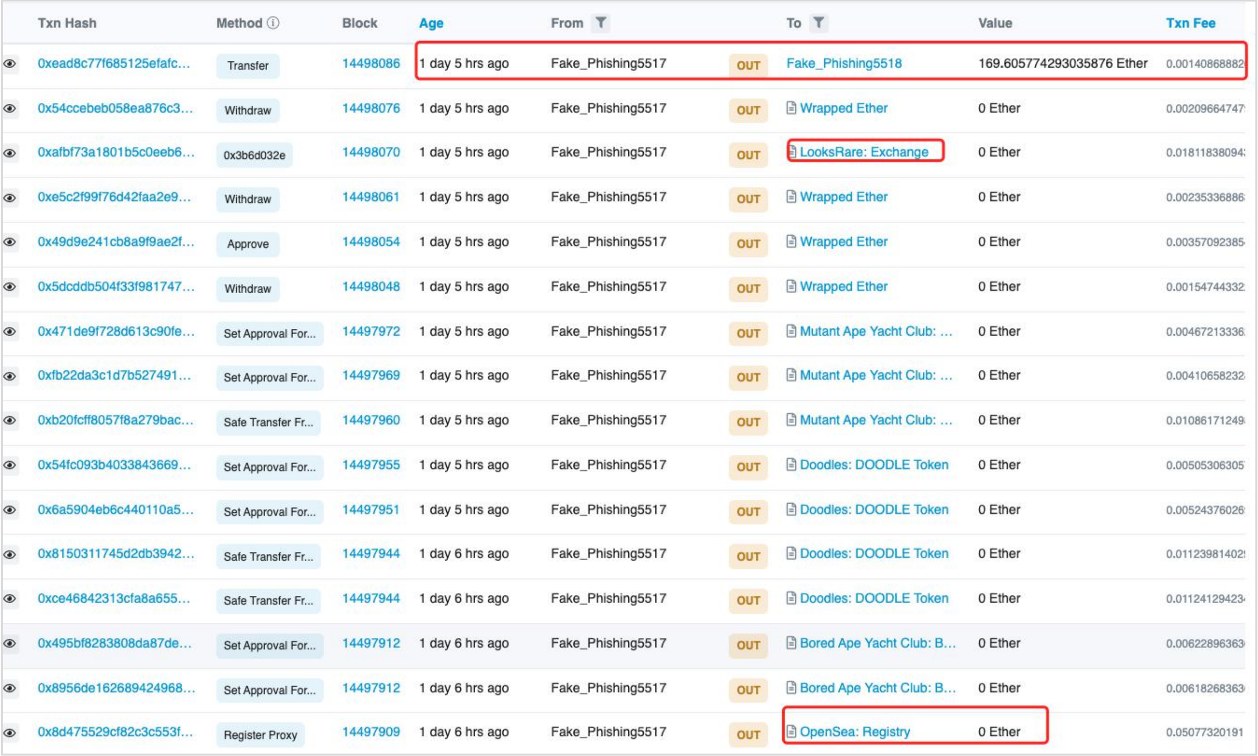
2) In the past few minutes, the attacker transferred these 4 NFTs to his own Address.



👁	0xafbf73a1801b5c0eeb6...	1 day 5 hrs ago	Fake_Phishing5517	OUT	0xaeda6fde06d7d067e7...	768	Doodles (DOODLE)	View NFT >
👁	0xd28246dbe4baab2065...	1 day 5 hrs ago	Fake_Phishing5517	OUT	0x37cfb095007b9801bb...	16500	MutantApeYac... (MAYC)	View NFT >
👁	0x744e80ecf463615115...	1 day 5 hrs ago	Fake_Phishing5517	OUT	0xf794a0880f0ae7854b6...	3738	BoredApeYach... (BAYC)	View NFT >
👁	0xa1e9d07ebaff75e2f1e...	1 day 5 hrs ago	Fake_Phishing5517	OUT	0x2d1eadf8cdd4c9d253...	725	Doodles (DOODLE)	View NFT >
👁	0xb20fcff8057f8a279bac...	1 day 6 hrs ago	mr333.eth	IN	Fake_Phishing5517	16500	MutantApeYac... (MAYC)	View NFT >
👁	0x8150311745d2db3942...	1 day 6 hrs ago	0xfc916b9e6ccd2498b0c...	IN	Fake_Phishing5517	768	Doodles (DOODLE)	View NFT >
👁	0xce46842313cfa8a655...	1 day 6 hrs ago	0xfc916b9e6ccd2498b0c...	IN	Fake_Phishing5517	725	Doodles (DOODLE)	View NFT >
👁	0x16c49cdd40d8be8e3e...	1 day 6 hrs ago	0x71de2148051a7544a0...	IN	Fake_Phishing5517	3738	BoredApeYach... (BAYC)	View NFT >

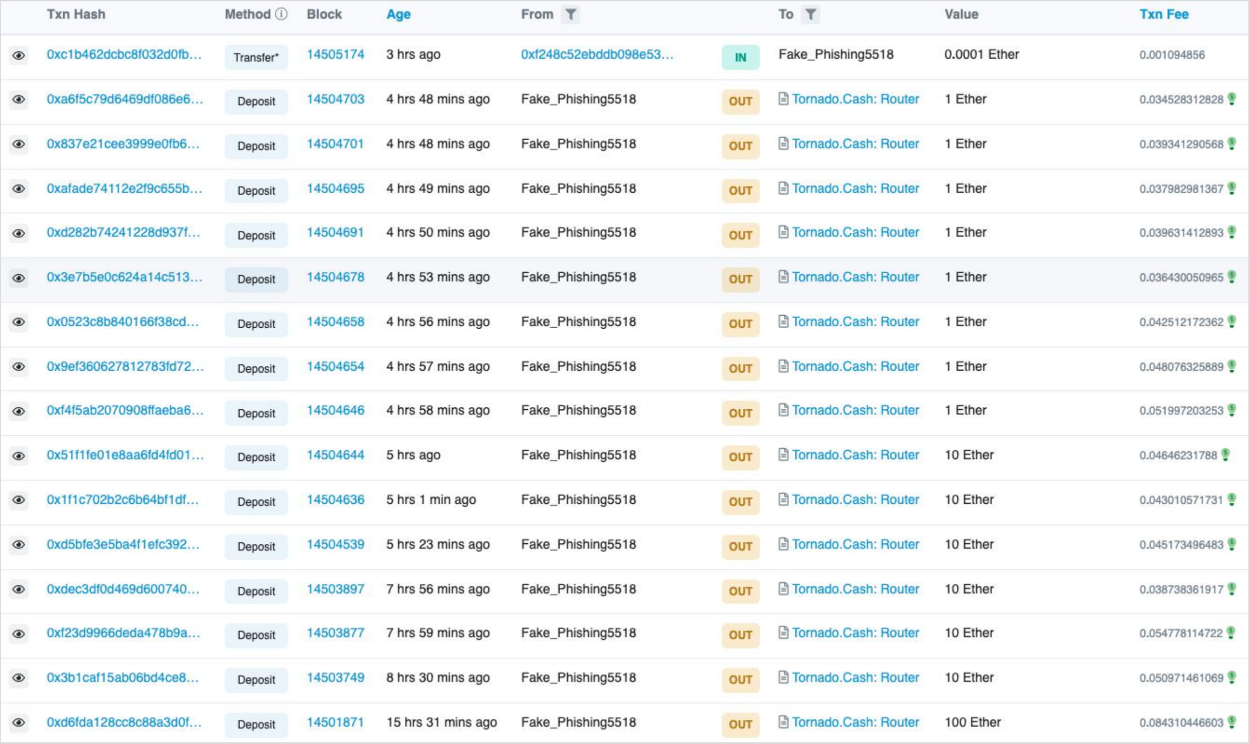
[Download **CSV Export**]

3） Sell the stolen NFT on LooksRare and OpenSea to get about 169.6 ETH.



	Txn Hash	Method ⓘ	Block	Age	From		To	Value	Txn Fee
👁	0xead8c77f685125efafc...	Transfer	14498086	1 day 5 hrs ago	Fake_Phishing5517	OUT	Fake_Phishing5518	169.605774293035876 Ether	0.00140868882
👁	0x54ccebeb058ea876c3...	Withdraw	14498076	1 day 5 hrs ago	Fake_Phishing5517	OUT	Wrapped Ether	0 Ether	0.00209664747
👁	0xafbf73a1801b5c0eeb6...	0x3b6d032e	14498070	1 day 5 hrs ago	Fake_Phishing5517	OUT	LooksRare: Exchange	0 Ether	0.01811838094
👁	0xe5c2f99f76d42faa2e9...	Withdraw	14498061	1 day 5 hrs ago	Fake_Phishing5517	OUT	Wrapped Ether	0 Ether	0.00235336886
👁	0x49d9e241cb8a9f9ae2f...	Approve	14498054	1 day 5 hrs ago	Fake_Phishing5517	OUT	Wrapped Ether	0 Ether	0.00357092385
👁	0x5dcddb504f33f981747...	Withdraw	14498048	1 day 5 hrs ago	Fake_Phishing5517	OUT	Wrapped Ether	0 Ether	0.00154744332
👁	0x471de9f728d613c90fe...	Set Approval For...	14497972	1 day 5 hrs ago	Fake_Phishing5517	OUT	Mutant Ape Yacht Club: ...	0 Ether	0.00467213336
👁	0xfb22da3c1d7b527491...	Set Approval For...	14497969	1 day 5 hrs ago	Fake_Phishing5517	OUT	Mutant Ape Yacht Club: ...	0 Ether	0.00410658232
👁	0xb20fcff8057f8a279bac...	Safe Transfer Fr...	14497960	1 day 5 hrs ago	Fake_Phishing5517	OUT	Mutant Ape Yacht Club: ...	0 Ether	0.01086171249
👁	0x54fc093b4033843669...	Set Approval For...	14497955	1 day 5 hrs ago	Fake_Phishing5517	OUT	Doodles: DOODLE Token	0 Ether	0.00505306305
👁	0x6a5904eb6c440110a5...	Set Approval For...	14497951	1 day 5 hrs ago	Fake_Phishing5517	OUT	Doodles: DOODLE Token	0 Ether	0.00524376026
👁	0x8150311745d2db3942...	Safe Transfer Fr...	14497944	1 day 6 hrs ago	Fake_Phishing5517	OUT	Doodles: DOODLE Token	0 Ether	0.01123981402
👁	0xce46842313cfa8a655...	Safe Transfer Fr...	14497944	1 day 6 hrs ago	Fake_Phishing5517	OUT	Doodles: DOODLE Token	0 Ether	0.01124129423
👁	0x495bf8283808da87de...	Set Approval For...	14497912	1 day 6 hrs ago	Fake_Phishing5517	OUT	Bored Ape Yacht Club: B...	0 Ether	0.00622896363
👁	0x8956de162689424968...	Set Approval For...	14497912	1 day 6 hrs ago	Fake_Phishing5517	OUT	Bored Ape Yacht Club: B...	0 Ether	0.00618268363
👁	0x8d475529cf82c3c553f...	Register Proxy	14497909	1 day 6 hrs ago	Fake_Phishing5517	OUT	OpenSea: Registry	0 Ether	0.05077320191

(4) Transfer the stolen currency to the Tornado currency mixing platform through the address 0x6e85c36e75dc03a80f2fa393055935c7f3185b15.



	Txn Hash	Method ⓘ	Block	Age	From		To	Value	Txn Fee
👁	0xc1b462dcbc8f032d0fb...	Transfer*	14505174	3 hrs ago	0xf248c52ebddb098e53...	IN	Fake_Phishing5518	0.0001 Ether	0.001094856
👁	0xa6f5c79d6469df086e6...	Deposit	14504703	4 hrs 48 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.034528312828
👁	0x837e21cee3999e0fb6...	Deposit	14504701	4 hrs 48 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.039341290568
👁	0xafade74112e2f9c655b...	Deposit	14504695	4 hrs 49 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.037982981367
👁	0xd282b74241228d937f...	Deposit	14504691	4 hrs 50 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.039631412893
👁	0x3e7b5e0c624a14c513...	Deposit	14504678	4 hrs 53 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.036430050965
👁	0x0523c8b840166f38cd...	Deposit	14504658	4 hrs 56 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.042512172362
👁	0x9ef360627812783fd72...	Deposit	14504654	4 hrs 57 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.048076325889
👁	0xf4f5ab2070908ffaeba6...	Deposit	14504646	4 hrs 58 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	1 Ether	0.051997203253
👁	0x51f1fe01e8aa6fd4fd01...	Deposit	14504644	5 hrs ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	10 Ether	0.04646231788
👁	0x1f1c702b2c6b64bf1df...	Deposit	14504636	5 hrs 1 min ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	10 Ether	0.043010571731
👁	0xd5bfe3e5ba4f1efc392...	Deposit	14504539	5 hrs 23 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	10 Ether	0.045173496483
👁	0xdec3df0d469d600740...	Deposit	14503897	7 hrs 56 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	10 Ether	0.038738361917
👁	0xf23d9966deda478b9a...	Deposit	14503877	7 hrs 59 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	10 Ether	0.054778114722
👁	0x3b1caf15ab06bd4ce8...	Deposit	14503749	8 hrs 30 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	10 Ether	0.050971461069
👁	0xd6fda128cc8c88a3d0f...	Deposit	14501871	15 hrs 31 mins ago	Fake_Phishing5518	OUT	Tornado.Cash: Router	100 Ether	0.084310446603

It is worth noting that the attack address (0xe34f00) was used 3 or 4 days ago.

The entire attack process is obviously not automated through the contract, but someone released a "bait" and waited for Jay Chou to take the bait.

Manual operation is done within. We analyze that this time is different from the previous OpaSea phishing incident for all users, but a precise phishing attack against Jay Chou. It may be that people around Jay Chou obtained the authorization of Jay Chou's wallet address through a specific phishing website.

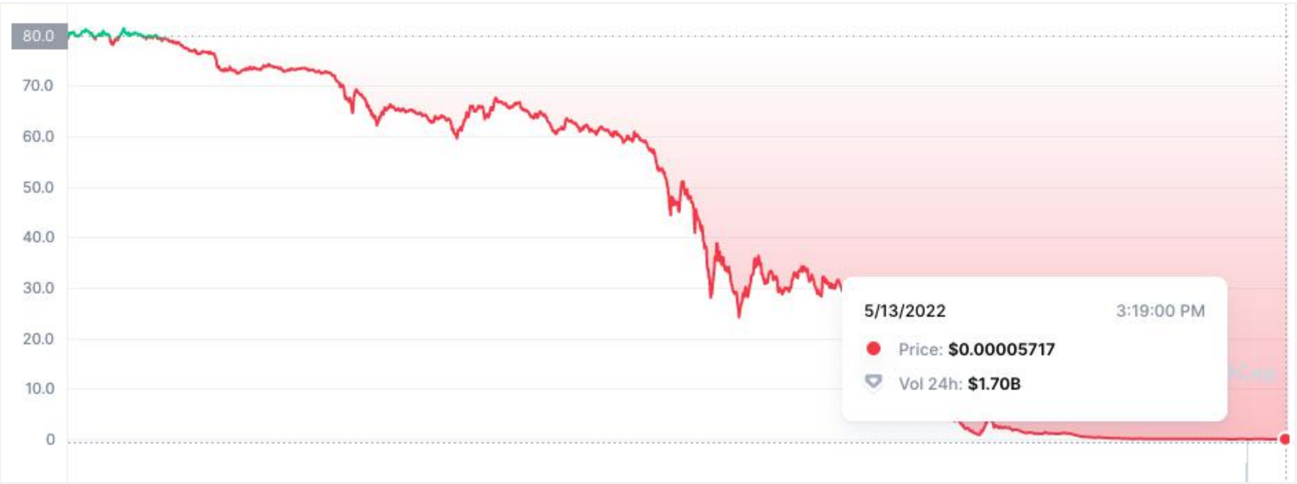
1. On the one hand, the attacker knows Jay Chou's specific wallet address, so he can immediately find out that Jay Chou's account is hooked and execute the follow-up immediately.

2. The attack address did not conduct any other phishing attacks before or after the attack, and was silent, which did not conform to the behavior logic of phishing attacks.

Security Suggestions: SharkTeam reminds you not to visit websites you are unfamiliar with or unsure about, and never authorize your address to any contract or project you are unsure about.

4. Crypto Wars

On May 13, Terra, the second largest economy in the world of decentralized finance, completely failed in this unprecedented crypto storm. In the five days from May 8 to today, Terra’s market value fell from nearly $25 billion to less than one billion. Terra’s main currency, Luna, fell from the original $80 to 0.00005, basically returning to zero. The Terra blockchain has been temporarily closed, and the algorithmic stable currency UST fell to $0.17.

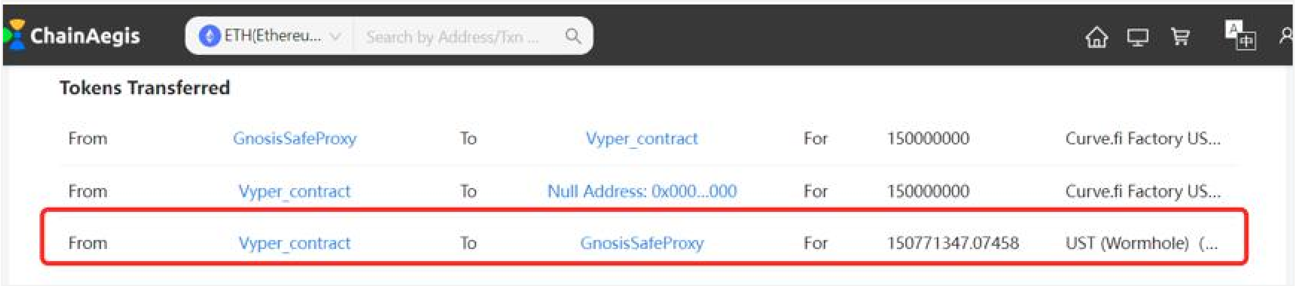


Objectively speaking, both views have their own basis. From the first day of UST's birth, there is a sword of Damocles hanging on its head. This sword of Damocles is not UST/Luna. mechanism, but rather the liquidity and pressure-bearing capacity of UST. If the liquidity of UST reaches a certain level, it will be difficult to beat (more than 4 billion US dollars), so UST, including other algorithmic stablecoins, is a confidence game in itself, winning by confidence and losing by confidence.

(1) 84 million breaking the balance: LFG's first mistake and the first suspicion of a premeditated attack

Like most stablecoins, the central battleground for the 1:1 peg between UST and the U.S. dollar is the decentralized stablecoin exchange Curve. Previously, the peg between UST and the U.S. dollar was mainly based on the UST-3Crv pool on Curve. Since March, preparations have been made to create a $4 billion UST+USDT+USDC+FRAX 4pool on Curve).

On May 8, LFG's pool address (0x6a97B6) withdrew $150 million in UST liquidity from the UST-3Crv pool.



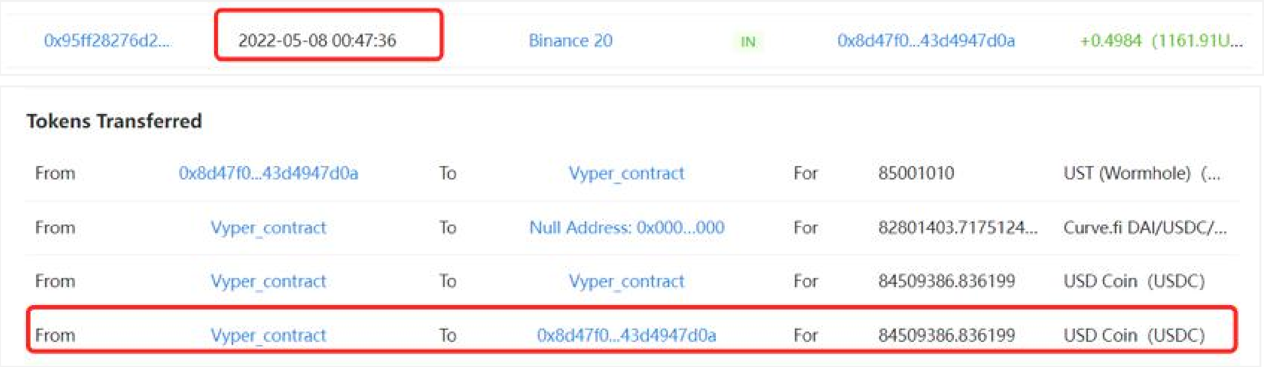
Tokens Transferred

From	GnosisSafeProxy	To	Vyper_contract	For	150000000	Curve.fi Factory US...
From	Vyper_contract	To	Null Address: 0x000...000	For	150000000	Curve.fi Factory US...
From	Vyper_contract	To	GnosisSafeProxy	For	150771347.07458	UST (Wormhole) (...

This address has been actively participating in the Luna and UST ecosystem since receiving initial funding from Coinbase on December 11, 2021.

This withdrawal of funds, although Terra was preparing for the construction of 4pool, also directly reduced the liquidity in UST-3Crv to about $700 million. According to Curve's liquidity mechanism, if someone uses half of TVL's UST (more than 300 million) to exchange for 3CRV (3pool), the UST liquidity in UST-3Crv will be exhausted, and it will return to zero in a short time.

About 10 minutes later, a new address (0x8d47F0) that only became active on May 8 sold more than 84 million UST to UST-3Crv, causing UST-3Crv to lose balance. This address was only activated 5 hours before the attack, and the new address was activated to hide the identity and transfer a large amount of funds. This is the first doubt (we know that the address of the giant whale is generally protected by mechanisms such as hardware wallets and multi-signatures. New addresses are enabled, and large transactions usually do not occur immediately).

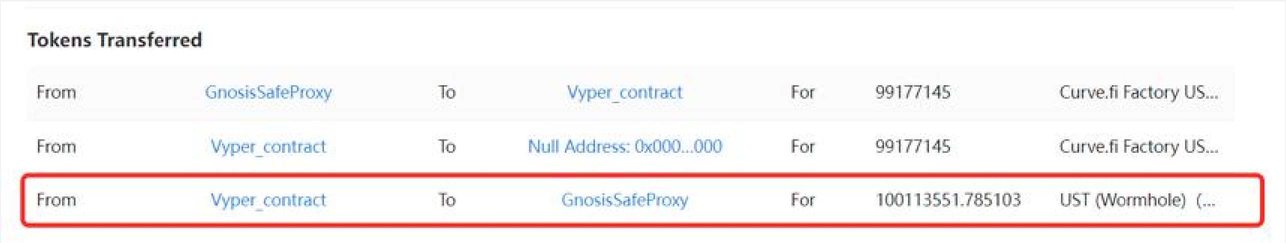


0x95ff28276d2...	2022-05-08 00:47:36	Binance 20	IN	0x8d47f0...43d4947d0a	+0.4984 (1161.91U...

Tokens Transferred

From	0x8d47f0...43d4947d0a	To	Vyper_contract	For	85001010	UST (Wormhole) (...
From	Vyper_contract	To	Null Address: 0x000...000	For	82801403.7175124...	Curve.fi DAI/USDC/...
From	Vyper_contract	To	Vyper_contract	For	84509386.836199	USD Coin (USDC)
From	Vyper_contract	To	0x8d47f0...43d4947d0a	For	84509386.836199	USD Coin (USDC)

After realizing that UST-3Crv was out of balance, LFG withdrew 100 million UST from UST-3Crv through another fund pool address (0xe89DA2) to restore the balance of the liquidity pool without immediately replenishing liquidity.



Tokens Transferred

From	GnosisSafeProxy	To	Vyper_contract	For	99177145	Curve.fi Factory US...
From	Vyper_contract	To	Null Address: 0x000...000	For	99177145	Curve.fi Factory US...
From	Vyper_contract	To	GnosisSafeProxy	For	100113551.785103	UST (Wormhole) (...

This leads to a further drop in the liquidity of UST-3Crv to around 500 million, and it only takes over $200 million to deplete the UST liquidity. This was the first mistake LFG made.

(2) Save the market: LFG made the second mistake and the second doubt

After LFG withdrew 150 million and 100 million in a row, including the chief security officer of Polygon and KOLs who opposed Terra immediately publicly expressed their doubts about LFG's two withdrawals. There were all kinds of rumors in the market, and there were overwhelming voices questioning LFG's cash out. Although Terra founder DK quickly made a statement: the first 150 million withdrawal is to prepare for 4pool, and the second 100 million is to balance liquidity, but the market is full of doubts about UST and Terra.

We conducted sentiment analysis on the Twitter messages about UST (50,000 pieces) 3 hours after the incident, and found that 78.32% of the messages were both questioning and negative, but historically the tweets supporting UST and questioning UST tended to tend to In the state of reciprocity, it can be seen from the data that the wind of public opinion has completely changed, and the balance is being quietly broken. This is the second doubt. Someone is manipulating or guiding public opinion.

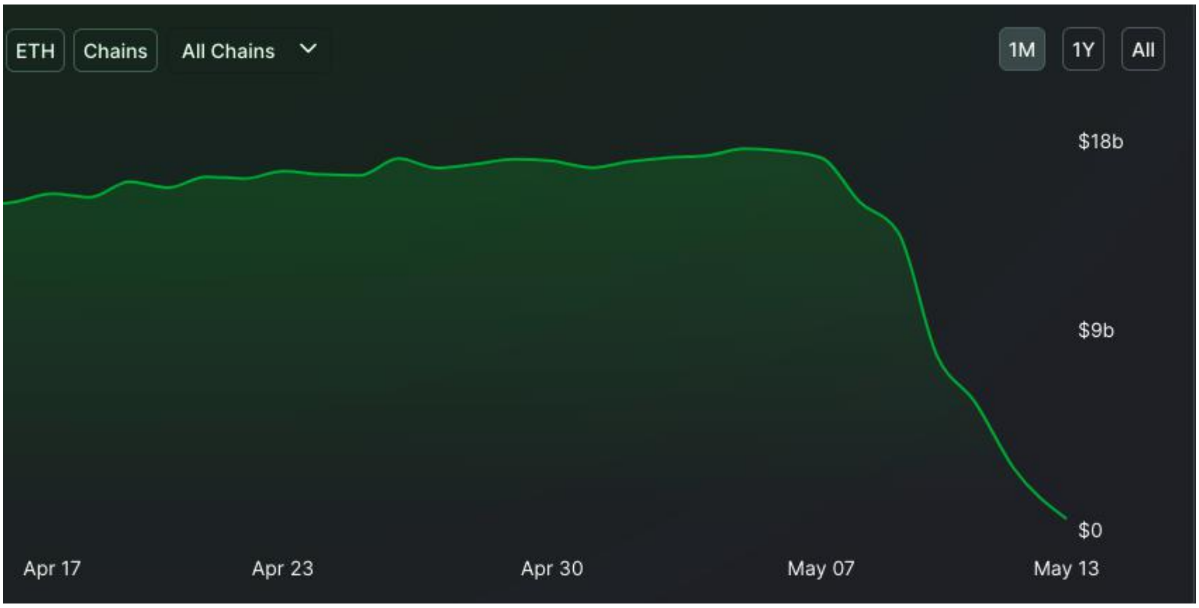
Market sentiment has deteriorated as a result of the effect in public opinion. Since May 8, giant whales have been selling UST continuously, and the market's selling pressure on UST has increased sharply. LFG uses market maker Jump Trading to sell ETH on the open market and afterwards buys back UST until the address is exhausted.

At this time, LFG has already committed the second fatal mistake: starting the bailout without a strategy. The lack of strategy is reflected in two aspects. On the one hand, a single address exhausted funds to save the market, causing LFG to sell its assets to recover. Everyone is analyzing how much wealth LFG has. In one calculation, there are only more than 70,000 bitcoins (2 billion), and the UST in the market There are nearly 18 billion, which is simply unacceptable; on the other hand, the market public opinion has not been corrected in time. You may ask, what should I do if the selling pressure increases? Just buy it back calmly and leave no trace, and do positive PR to let everyone know that the market is solving the problem by itself.

Who to save? Only those who are sick and have problems need to be saved. The loss of market confidence is the real culprit that has dragged UST into the abyss, and it's all of LFG's own making.

(3) Selling BTC: LFG made the third mistake and the third doubt

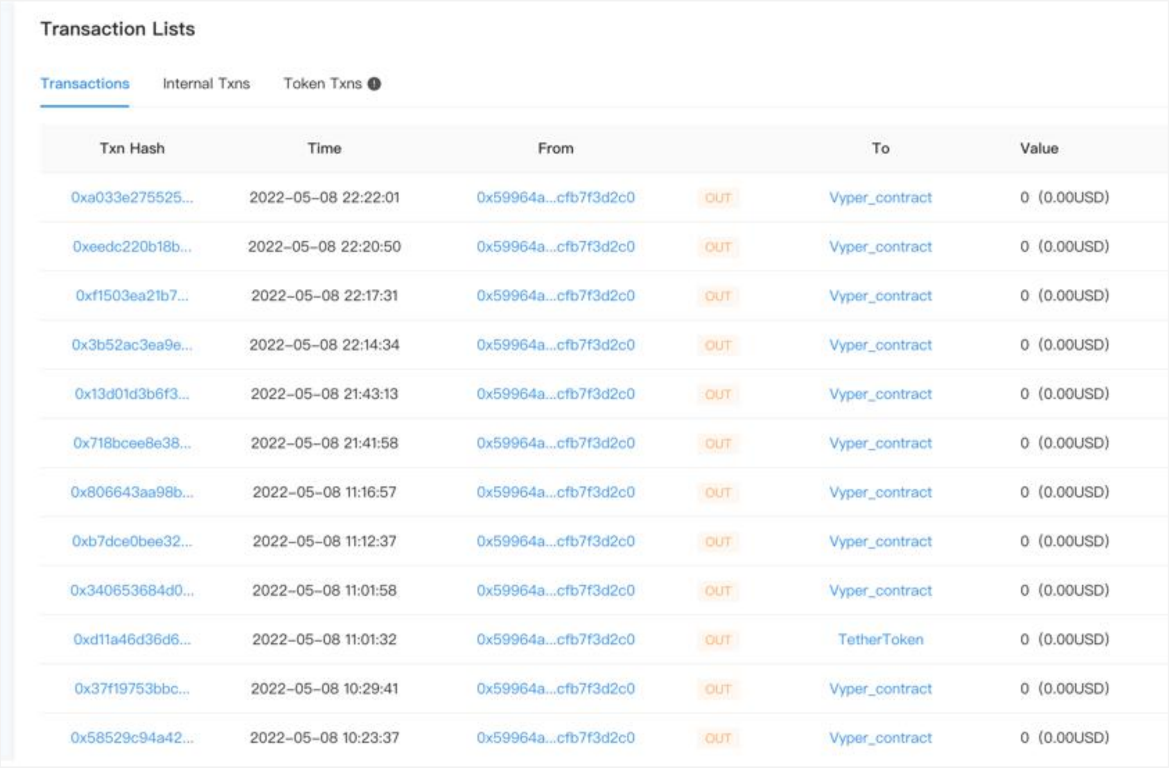
After the de-anchoring event on May 8, the 18 billion UST locked in Anchor began to be dumped on the market due to the loss of confidence and the spread of panic.



LFG officially announced the use of $700 million in Bitcoin reserves to maintain the stability of UST. However, there are 18 billion USTs in the market, 7 to 180, the market fear is further strengthened, and everyone starts to "run for their lives". Maybe DK also noticed that the funds were not enough, and sent a tweet: "More funds are being mobilized", you must know that more than 70,000 bitcoins have been prepared since March, and the $18 billion LFG will not be available in a short period of time. It may be raised, which is equivalent to telling everyone to speed up the "escape".

However, $700 million in bitcoin was thrown into the market, causing the price of bitcoin to plummet, and the market began to liquidate in a sequence of events, including the sale of UST and Luna. This is LFG's third mistake. By May 10, LFG had realized that its strategy of selling Bitcoin had failed and that the market could not manage it, so it stopped saving the market and decided to let it evolve on its own.

We found a third suspect in this round of UST sell-offs. After the May 8 incident, a new address (0x59964a), which was also activated on May 8, began reverse operations and absorbed more than 600 million UST in the market.

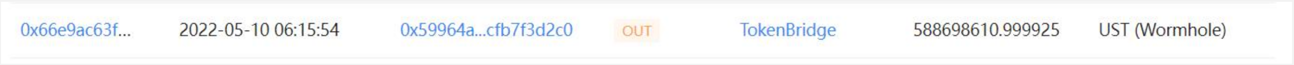


Transaction Lists

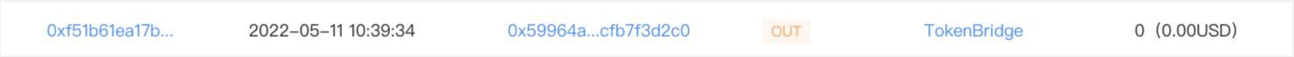
Transactions | Internal Txns | Token Txns

Txn Hash	Time	From		To	Value
0xa033e275525...	2022-05-08 22:22:01	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0xeedc220b18b...	2022-05-08 22:20:50	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0xf1503ea21b7...	2022-05-08 22:17:31	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0x3b52ac3ea9e...	2022-05-08 22:14:34	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0x13d01d3b6f3...	2022-05-08 21:43:13	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0x718bcee8e38...	2022-05-08 21:41:58	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0x806643aa98b...	2022-05-08 11:16:57	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0xb7dce0bee32...	2022-05-08 11:12:37	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0x340653684d0...	2022-05-08 11:01:58	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0xd11a46d36d6...	2022-05-08 11:01:32	0x59964a...cfb7f3d2c0	OUT	TetherToken	0 (0.00USD)
0x37f19753bbc...	2022-05-08 10:29:41	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0x58529c94a42...	2022-05-08 10:23:37	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)

Then there was a one-time sell-off of 588 million USTs on May 10 and nearly 30 million USTs on May 11.

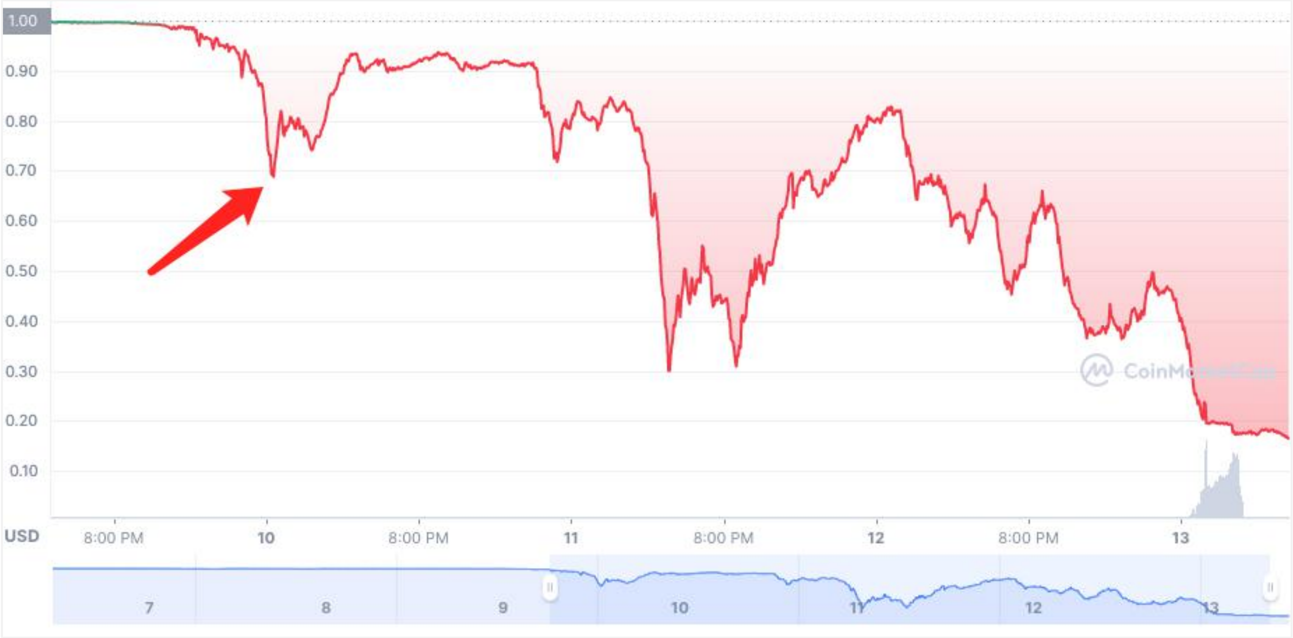


0x66e9ac63f...	2022-05-10 06:15:54	0x59964a...cfb7f3d2c0	OUT	TokenBridge	588698610.999925	UST (Wormhole)



0xf51b61ea17b...	2022-05-11 10:39:34	0x59964a...cfb7f3d2c0	OUT	TokenBridge	0 (0.00USD)

It can be said that the sell-off of this new address on May 10 made the severe de-anchoring of UST on May 10 inevitable. In fact, the lowest point of UST fell to 0.6 on May 10, which was seriously de-anchored, and LFG had used most of their reserves and almost ran out of ammunition and food. The subsequent process and results can be imagined.



The above three doubts make us have to suspect that this is a long-planned Soros-style financial attack (if you don’t know the operational logic of the Soros attack, you can check it out on the Internet, and I won’t go into details here),

The market is also full of such voices. Capital is profit-seeking. If it is financial hunting, it must be profitable. If this incident is an attack, will the attacker make money?

There are many voices in the market saying that some institutions raised 10w bitcoins for this attack. We use 10w bitcoins to estimate how much the attacker can gain if the incident is a financial attack.

1) Ambush: Assuming that the attacker's 10w bitcoins created a short position on March 22 when LFG started to accumulate bitcoin, the bitcoin price on March 22 was about $42,000, which is equivalent to creating $4.2 billion in bitcoin short position. Once the price of Bitcoin drops, the attacker will be rewarded. (And since March, Bitcoin has begun to show signs of decline, which also reduces the risk of shorts to a certain extent).

(2) Waiting for the opportunity: With the impact of the Fed’s interest rate hike, the Russian-Ukrainian war and other factors, the cryptocurrency market continued to decline, and the attacker’s attack time gradually began to mature.

(3) The time is ripe: the attackers set LFG to deploy 4pool to raise a large amount of funds from the existing liquidity pool as an opportunity to monitor the dynamics of LFG at all times. When the news is received on May 8 that LFG will start to allocate funds, it will start to

transfer funds from Binance. $84 million was removed as attack principal to prepare for attack. On the same day, LFG moved out 150 million UST as scheduled and launched the attack 10 minutes later.

(4) Attack strategy: smash UST and influence public opinion. On May 8th, 84 million USTs were temporarily de-anchored and affected public opinion. On May 9th, we continued to observe market sentiment and UST dynamics. When a large number of giant whales were found to sell UST or extract UST from Anchor, the attack strategy took effect (if If there is no market panic, continue to go back to the previous step and wait for the opportunity).

(5) Fatal blow: The attackers began to use another 600 million US dollars to absorb the UST thrown from the market and prepare for the fatal blow. On the morning of May 10th, the attacker threw the UST to a low of 0.6. Anchor, market confidence was defeated.

(6) Take the money and leave: After that, the attacker only needs to wait for LFG to use the more than 70,000 bitcoins in the reserve to save the market, wait for the bitcoin to plummet and profit from the 4.2 billion bitcoin shorts (not the attacker here for the time being) Whether part of the funds shorted Luna).

Principal: 4.2 billion shorts + 84 million attack start-up funds + 600 million attack reserves, nearly $4.9 billion (if the $600 million UST smashing is not an attacker's behavior, but a market behavior, the principal is 4.3 billion).

Cost: According to Curve's fee mechanism and fully consider the price fluctuation of UST during the attack process. 84 million is calculated at 1%, the first attack cost is 840,000; the second 600 million US dollar attack cost is calculated at 10%, and the cost is 60 million US dollars (if 600 million is market behavior, the cost here is 0).

Gains: If the attackers closed their positions on May 10 when Bitcoin was at $32,000, the $4.2 billion Bitcoin shorts would have made $952 million in gains.

Summary: Less than 4.5 billion in principal and less than 100 million in attack cost, with a profit of nearly $1 billion. And because of the existence of the UST death spiral, this kind of attack opportunity is bound to appear constantly, and if you seize it once, it will destroy the entire ecology and make a profit.

Summary： Stablecoins are the liquidity checkpoint of decentralized finance, full of benefits and risks. The stablecoin war has just begun and is far from over:

(1) On May 10th, May 11th, and May 12th, the U.S. Treasury Department kept saying that it would supervise stablecoins, and the SEC claimed that it would investigate the UST project party at any time. UST is a project of the Korean DK, which reminds people of the IMF's intervention and impact on the Korean economy during the economic crisis a few years ago. This should be a wake-up call for any stable currency, how to develop, how to supervise, and think deeply about the value industry and the relevant financial departments of various countries.

(3) Market risk: As institutions continue to enter the market, the crypto market may gradually become a game for professionals and capitalists, and high-level financial games will continue to occur, and high returns will no longer be the norm. Issues that both projects and users have to face and think carefully about.

(3) What should be the security mechanism of stablecoins: whether it is anchored by real assets like USDT and USDC, or algorithmic stablecoins such as DAI and UST. Are algorithmic stablecoins necessarily insecure? In fact, it is not always the case. Taking UST as an example, if LFG's $4 billion 4pool is completed, it will cost at least $2 billion to successfully prevent it from breaking the anchor. attack, only time will tell. Regardless of the type of stablecoin, the security of the economic model and on-chain risk monitoring and early warning are essential.

5. Summary

In the second quarter of 2022, there are two typical characteristics of Web3 security situation: on the one hand, the risk types of different chains are quite different, which is closely related to the differentiated business layout and underlying architecture; On the other hand, the security risks and attack types faced by business ecosystems such as defi, NFT and gamefi are very different from each other, which is related to their own business models and the construction of developer ecosystems.

Defi security remains the focus of attention in the second quarter of 2022, with about 75.1%

of attacks occurring in the field of Defi. However, although NFT, cross chain bridge and CEX security incidents are not as frequent as those of Defi, several incidents have caused huge losses, and the number of phishing attacks against NFT increased significantly in the second quarter. Security should be strengthened for all types of Web3 projects. Sharkteam reminds that Web3 team must pass the professional smart contract audit before the project is put on the shelves. After the project is put on the shelves, they also need to be aware of the situation of the project operation, so as to prevent trouble from happening and create better value for users.

SharkTeam

In Math，We Trust!

https://sharkteam.org

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg

北京 · 苏州 · 南京 · 广州 · 成都