Intelligence On Chain

Investigation Addendum#1 - IOC Beanstalk

Blockchain(s)	Ethereum & BTC
Transaction Hash	Etherscan Transaction Hash
Attacker Address	0x1c5dcdd006ea78a7e4783f9e6021c32935a10fb4
Date of Exploit	17 April 2022

Introduction - Intelligence On Chain

- At the end of April 2023, Intelligence on Chain was contracted by the Beanstalk DAO to commence a preliminary investigation of its 2022 exploit.
- **This investigation remains fundamentally incomplete, in the sense of the exploiter remaining unknown.**
- In sharing our findings, other investigators may utilize the data to continue to follow the trail.
- The following represents an addendum to **the first report,** describing some findings & observations which have come to light in greater detail.
- This addendum focused on open-source intelligence uncovered since the release of the first Beanstalk Report.
- A more substantive addendum was shared with federal investigators. Significant portions have been redacted.

Defining the Scope of the Addendum Report

Following the publication of IoC's initial investigation report on 31 August 2023 for the Beanstalk exploit in April 2022, IoC held a call with the Beanstalk community in its Discord server on 9/20/23 to go over the report and answer any questions pertaining to its findings.

During the call, a Beanstalk community member posed a question in the Discord chat that was read out loud by the moderator and which is of notable mention.

As cited, the question posed was: "Has anyone done any overlaying of the Discord data - particularly from our server - with the information that you guys have put together?"[1]

In response, IoC confirmed that the Discord data was considered and it underscored the importance of building a timeline of events in any exploit's investigation.

As IoC's monitoring work extended through the end of Q1 2024, it became increasingly evident from its periodic perusal of discussions in Beanstalk's Discord server that there were several remaining community members which had lingering and unanswered questions relating to the project's operations, etc.

Thus, in approaching the two year anniversary of the Beanstalk exploit, and in light of the above mentioned observations, IoC considered it appropriate to delve deeper into the timeline of events when compiling the addendum report, particularly as it pertained to information relating to the post-exploit "Barn Raise," the "Replant," and the developments thereafter linked to Beanstalk and its associated project, Root Finance aka Root Markets aka Root Labs.

It is IoC's estimation that these findings, having been gathered upon closer scrutiny of readily accessible references in the public domain, are of importance to highlight in this addendum report for the purpose of transparency so that Beanstalk users are at least better informed of the context surrounding the protocol's development in the immediate aftermath of the exploit, and what would happen afterward.

1. A High-Level Overview of Beanstalk's Timeline of Events, Post-Exploit

Development of the Beanstalk Protocol was carried out by multiple parties who seemingly had distinct and separate roles, yet whose contributions ultimately reflected considerable overlap upon closer examination.

The aforementioned nature of the protocol's "intertwined" operations is evidenced in this Blockworks article from July 2022 (emphasis added by investigators):

> *"Beanstalk-built market protocol Root **received $9 million in seed funding** to develop a zero-fee decentralized marketplace.*
> *Announced Tuesday, the funding round was led by Road Capital, Nima Capital, Soma Capital **and Manifest Crypto...** Parth Patel, founding member of Root*

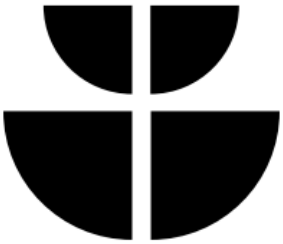
[1] The question does not appear to be available for viewing in the Discord and the community member who posed it is no longer present in the server.

> *Labs,* ***emphasized the funding round was for Root, not for Beanstalk, though the development teams are intertwined.***
> *"The opportunities to invest in Beanstalk are equitable for all," Patel told Blockworks, adding the funding round was meant "to help provide liquidity on the markets we make on top of Beanstalk."*
> *Root's fundraise comes weeks before Beanstalk's "Replanting," when the protocol will reopen after being paused since April. In the interim, Beanstalk has been running a "Barn Raise" recapitalization campaign, selling Fertilizer tokens that accrue interest based on Bean token mints.*
> ***The Barn Raise will continue until all compromised investors are repaid,*** *though only 15% of the $77 million hole has been filled so far, according to Patel.*
> ***Root said it spent a "significant portion" of its seed funding on Fertilizer,*** *and it* ***hopes to use the Bean yield to fund its treasury.****"*[2]

It would be over a year later, in **August 2023**, that the public would learn **that the Publius collaborators are behind Manifest Crypto when the Basin whitepaper is published** bearing their names and associated email addresses on page 1:

[2]Kubinec, Jack. "Team behind Hacked Beanstalk Stablecoin Raises $9M for Market Protocol." *Blockworks*, 27 July 2022

Basin: A Composable EVM-Native Decentralized Exchange Protocol



Brendan Sanderson
brendan@manifestcrypto.org

Ben Weintraub
ben@manifestcrypto.org

Brean
brean.beanstalk@protonmail.com

Silo Chad
silochad@protonmail.com

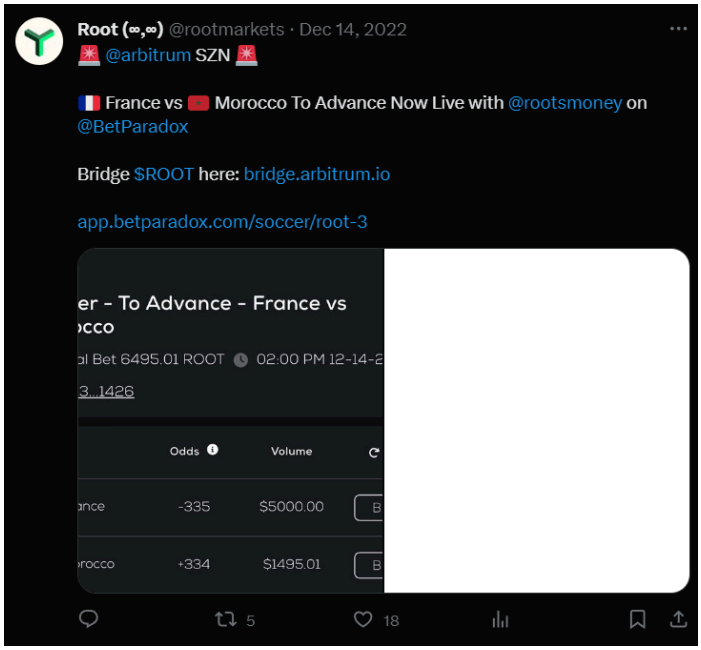
Beanstalk Farms
beanstalkfarms@protonmail.com

basin.exchange

Published: August 23, 2023
Modified: August 23, 2023
Whitepaper Version: 1.0.0
Code Version: 1.0.0[1]

(screenshot taken 1-4-2024)

Root Finance (aka Root Labs aka Root Markets) appears to have been wound down with little fanfare at the end of 2022 or early 2023, lacking any clear announcement of its deprecation. RootMarkets' final post on Twitter/X, as of the publication of this addendum, was a football-related post made in December 2022:



(screenshot taken 11-25-2023)

The Dune dashboard created for the Beanstalk Barn Raise **reinforces where the money was spent,** as was conveyed when Root Finance announced its seed raise (*"Root said it spent a "significant portion" of its seed funding on Fertilizer"*[3]:

Top Holders bean-barn-raise-top-holders

account	fertilizer
1. 0x735cab9b02fd153174763958ffb4e0a971dd7f29	8,937,419
2. 0x56a201b872b50bbdee0021ed4d1bb36359d291ed	788,138
3. 0x9a00beffa3fc064104b71f6b7ea93babdc44d9da	415,322
4. 0x7b2366996a64effe1af089fa64e9cf4361fddc6e	238,123

The 0x735 address appears to be yet another GnosisSafe wallet amongst the network of Publius and collaborator-controlled wallets, and remains highly active.

Roottoken.org appears to be still online, but its databases do not properly function, and its whitepaper purports to have been partially authored by "Publius," reinforcing the Blockworks article in which it was reported that the development teams are, in fact, intertwined:

[3] *Kubinec, Blockworks, July 2022*

Root: Fungibility for Beanstalk Silo Deposits

Kokonut, Mistermanifold, Sarrdinero and Publius
roottoken@protonmail.com
roottoken.org

Published: November 16, 2022
Modified: January 24, 2023
Whitepaper Version: 1.0.3
Code Version: 1.0.1[1]

(screenshot taken 11-14-2023)

The division between where these companies end, and where Beanstalk Farms begins, is impossible to discern. The Beanstalk community, vis-a-vis its DAO, has primarily funded Beanstalk Farms, a self-professed decentralized development organization, to work on development for the protocol.

(screenshot taken via Twitter/X)

2. Miscellaneous On-Chain Observations

The creation of the Beanstalk CoOp (by this address and located at this address) was funded by this transaction hash originating out of TornadoCash's 1ETH contract *on the very day of OFAC sanctioning,* and using the ETH to finance the coop wallet's operations.

The Beanstalk CoOp was funded with 90,000 $BEANs in December 2022 as denoted in the Bean Sprout operations report from that month:

Expenses by Date

BSM transaction history can be viewed on Safe.

Date	Amount	Reason	Transaction
12/12/2022	90,000 Beans	BSP-9 funded the Coop with 90,000 Beans for Chicken Bonds.	Etherscan
12/15/2022	10,000 Beans	Payroll for 12/1/22 through 12/15/22.	Etherscan
12/31/2022	10,000 Beans	Payroll for 12/16/22 through 12/31/22.	Etherscan
Total expenses	**110,000 Beans**		

(screenshot taken 25 March 2024).

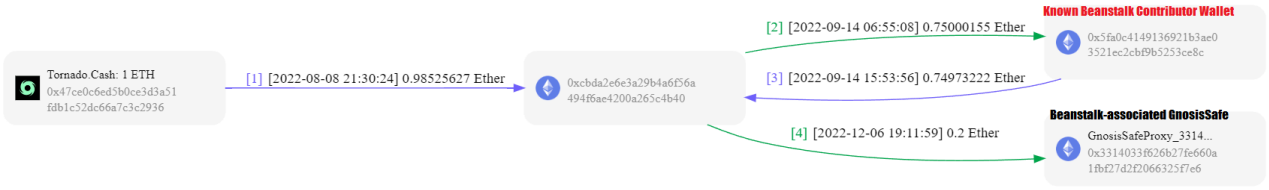
In addition, the Flash Depot contract, located at this address and created by this address, was financed by ETH originating from the same Tornado.Cash withdrawal.

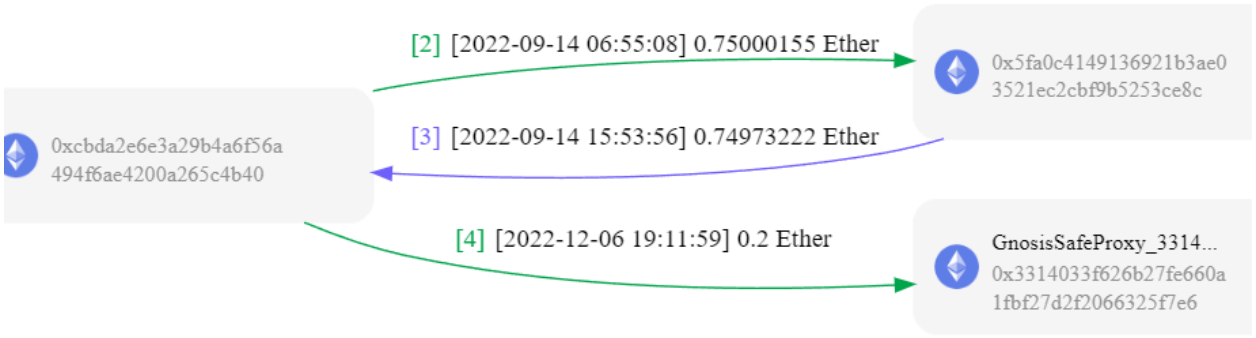
"Publius" is listed as a creator of this contract on-chain:

```
* @title FlashDepot
* @author Publius, Brean
```

This raises **significant questions** at this junction which we cannot answer, particularly:

- *What was the purpose of some of the contributors to a protocol that was exploited, and saw its exploited funds routed through Tornado.Cash, then utilizing Tornado.Cash to fund future development work after Tornado.Cash was sanctioned?*





As of 10 December 2023, the wallet known to be the Root Finance wallet within the community began to sell its $BEANs from new mints first for ETH, then trading the ETH for $PEPE meme coins.

It remains unclear how buying $PEPE will enable Root to "create markets for asset futures, non-fungible tokens (NFTs), and sports and political election betting" (see Blockworks article).

3. Concluding Remarks

A majority of findings associated with the Ethereum-Ren-Ethereum (E-R-E) extended fund pattern referenced in the initial report have been handed to law enforcement. Investigators remain confident in their original conclusions with respect to the E-R-E extended fund pattern; lacking sufficient information, their theses remain ambiguous.

The E-R-E extended fund pattern concentrated exclusively on the 100 ETH outputs originating from Tornado.Cash. However, numerous 1 ETH and 10 ETH deposits to Tornado.Cash were also made by the April 2022 Beanstalk exploiter.

The first Beanstalk Report was **explicitly *outwardly focused*** with respect to Beanstalk itself, and focused on 100ETH batches exiting the OFAC-sanctioned crypto mixer Tornado.Cash. There exist many withdrawals from the 1 ETH and 10 ETH contracts that make demixing them a far more challenging process.

This addendum represents **new context, *in addition to other findings,*** which cannot be disclosed and must be redacted from the public report because the investigation remains ***ongoing.***

Although this addendum report concludes IoC's formal monitoring work period and is the final deliverable pertaining to its investigation of the April 2022 Beanstalk exploit, this case nevertheless remains open, and IoC will continue to consider any future

developments or new information that may be applicable to leading to a definitive closure.

The broader DeFi, security, and white hat communities are encouraged to consider IoC's findings or reach out for collaborative efforts in this regard, and there remains a 40% bounty available to anyone who is somehow able to recover the stolen funds; this bounty is also available to the exploiter, should they ultimately decide to do the right thing and return the funds. Details on the bounty are available here.