SharkTeam

Web3 安全态势感知报告

2022 年 Q2

2022 年 7 月 25 日

SharkTeam 的愿景是全面保护 Web3 世界的安全。团队成员分布在北京、南京、苏州、硅谷，由来自世界各地的经验丰富的安全专业人士和高级研究人员组成，精通区块链和智能合约的底层理论，提供包括智能合约审计、链上分析、应急响应等服务。已与区块链生态系统各个领域的关键参与者，如 Huobi Global、OKC、polygon、Polkadot、imToken、ChainIDE 等建立长期合作关系。

目录

1．Web3 安全现状概览

2022 年上半年 Web3 生态因黑客攻击损失超 20 亿美元，相较于 2021 年全年损失的 15.5 亿美元，2022 年上半年的损失已超过 2021 全年总和。

在 Q2 季度，最常见的攻击手法为合约漏洞利用、闪电贷攻击和钓鱼攻击。DeFi 仍然是最易受到攻击的 Web3 业务，其次是 NFT。

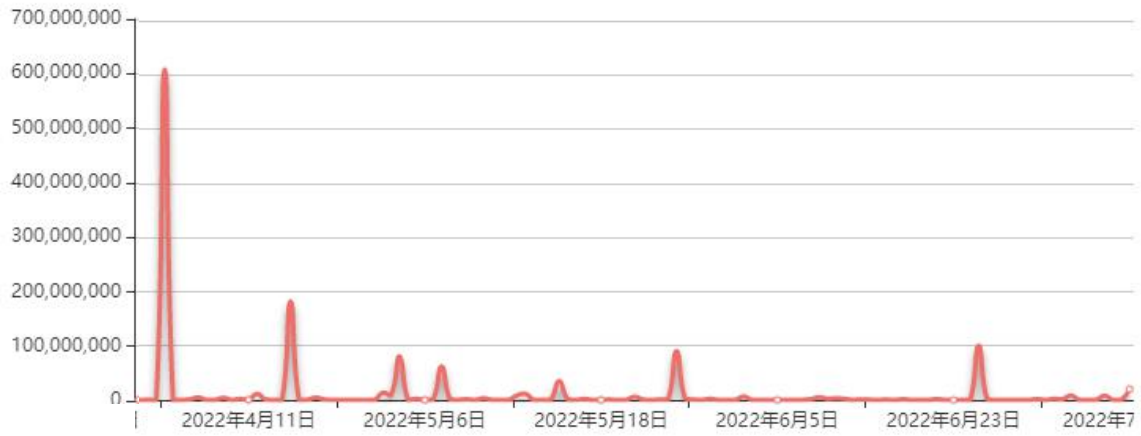
随着 Web3 生态的发展，各国政府也颁布了一系列政策，其中最具影响的是由美国拜登政府所签署的关于加密货币监管框架的行政命令，以及欧盟的 MiCA 法案。

总的来说，持续不断的熊市以及不间断的黑客攻击使 2022 Web3 生态面临挑战。

2．事件类型分析

Web3 生态 2022 年 Q2 被公开的安全事件 49 起；

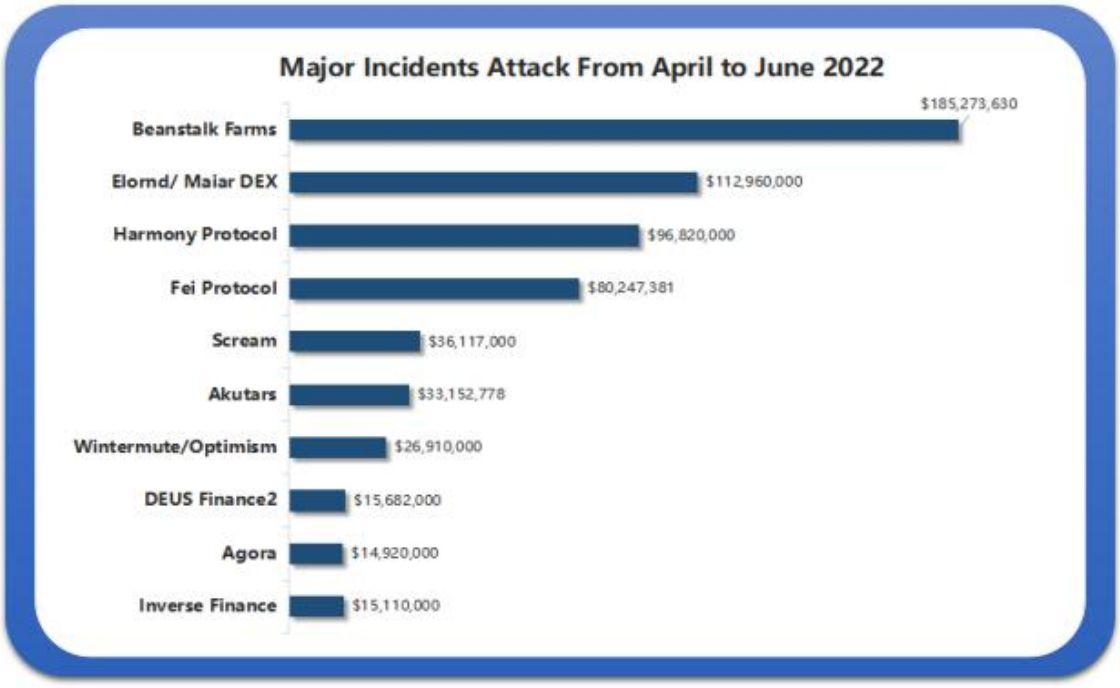
损失总金额约 $721,163,820 ；



2022 年第二季度 SharkTeam 共监测到 Web 3 领域主要攻击事件 49 起，总损失约 7 亿 2116 万美元。其中损失达一亿美元及以上的攻击事件 3 起，千万美元以上的攻击事件共 12 起，百万美元以上的攻击事件共 28 起。损失最高的事件是 Beanstalk Farms、Elrond 和 Harmony，分别为 1 亿

8200 万美元、1 亿 1300 万美元和 1 亿美元。

2.1 合约漏洞利用



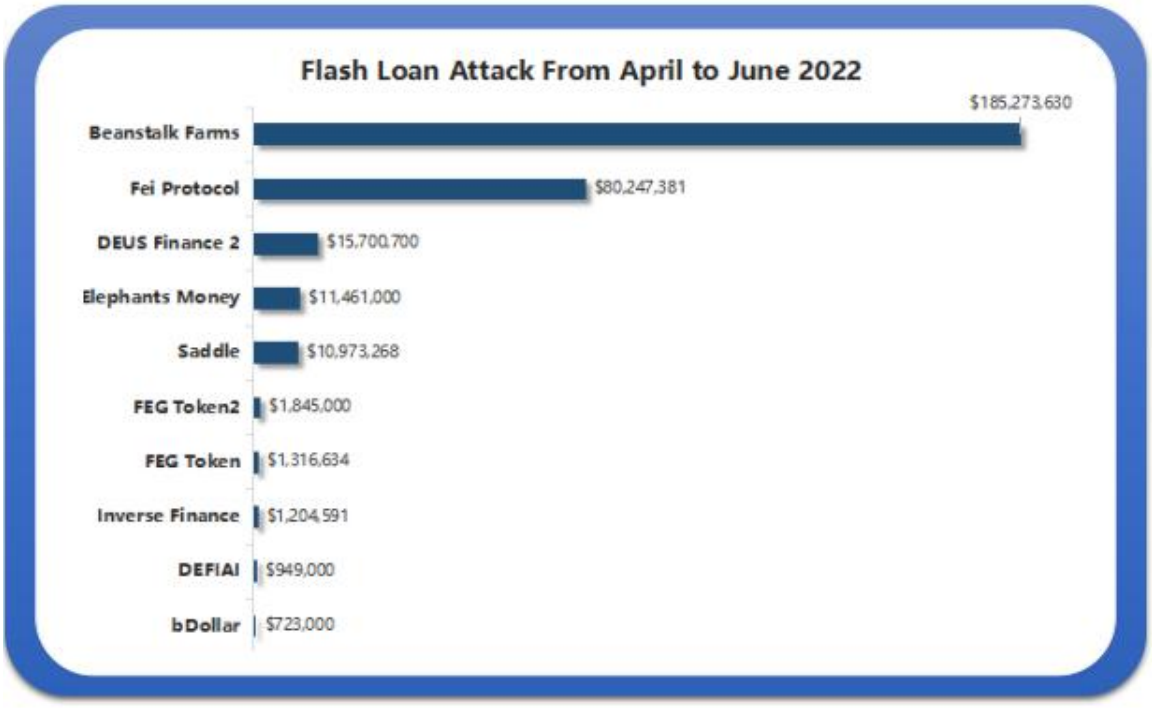
合约漏洞利用中包含了黑客不同的攻击手段，简单来说就是黑客利用基础设施或某些项目代码中的漏洞进行攻击。比如可能是多签密钥被泄露，或是铸币功能、重入问题或预言机本身存在的缺陷。虽然与本季度利用合约漏洞的攻击事件出现减少趋势，但此类型的攻击往往破坏性较强。

Q2 季度发生的合约漏洞利用，所造成的损失超过 5.3 亿美元，攻击次数达 40 次。与 Q1 相比，损失金额下降约 56.7%。但令人惊讶的是，攻击次数并未下降，实际上从 32 次增加到 40 次。

造成这种差异的主要原因是对 Ronin 网络的攻击，造成 6.24 亿美元的损失，占 Q1 漏洞利用损失的一半以上。 然而，即使没有 Ronin 攻击，每次攻击所损失的平均资金也从 1890 万下降到 1340 万。

2.2 闪电贷攻击

Flashloan 仍然是 Web3 安全的主要痛点之一，本季度有 28 次攻击涉及闪电贷，总共损失了 310,002,694 美元。与 Q1 相比，攻击次数和攻击损失的金额都有着巨大的增长。攻击次数从 Q1 的 15 次增加到第二季度的 28 次，增加了 46.4%，损失的资金金额从第一季度的 13,978,452 美元增加到第二季度的 310,002,694 美元，增加了 2000% 以上。



占本季度亏损最高的是黑客针对 Beanstalk Farms 盗取了 1.85 亿美元的安全事件。其次针对 Fei 协议的 8024 万美元闪电贷攻击也占了很大一部分。

对比 Q1 来看，最大的闪电贷事件是针对 Deus Finance 的 300 万美元攻击。然而即使没有这些，Q2 的闪电贷款攻击仍然比第一季度更具破坏性。以 Q1 和 Q2 为基准，我们可以预测损失近 6.78 亿美元，比上一年增加了 81%。此外，闪电贷攻击很少“只是”闪电贷攻击，它们通常涉及预言机、流动性以及更多合约漏洞利用。

2.3 钓鱼攻击

2022 年 Q2 的网络钓鱼攻击频率也有所增加。在 Q1 仅有 106 次，在 Q2 攻击次数翻倍增长达到近 300 次。

此外，Discord 已成为绝大多数钓鱼攻击尝试的载体。一方面，这表明它是人们首选的加密货币 / NFT 社交场景。但另一方面，相关报告也指出了它长期存在的安全问题。

在 Q2，虽然钓鱼攻击的次数增加了，但是由钓鱼攻击造成的损失较上一季度下降了 14.7%，为 3772 万美元。要归结为当前的加密货币熊市，这使得缺乏经验的投资者变得不那么容易被各种欺诈信息所愚弄。

2.4 Rugpulls

Rugpulls 仍很严重，本季度发生了 91 次，造成了 39,421,648 美元的损失。虽然这比第一季度增加了 18%，但与 2021 相比 Q2 此分类攻击有所下降。这很可能是持续熊市的导致的结果。

在经历了 Q2 发生的几件重大事件，如 Three Arrows Capital 破产和 Terra 的崩盘，导致投资者们对于手中的资产使用更加谨慎。

如上安全事件类型在 Q2 季度较常见，我们是否会迎来进入一个更好、更安全的加密市场，以及部分风险指标的下降是否会继续，这些都还有待观察，Web3 生态的安全将取决于投资者的安全认知程度、项目团队是否具有更好的安全机制以及市场是否简历更加完善的监管机制。

3. 典型案例分析

3.1 交易重放+管理漏洞，2000 万枚 OP 被盗事件分析

2022 年 6 月 9 日，据 Optimism 与加密货币做市商 Wintermute 透露，2000 万个 Optimism 代币被黑客盗取。6 月 9 日，Optimism 基金会向 Wintermute 授予了 2000 万枚 OP 代币.

交易发送完成后，Wintermute 发现无法访问这些代币，因为提供的地址是他们尚未部署到 Optimism/L2 的 Ethereum/L1 多签地址。该 Optimism/L2 多签地址由黑客部署，2000 枚 OP 代币也被黑客盗取。

5 月 27 日，Optimism 基金会通过多签合约分两次向 Wintermute 的多签合约地址转账 2000 万 OP 代币，并且在 26 日转账 1 枚 OP 代币，3 笔交易如下：

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)

根据交易时间以及交易中 OP 代币数量，我们分析，在 26 日，Optimism 基金会向 Wintermute 多签合约地址转账 1 枚 OP 代币作为测试，Optimism 基金会在 Wintermute 确认收到代币后将 2000 万枚 OP 代币通过连续的两笔交易发送给 Wintermute 多签合约地址。接收地址是 Wintermute 在 Ethereum/L1 上已部署的多签合约地址，因此 Wintermute 仅仅验证是否接收到了代币，但并没有验证该地址在 Optimism/L2 上的所有权，而此时在 Optimism/L2 上并没有实际部署多签合约，

这才给了黑客可乘之机。

首先，我们看一下 Optimism/L2 上的 0x4f3a 合约部署交易：

txHash 是 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)

注意到，该合约部署时间是 6 月 5 日，其中 Wintermute/OP Exploiter 是黑客的一个地址，简记为 0x60b2。

该交易是如何准确生成 0x4f3a 合约地址的呢？黑客重放了 3 笔交易，尤其是最后的 Gnosis Safe Proxy Factory 1.1.1 合约创建的交易，如下所示：

（1）Ethereum/L1 上的交易如下：

0x75a42f240d22951897...	0x60806040	9084508	2019-12-10 18:20:36	Gnosis Safe: Deployer 3	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

0x1aa7

（2）Optimism/L2 上的交易：

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

通过重放交易，黑客在 Optimism/L2 上面创建了跟 Ethereum/L1 上完全相同（地址与合约代码相同）的 Gnosis Safe：Proxy Factory 1.1.1 合约，其中创建代理合约函数如下：

```
64  contract ProxyFactory {
65
66      event ProxyCreation(Proxy proxy);
67
68      /// @dev Allows to create new proxy contact and execute a message call to the new proxy within one transaction.
69      /// @param masterCopy Address of master copy.
70      /// @param data Payload for message call sent to new proxy contract.
71      function createProxy(address masterCopy, bytes memory data)
72          public
73          returns (Proxy proxy)
74      {
75          proxy = new Proxy(masterCopy);
76          if (data.length > 0)
77              // solium-disable-next-line security/no-inline-assembly
78              assembly {
79                  if eq(call(gas, proxy, 0, add(data, 0x20), mload(data), 0, 0), 0) { revert(0, 0) }
80              }
81          emit ProxyCreation(proxy);
82      }
```

Gnosis Safe：Proxy Factory 1.1.1 合约使用的是 0.5 版本的 Solidity，使用 new 来创建合约时使用的是 create 命令，而不是 create2。使用 create 命令创建合约，合约地址是 msg.sender 以及 nonce 来计算的。在 Ethereum/L1 上面，创建多签合约 0x4f3a 的 msg.sender 就是 Gnosis Safe：Proxy Factory 1.1.1 的地址，黑客在 Optimism/L2 通过重放交易来创建于 Gnosis Safe：Proxy Factory 1.1.1 合约的主要目的就是为了保证在 Optimism/L2 上创建合约 0x4f3a 的 msg.sender 与在 Ethereum/L1 上一致，那么黑客可以很方便的通过智能合约（合约 0xe714）调用 createProxy 函数来创建出地址是 0x4f3a 的合约。

另外，合约 0xe714 的部署是在 6 月 1 日的以下交易中完成的：

txHash：0x69ee67800307ef7cb30ffa42d9f052290e81b3df6d3b7c29303007e33cd1c240

发起交易地址是 0x8bcfe4f1358e50a1db10025d731c8b3b17f04dbb（简记为 0x8bcf），这也是黑客所持有的地址。同时，这笔交易也是 0x8bcf 发起的第一笔交易，资金来源于 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

整个过程从时间上看，

（1）5 月 27 日，Optimism 地址 0x2501 向 Optimism/L2 上的 0x4f3a 地址转账 2000 万 OP，0x4f3a 地址在 Ethereum/L1 上是 Wintermute 的多签合约地址，但此时在 Optimism/L2 上面并没有部署合约；

（2）6 月 1 日，黑客地址 0x8bcf 部署合约 0xe714。

（3）6 月 5 日，黑客通过重放 Ethereum/L1 上的交易创建了 Gnosis Safe：Proxy Factory 1.1.1 合约，其地址与 Ethereum/L1 上一样；然后地址 0x60b2 通过合约 0xe714 部署了多签合约 0x4f3a，合约所有权归黑客所有，因此 5 月 27 日转入的 2000 万 OP 被黑客盗取。

（4）6 月 5 日，多签合约 0x4f3a 在接收到 2000 万 OP 后，将 100 万 OP 转账给黑客地址 0x60b2，然后将 100 万 OP 兑换成了 720.7 Ether。

（5）6 月 9 日，合约 0x4f3a 将其中的 100 万 OP 转账给了账户地址 0xd8da， 其他的 1800 万 OP 仍然在合约 0x4f3a 中。

安全建议：引发本次安全事件的根本原因是交易重放、Solidity 旧版本漏洞以及主链和侧链交易签名验证等综合因素，并不是因为项目方合约代码存在漏洞。另外，针对本次事件，项目方反应不及时、对合约管理不严格等也给了黑客可乘之机；从攻击时间线和攻击准备上看，也不排除 OP 内部有内鬼串通作案的可能。

3.2 闪电贷+提案攻击-Beanstalk Farms 攻击事件分析

2022 年 4 月 17 日，Beanstalk Farms 遭黑客攻击，损失超过 8000 万美元，包括 24830 ETH 和 3600 万 BEAN。

攻击者地址：0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4

攻击合约地址：0x728ad672409da288ca5b9aa85d1a55b803ba97d7

被攻击合约地址：0xC1E088fC1323b20BCBee9bd1B9fC9546db5624C5

关键攻击交易：0xcd314668aaa9bbfebaf1a0bd2b6553d01dd58899c508d4729fa7311dc5d33ad7

攻击过程包含的交易如下：

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

攻击过程分析如下：

（1）代币兑换

攻击者在通过 UniswapV2 将 73 ETH 兑换为 212k BEAN。

交易：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)

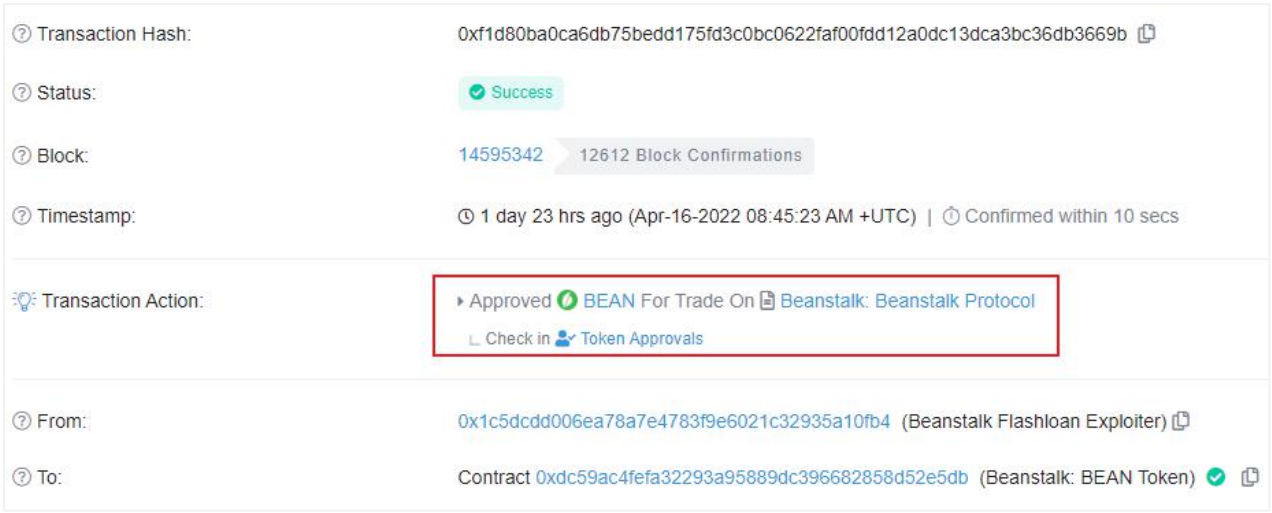
To: Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (Uniswap V2: Router 2)
TRANSFER 73 Ether From Uniswap V2: Ro... To Wrapped ...

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）代币授权

攻击者将 BEAN 授权给 Beanstalk Protocol 合约。

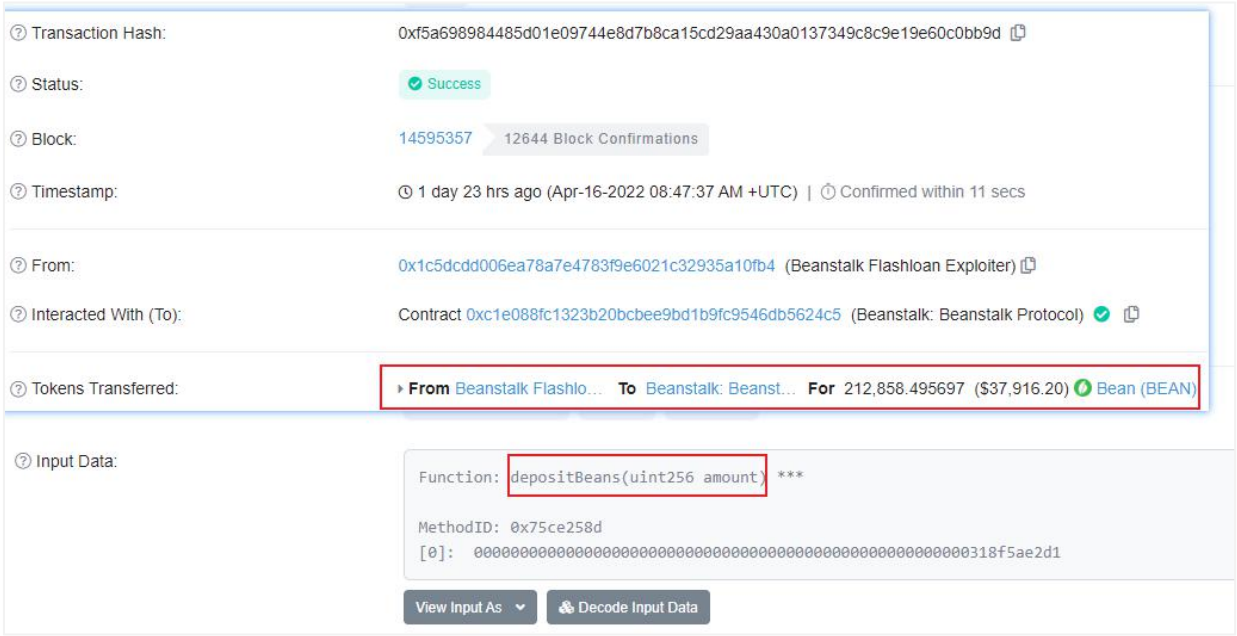
交易：0xf1d80ba0ca6db75bedd175fd3c0bc0622faf00fdd12a0dc13dca3bc36db3669b



（3）代币存储

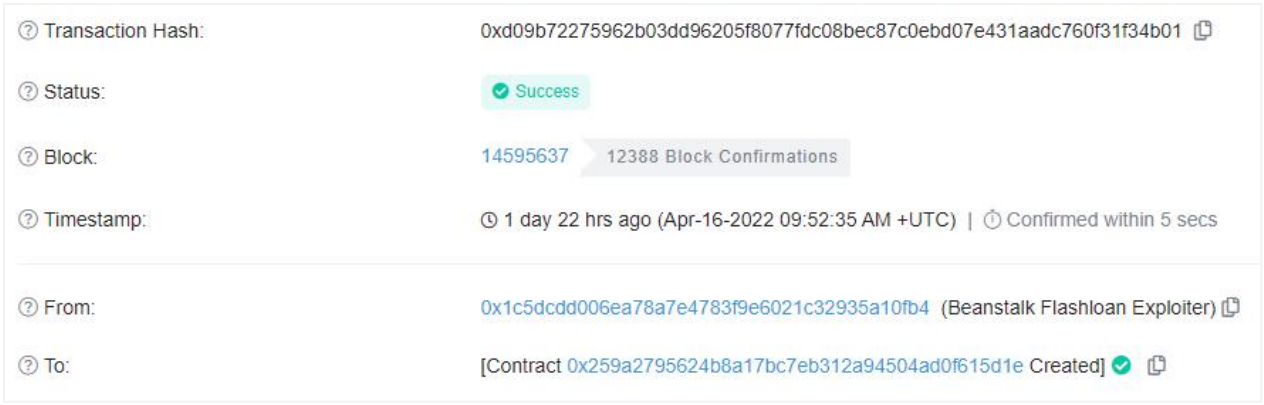
攻击者将兑换得到的 BEAN 存入 Beanstalk Protocol 合约，为攻击做准备。

交易：0xf5a698984485d01e09744e8d7b8ca15cd29aa430a0137349c8c9e19e60c0bb9d



（4）创建 InitBip18 提案合约

交易：0xd09b72275962b03dd96205f8077fdc08bec87c0ebd07e431aadc760f31f34b01

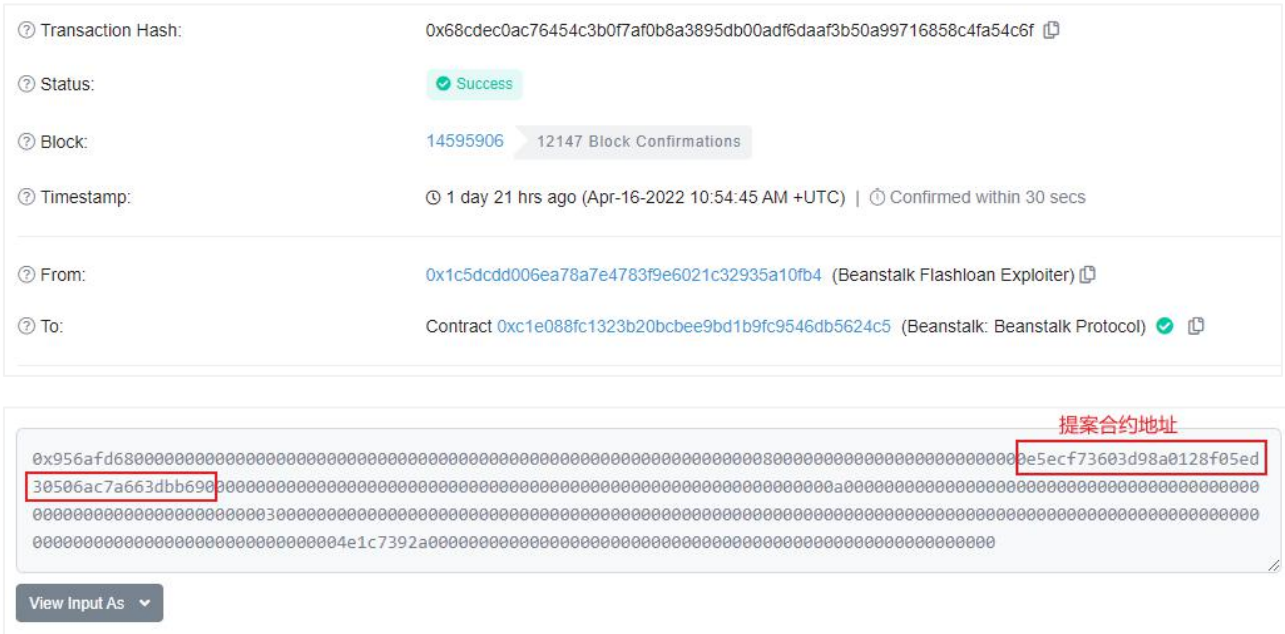


InitBip18 提案合约地址：0x259a2795624b8a17bc7eb312a94504ad0f615d1e

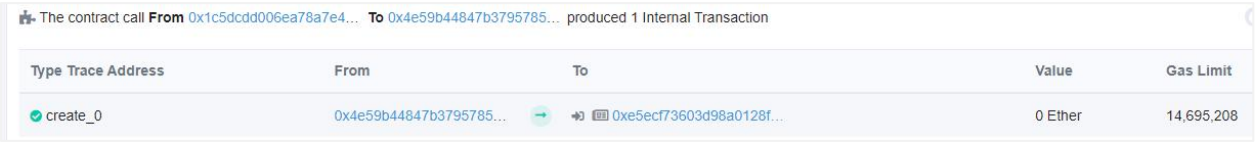
```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.13;

// 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）发起提案交易

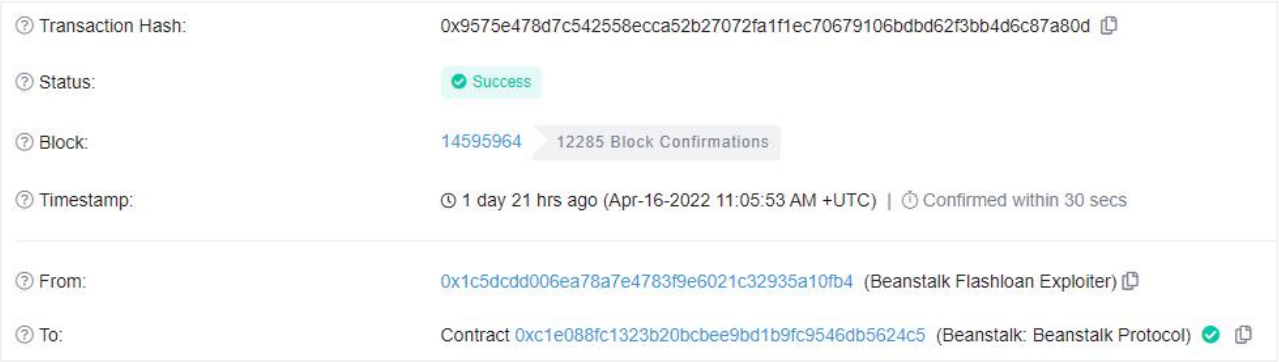
交易：0x68cdec0ac76454c3b0f7af0b8a3895db00adf6daaf3b50a99716858c4fa54c6f

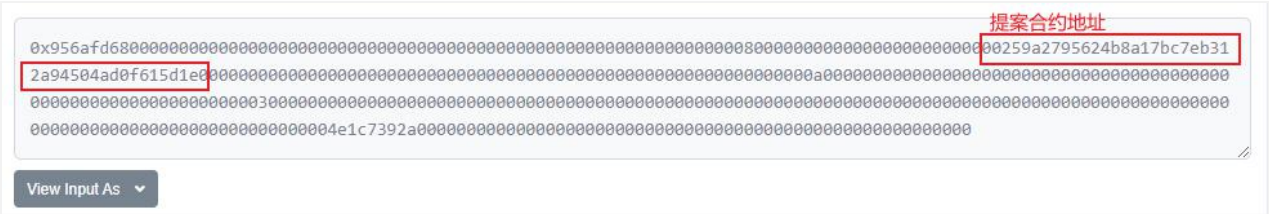


这里的提案合约地址是 0xe5ecf73603d98a0128f05ed30506ac7a663dbb69（简称合约 0xe5ec），该地址就是 InitBip18 提案合约中 Proposer Wallet。该合约是在交易 0x677660ce489935b94bf5ac32c494669a71ee76913ffabe623e82a7de8226b460 中创建的。



交易：0x9575e478d7c542558ecca52b27072fa1f1ec70679106bdbd62f3bb4d6c87a80d



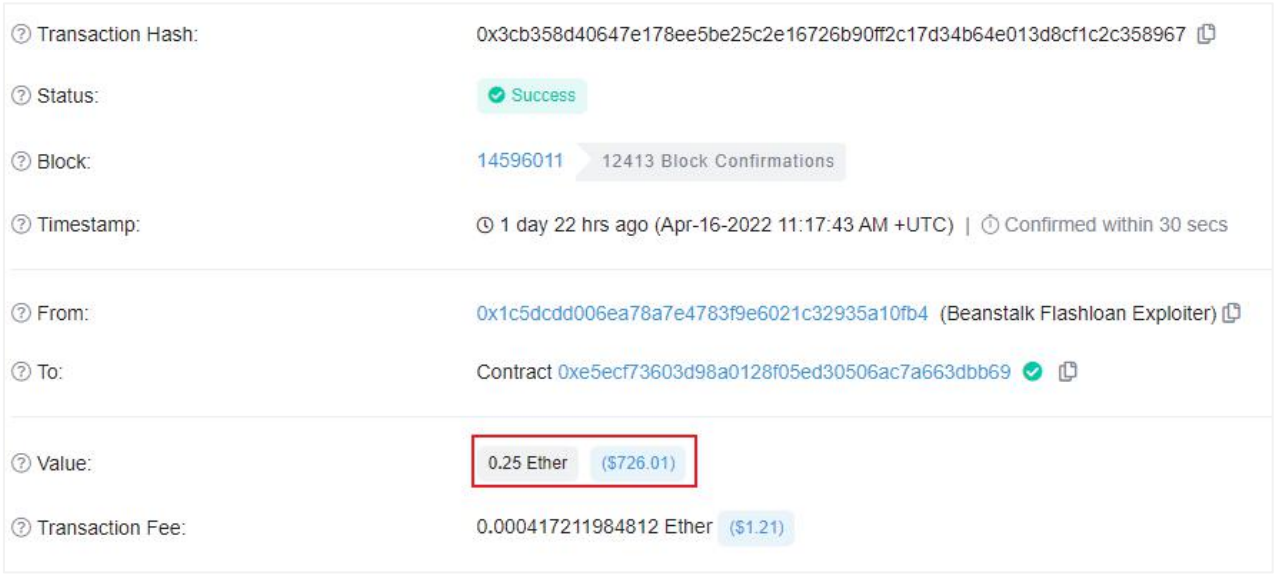


这里的提案合约地址就是上一步中的 InitBip18 提案合约。

（6）转账

攻击者向合约 0xe5ec 转入 0.25 ETH。

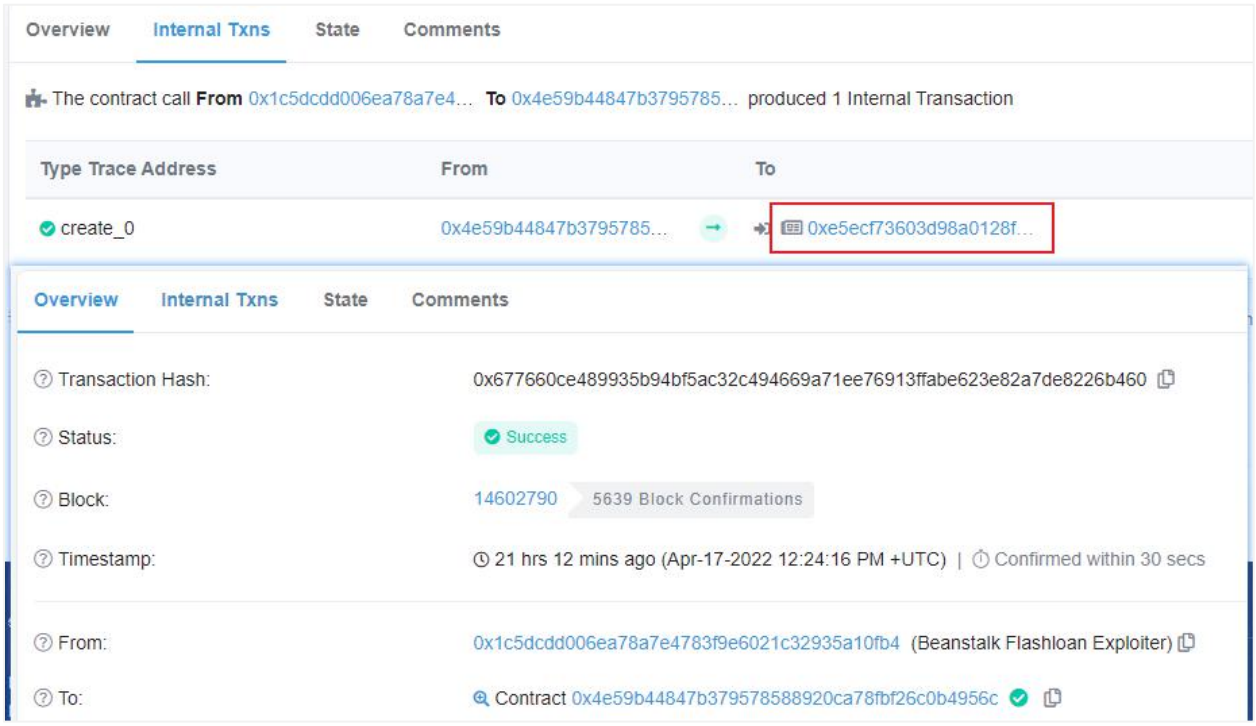
交易：0x3cb358d40647e178ee5be25c2e16726b90ff2c17d34b64e013d8cf1c2c358967



（7）创建提案合约 0xe5ec

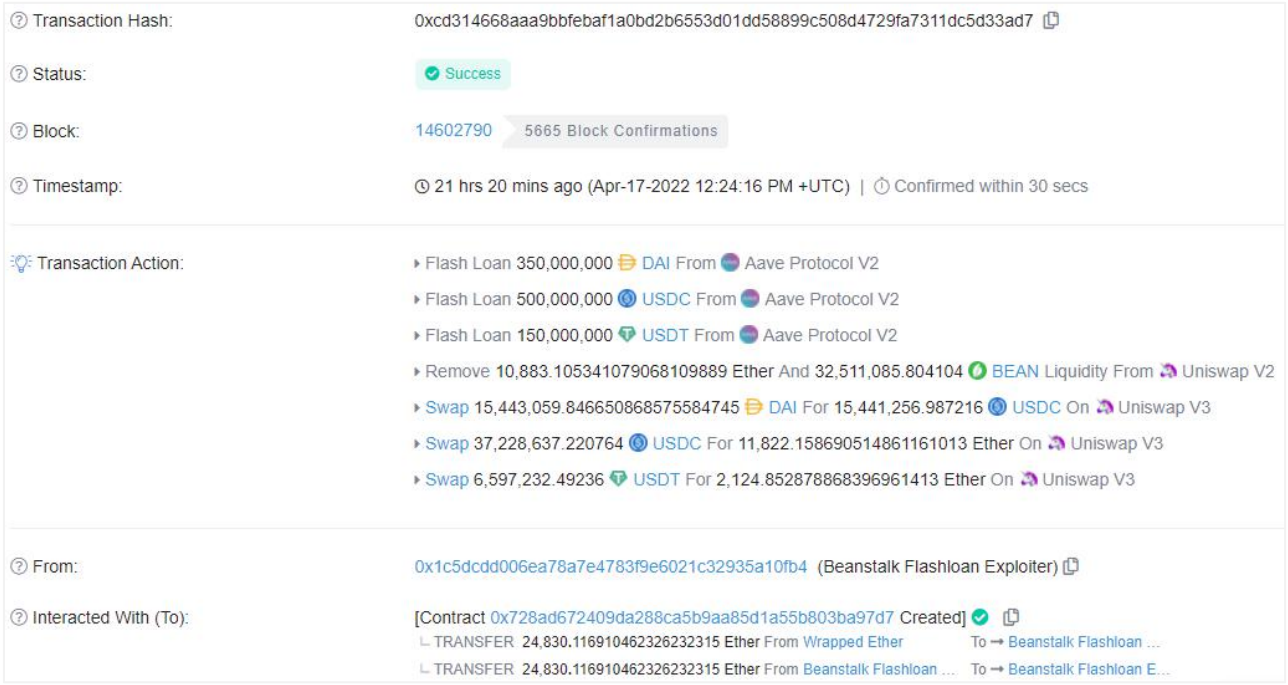
交易：0x677660ce489935b94bf5ac32c494669a71ee76913ffabe623e82a7de8226b460

在交易内部，创建了提案合约 0xe5ec。



（8）发起攻击

交易：0xcd314668aaa9bbfebaf1a0bd2b6553d01dd58899c508d4729fa7311dc5d33ad7



详细的攻击过程如下：

(a) 通过闪电贷从 Aave 平台借入 350M DAI，500M USDC 以及 150M USDT，从 Uniswap 平台借贷 32.1M BEAN，从 SushiSwap 平台借入 11.6M LUSD

(b) 将借入的 DAI、USDC 以及 USDT 全部投入到 Curve DAI/USDC/USDT 流动性矿池中，铸造出 979,691,328 个流动性代币 3Crv。

(c) 将 15M 3Crv 兑换成 15,251,318 LUSD，将 964,691,328 3Crv 添加流动性获得 795,425,740 BEAN3CRV-f，将 32,100,950 BEAN 以及 26,894,383 LUSD 添加流动性，获取 58,924,887 BEAN3CRV-f

(d) 使用上面得到的所有 BEAN3CRV-f 提案进行投票，使提案通过并执行。然后获得了 36,084,584 BEAN，0.5407 UNI-V2，874,663,982 NEAN3CRV-f 以及 60,562,844 BEANLUSD-f

(e) 移除流动性获得 1,007,734,729 3Crv 以及 28,149,504 LUSD

(f) 归还 SushiSwap 闪电贷的 11,678,100 LUSD 以及 32,197,543 BEAN，其中包含了手续费。

(g) 将剩余的 16,471,404 LUSD 兑换成 16,184,690 3Crv。

(h) 移除流动性 3Crv，得到 522,487,380 USDC，365,758,059 DAI 以及 156,732,232 USDT。

(i) 向 Aave 平台分别存入 350,315,000 DAI，500,450,000 USDC 以及 150,135,000 USDT 用于偿还闪电贷以及手续费。

(j) 移除 0.5407 UNI-V2 的流动性，获得 10,883 WETH 以及 32,511,085 BEAN 并归还闪电贷的金额以及手续费。

(k) 向 Ukraine Crypto Donation 捐赠了 250k USDC

(l) 将剩余的 Token 兑换成 WETH

(m) 将所得的 24,830 WETH 提取出来，并转账到攻击者地址，完成攻击。

（9）混币

攻击者将获得的 ETH 分批次存入混币平台 Tornash.Cash，实施混币。

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）安全建议

我们回顾整个攻击过程，如下：

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

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

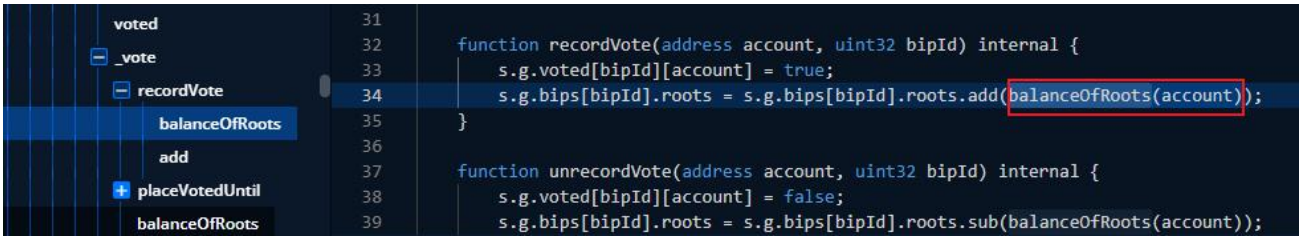
将 BEAN 授权给 Beanstalk Protocol 合约

将 73 ETH 兑换为 212k BEAN

从时间上看，攻击者在 16 号做足了准备工作，隔了整 1 天的时间，在 17 号发起了攻击。这是

因为提案后 1 天才能开始投票。

另外，从整个攻击过程看，攻击者在发起攻击的详细过程中，分析整个交易发现，投票合约中的票数是由账户中的 BEAN3CRV-f 代币持有量计算得到的。



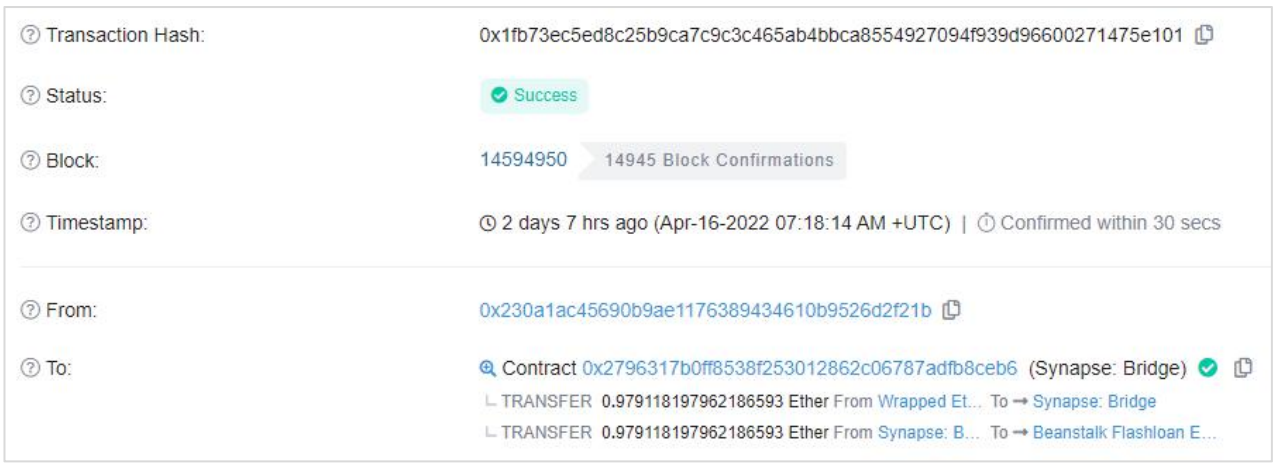
攻击者利用了该漏洞，通过闪电贷获得大量代币，将这些代币投入到矿池中，临时获得大量的 BEAN3CRV-f 代币，从而获得了绝对的票数优势，使得自己的提案可以由自己决定，而不需要其他人的投票。最终盗取了大量的 Token。

另外，分析攻击者地址的内部交易，如下：

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

我们发现，攻击者地址发起攻击的启动资金来自于 Synapse Bridge，如下：

交易：0x1fb73ec5ed8c25b9ca7c9c3c465ab4bbca8554927094f939d96600271475e101



本次安全事件的原因在于票数是由账户持有的代币得到的，而账户持有的代币是可以通过闪电贷在一笔交易内获取到的，而且可以获取的很大的数量。SharkTeam 提醒您：

（a）将投票和执行分离，保证投票和执行不在同一个区块时间，即不能在同一笔交易内同时完成投票和执行，这样也可以避免闪电贷带来的风险。

（b）增加权限，禁止合约投票，只能够通过 EOA 账户来投票，这样就可以规避闪电贷带来的影响。

（c）项目方以及社区成员应高度关注所有提案，对于有风险的提案， 应及时做出反应以及通知，尽可能的杜绝恶意提案的执行。

（d）在项目上线运行前，可以进行多次全面的合约审计，尽可能的保证合约的安全性。

3.3 周天王的愚人节-NFT 钓鱼攻击事件分析

2022 年 4 月 1 日，愚人节，周杰伦在 Instagram 上发文称持有的 BAYC#3738 NFT 已被盗了！同时被盗的还有 MAYC #16500 Doodles #768 Doodles #725，价值 169.6 ETH，超过 300 万元。攻击者地址：0xe34f004bdef6f069b92dc299587d6c8a731072da

（1）周董被钓鱼，应该是通过某个钓鱼网站将 0x71de2 开头的钱包地址签名授权（approve）交易，将 NFT 的权限授予了攻击者地址（0xe34f00），这时周董还没意识到自己的 NFT 已经处于风险之中。

（2）仅仅过去几分钟，攻击者就将这 4 个 NFT 转移到自己的地址中。

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）在 LooksRare 和 OpenSea 上将盗取的 NFT 卖掉，获得约 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）通过地址 0x6e85c36e75dc03a80f2fa393055935c7f3185b15 将脏款转入 Tornado 混币平台。

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

值得注意的是，攻击地址（0xe34f00）在 3、4 天前在开始使用，整个攻击过程很明显不是通过合约自动化执行，而是有人放出“诱饵”后等待周董上钩，之后一气呵成，在很短时间内手动操作完成。我们分析这次不同于之前面向所有用户的 OpeaSea 钓鱼事件，而是一次针对周董的

精准钓鱼攻击，可能是周董周围的人通过特定钓鱼网站获得了周董的钱包地址授权。

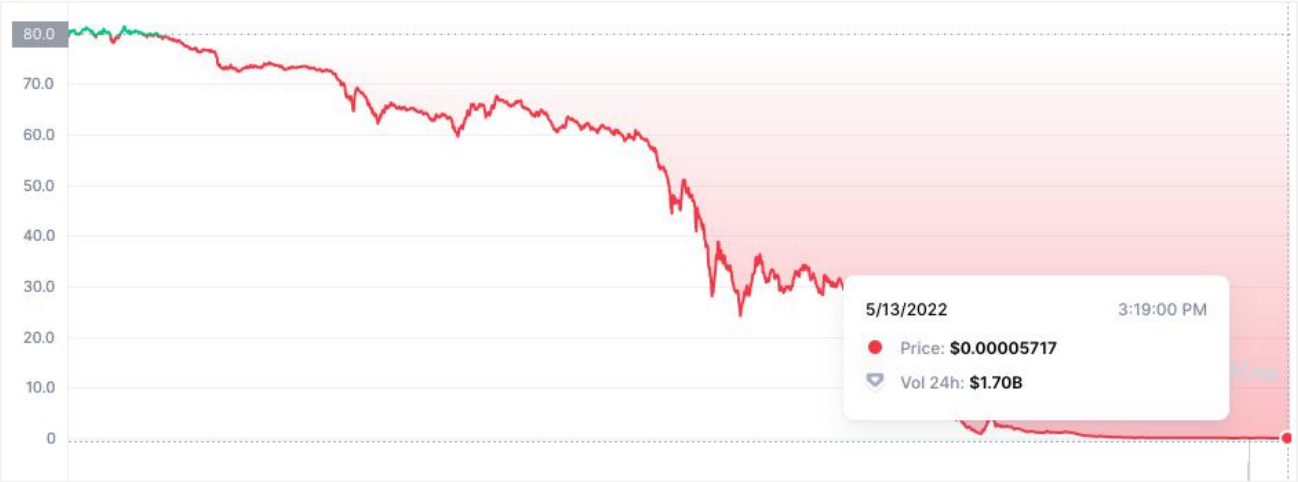
（a） 攻击者一方面知道周董具体的钱包地址，所以能第一时间发觉周董账号上钩并立即执行后续。

（b） 攻击地址在此次攻击前和攻击后都没有进行任何其他钓鱼攻击，处于静默，这不符合钓鱼攻击的行为逻辑。

安全建议：SharkTeam 提醒您，不要访问您不熟悉或不确定的网站，坚决不要将您的地址授权给任何您不确定的合约或项目。

4.加密战争

5 月 13 日，原去中心化金融世界的第二大经济体 Terra 在这场史无前例的加密风暴中彻底失败。从 5 月 8 日到今天的 5 天时间里，Terra 市值从原来近 250 亿美元跌至不到 10 亿。Terra 主币 Luna 从原 80 美元跌至 0.00005，基本归零，Terra 区块链已暂时关闭，算法稳定币 UST 跌至 0.17 美元。



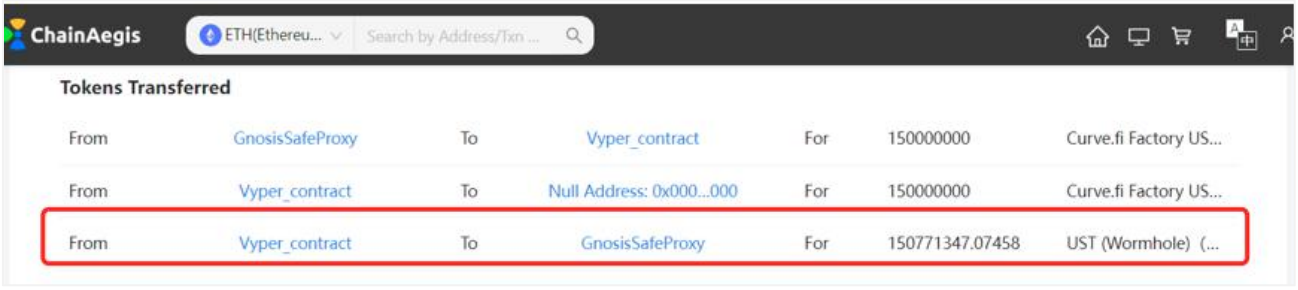
在我们之前的分析《去年 519，今年 510—从链上分析的角度看，LUNA 会不会真的陷入死亡螺旋》中详细的介绍了此次 Luna 死亡螺旋产生的原因。但这次事件真的只是一次不可预测的完美风暴吗？或是一次蓄谋已久的金融围猎呢？行业内关于这个问题的讨论也非常多，但更多的

还是主观猜测，不如让我们一起客观的进行分析，让线索说话、让数据说话。

（1）8400 万打破平衡：LFG 的第一个错误和蓄谋攻击的第一个疑点

和大多数稳定币一样，UST 与美元的 1:1 锚定的中心战场是去中心化稳定币交易所 Curve，之前 UST 与美元的的锚定主要基于 Curve 上的 UST-3Crv 池（Terra 从今年 3 月开始一直筹备在 Curve 上创建 40 亿美元的 UST+USDT+USDC+FRAX 的 4pool）。

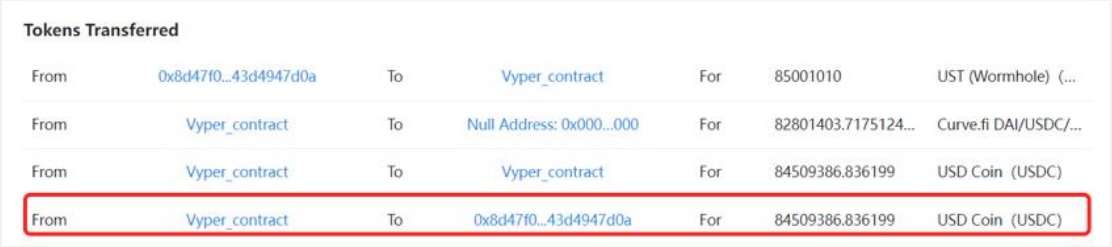
5 月 8 日，LFG 的资金池地址（0x6a97B6）从 UST-3Crv 池中撤走了 1.5 亿美元的 UST 流动性。



该地址从 2021 年 12 月 11 日从 Coinbase 获得初始资金后一直积极参与 Luna 与 UST 生态。

这次资金撤出虽然 Terra 是为了构建 4pool 做准备，但也直接导致 UST-3Crv 中的流动性降低到 7 亿美元左右。根据 Curve 的流动性机制，如果这时有人用 TVL 一半的 UST（3 亿多）去兑换 3CRV（3pool）就会导致 UST-3Crv 中 UST 流动性耗尽，短时会归零。

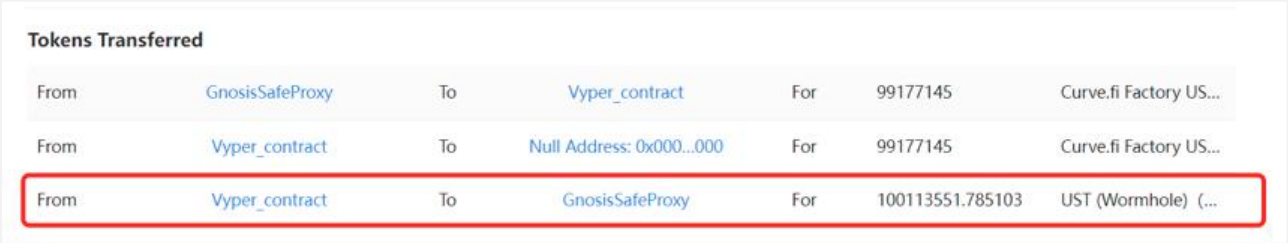
约 10 分钟后，一个 5 月 8 号当天才开始活跃的新地址（0x8d47F0）向 UST-3Crv 抛售了 8400 多万 UST，造成 UST-3Crv 失去平衡。这个地址是在攻击前 5 小时才启用的，启用新地址隐藏身份并调用大量资金，这是第一个疑点（我们知道巨鲸的地址一般都会通过硬件钱包、多签等机制保护，随意不会启用新地址，且通常不会立即进行大额交易）。



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)

在察觉 UST-3Crv 失去平衡后，LFG 通过另一个资金池地址（0xe89DA2）从 UST-3Crv 中撤出 1 亿的 UST 使流动性池恢复平衡，且没有立刻进行流动性补充。



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) (...

这导致 UST-3Crv 的流动性进一步下降到 5 亿左右，耗尽 UST 流动性只需要 2 亿多美元。这是 LFG 犯下的第一个错误。

（2）救市：LFG 犯下第二个错误和第二个疑点

LFG 连续撤出 1.5 亿和 1 亿资金后，包括 Polygon 首席安全官和各反对 Terra 的 KOL 立即公开表达了对 LFG 两次撤资的质疑，市场上各类谣言四起，质疑 LFG 套现的声音铺天盖地。虽然 Terra 创始人 DK 很快进行了声明：第一个 1.5 亿撤出是为 4pool 做准备，第二个 1 亿是为了平衡流动性，但是市场上充斥着的是对 UST 和 Terra 的质疑。

我们对事件发生后 3 小时的 Twitter 上关于 UST 的消息（5 万条）进行了情绪分析，发现 78.32% 的消息都是质疑和否定的，但历史上支持 UST 和质疑 UST 的 Twitter 一般呈现趋于对等的状态，从数据上可以看出舆论风向已经完全变了，平衡正在被悄然打破，这是第二个疑点，有人在操纵或引导舆论。

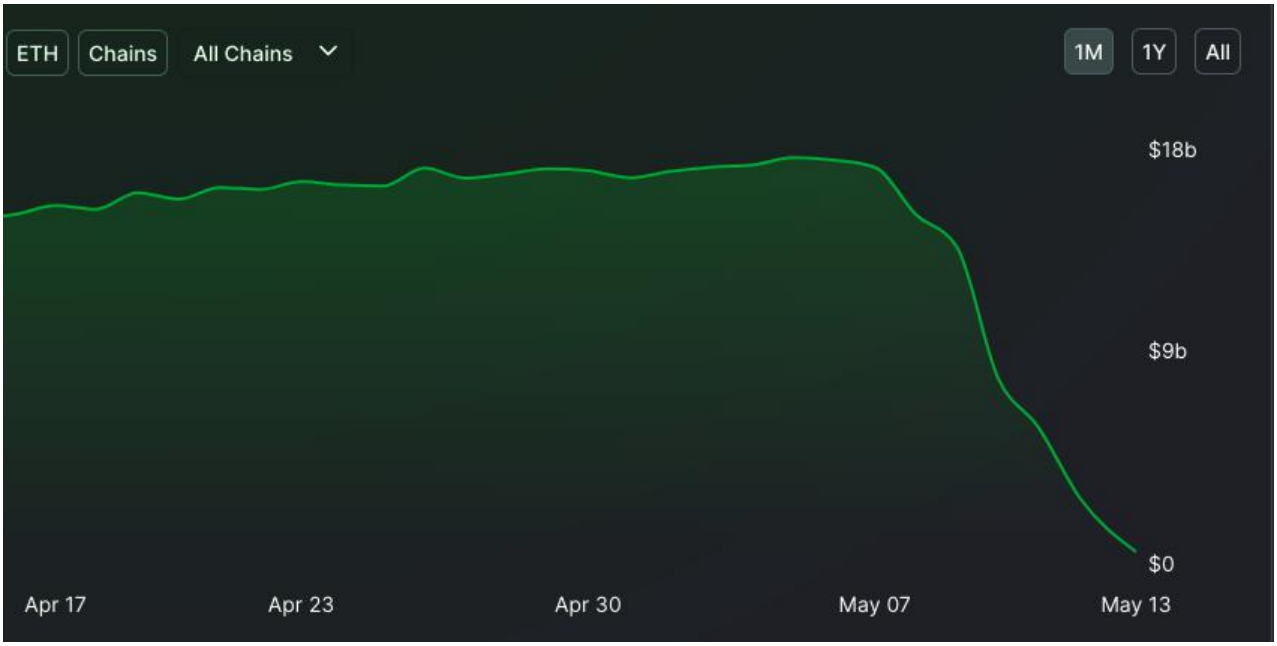
舆论风向的变化导致市场情绪的恶化，5 月 8 号开始不断有巨鲸抛售 UST，市场上 UST 抛压陡增。LFG 通过做市商 Jump Trading 在市场上抛售 ETH，回购 UST，直到该地址资金消耗殆尽。这时 LFG 已犯下了第二个致命错误：开始无策略的救市。无策略体现在两个方面，一方面单个

地址耗尽资金救市造成 LFG 在变卖家产挽回，大家都在分析 LFG 有多少家底，一算只有 7 万多个比特币（20 亿），市场上 UST 有近 180 亿，根本接不住；另一方面，没有及时拨正市场舆论风向。可能大家会问，那抛压增加要怎么办？不动声色的、不留痕迹的买回来就好了，做正向 PR，让大家知道市场正在自己解决问题。

什么人要救？生病的、有问题的人才要救。市场信心的丧失是把 UST 拖入深渊的真正元凶，而这一切是 LFG 自己造成的。

（3）卖 BTC：LFG 犯下第三个错误和第三个疑点

在 5 月 8 日的脱锚事件发生后，因信心的丧失和恐慌情绪的蔓延，锁在 Anchor 中的 180 亿 UST 开始被抛到市场上。



LFG 官方宣布动用 7 亿美元的比特币储备，用于维持 UST 稳定。市场上却有 180 亿 UST，7 比 180，市场恐惧进一步加强，大家开始“逃命”。可能 DK 也察觉到资金不够，手很欠的发了一条推文：“正在调集更多资金”，要知道 7 万多个比特币是从 3 月份开始筹备的，180 亿美元 LFG 短时根本不可能筹集到，等于在告诉大家要加速“逃命”。

但 7 亿美元的比特币抛入市场，造成比特币大盘暴跌，市场开始连环清算，Luna 也在其列，更

多的人开始抛售 UST 和 Luna，这是 LFG 犯下的第三个错误。到 5 月 10 日，LFG 认识到出售比特币的策略是失败的，市场根本接不住，开始停止救市，任市场发展。

在这一轮的 UST 抛售中，我们发现第三个疑点。一个同样是 5 月 8 日启用的新地址（0x59964a）5 月 8 日事件发生后开始反向操作，在市场上大量吸纳超过 6 亿的 UST。

Transaction Lists

Transactions | Internal Txns | Token Txns

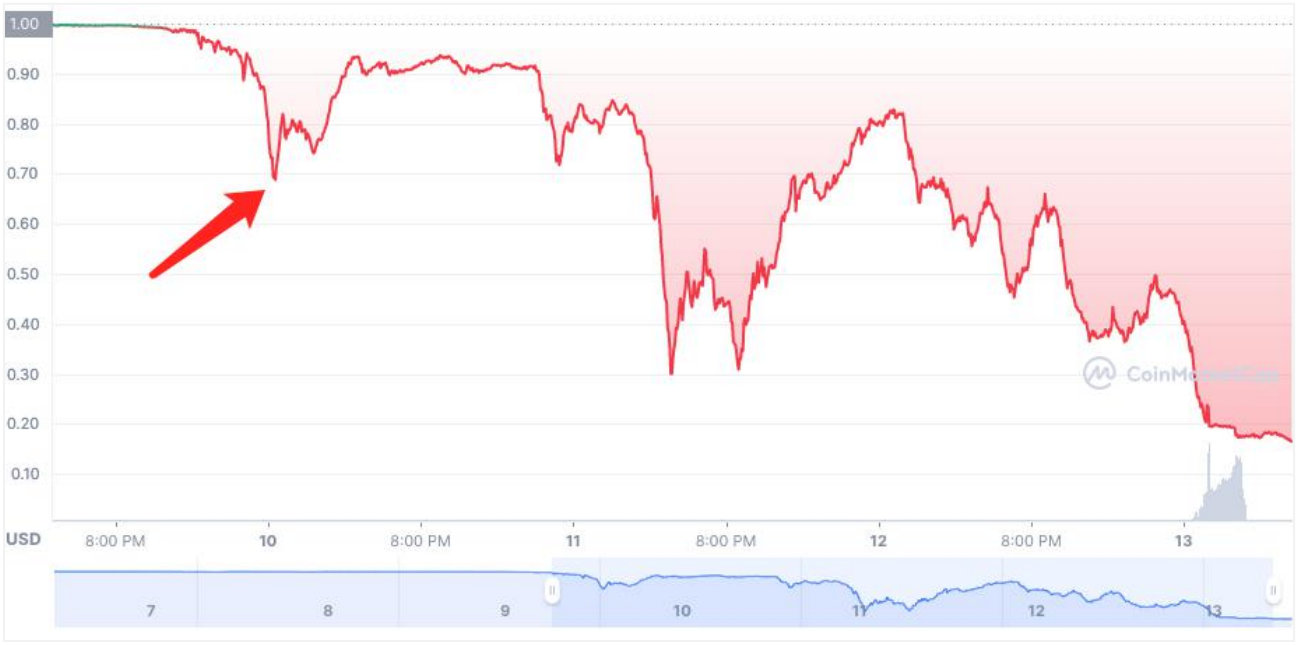
Txn Hash	Time	From		To	Value
0xa033e275525...	2022-05-08 22:22:01	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0xeedc220b18b...	2022-05-08 22:20:50	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0xf1503ea21b7...	2022-05-08 22:17:31	0x59964a...cfb7f3d2c0	OUT	Vyper_contract	0 (0.00USD)
0x3b52ac3ea9e...	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)

然后在 5 月 10 日一次性抛售了 5.88 亿个 UST，在 5 月 11 日又抛售了近 3 千万个 UST。

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)

可以说这个新地址在 5 月 10 日的抛售，使得 5 月 10 日的 UST 严重脱锚成为必然。而事实上 5 月 10 日 UST 最低点跌到 0.6，严重脱锚，而 LFG 已用了他们的大部分储备金，几乎弹尽粮绝，后面的过程和结果可想而之。



上面的三个疑点，让我们不得不怀疑这是一次蓄谋已久的索罗斯式金融攻击（如果不清楚索罗斯攻击的操作逻辑，可以去互联网上查阅，这里不做赘述），市场上也充斥着这种声音，资本是逐利的，如果是金融围猎一定有利可图，那这次事件如果是攻击，攻击者赚到钱了吗？

市场上很多声音说有机构筹集了 10w 个比特币用于此次攻击，我们就以 10w 比特币来估算此次事件如果是金融攻击，攻击者能获得多少收益。

（1）埋伏：假设攻击者的 10w 个比特币在 3 月 22 日 LFG 开始增持比特币时创建空头头寸，3 月 22 日比特币价格约为 42000 美元，相当于创建了 42 亿美元的比特币空头头寸。比特币价格一旦下跌，攻击者将获得回报。（且 3 月开始比特币已开始有下跌迹象，这也一定程度上降低了空头风险）。

（2）等待时机：随着美联储加息、俄乌战争等因素的影响，加密货币市场持续走低，攻击者的攻击时机逐步开始成熟。

（3）时机成熟：攻击者设定 LFG 为部署 4pool 从现有流动性池中筹集大量资金为时机，时刻监控 LFG 动态，当 5 月 8 日得到消息 LFG 会开始调拨资金时开始从币安中移除 8400 万美元作为攻击本金准备攻击。当天，LFG 如期移出 1.5 亿 UST 10 分钟后发动攻击。

（4）攻击策略：砸盘 UST 并影响舆论。在 5 月 8 日通过 8400 万 UST 造成短暂脱锚并影响舆论，5 月 9 日持续观测市场情绪和 UST 动态，当发现大量巨鲸开始抛售 UST 或从 Anchor 中提取 UST 时，攻击策略生效（如果没有造成市场恐慌则继续回到上面一步等待时机）。

（5）致命一击：攻击者开始动用另外 6 亿美元吸纳市场上抛出的 UST 并为致命一击做准备，5 月 10 日上午一次性抛出，将 UST 砸至 0.6 低点，严重脱锚，市场信心被击溃。

（6）拿钱走人：之后攻击者只需要等着 LFG 动用储备的 7 万多个比特币去救市，等待比特币大跌并通过 42 亿的比特币空头获利（这里暂不算攻击者是否部分资金做空了 Luna）。

本金：42 亿空头+8400 万攻击启动金+6 亿攻击准备金，近 49 亿美元（如果 6 亿美元的 UST 砸盘非攻击者行为，而是市场行为，则本金 43 亿）。

成本：根据 Curve 的手续费机制并充分考虑攻击过程中 UST 的币价波动。8400 万按照 1%计算，第一笔攻击成本 84 万；第二次 6 亿美元攻击成本以 10%计算，成本为 6000 万美元（如果 6 亿是市场行为，则这里成本是 0）.

收益：如果攻击者在 5 月 10 日比特币价格为 32000 美元时平仓离开，42 亿美元的比特币空头将获取 9.52 亿美元的收益。

总结：不到 45 亿的本金和不到 1 亿的攻击成本，获利近 10 亿美元。并且因为 UST 死亡螺旋的存在，这种攻击机会是必然会不断出现的，抓住一次就会摧毁整个生态并获利。

稳定币是去中心化金融的流动性关卡，充斥着利益和风险，稳定币战争才刚开始，远未结束：

（1）5 月 10 日、5 月 11 日、5 月 12 日，美国财政部不断发声要监管稳定币，SEC 声称会随时对 UST 项目方进行立案调查。而 UST 是韩国人 DK 的项目，让人不禁想起若干年前经济危机时期 IMF 对韩国经济的干预和影响。这一点对任何一个稳定币应该都是警醒，如何发展，如何监管，值的行业和各国金融相关部门深入思索。

（2）市场风险：随着机构不断入场，加密市场或逐步变成专业人事和资本家的游戏，高阶的

金融博弈将不断产生，高收益将不再是常态，如何警惕市场风险是每个项目和用户都必须面对和审慎思考的问题。

（3）稳定币的安全机制应该是什么：是类似 USDT、USDC 的现实资产锚定还是 DAI、UST 这种算法稳定币，算法稳定币一定不安全吗？其实也不尽然，以 UST 为例，如果 LFG 的 40 亿美元 4pool 组建完成，想要成功阻击到脱锚至少要 20 亿美元，门槛很高，无利可图的情况下还会不会有金融层面的攻击，这个只有交给时间来验证了。不管是什么类型的稳定币，经济模型的安全和链上风险监测预警都必不可少。

5.总结

2022 年第二季度，Web3 安全态势方面呈现两个典型特征：一方面不同公链的风险类型差别较大，这与不同公链差异化的业务布局和底层架构有较大关联；另一方面已形成不同的业务生态，DeFi、NFT、GameFi 等业务生态所面对的安全风险和攻击类型相互之间差别很大，这与自身业务模型和开发者生态建设有关。

DeFi 安全性仍然是 2022 年第二季度关注的焦点，大约 75.1% 的攻击发生在 DeFi 领域。但是，虽然 NFT、跨链桥、交易所安全事件没有 DeFi 事件那么频繁，但有几起事件造成了巨大的损失，而且第二季度针对 NFT 的钓鱼攻击次数明显增多，所有类型的 Web3 项目都应该加强安全性。SharkTeam 提醒项目方和生态方，在项目上架前一定要经过专业的智能合约审计并通过，上架后也要对项目运营情况做到态势感知，才能防患于未然，为用户更好的创造价值。

SharkTeam

In Math, We Trust!

https://sharkteam.org

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg