Intelligence On Chain

The Beanstalk Report

Investigators: @JPOnChain, @OxSaiyanGod, @ManiacalEngineer, @0xFantasy
Writer: @WoAs_Necksus

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

1. Table of Contents

2. The Beanstalk Report – Executive Summary

This report contains a public form of the investigation & analysis prepared by Intelligence on Chain, on behalf of the Beanstalk DAO, regarding the exploit which took place on 17 April 2022.

Since the Beanstalk DAO's approval of a formal investigation on 30 April 2023, Intelligence on Chain has been rigorously investigating this most sophisticated of flashloan attacks with **the goal of finding provenance** for further investigation.

The attacker deposited all stolen funds (24,830.1169104623262323 15 ETH) immediately into TornadoCash following the exploit.

As a mixer, TornadoCash relies upon withdrawals equaling deposits. When both volume, and the same fund quantities match, there exists **significant likelihood** of this being the targeted funds.

The subsequent OFAC sanctioning of TornadoCash lowered incoming volume **substantially,** thus increasing the likelihood of targeting the correct withdrawals exiting the 100ETH contract. Our investigation **remained focused on the 100 ETH contract.**

Investigators considered >1y worth of data, and in that span, **3,212 wallets have been analyzed, equating to a total of 7,647 transactions.**

The first observation we have: **no single wallet withdraws from TornadoCash a "perfect" target amount of ETH.** A plethora of wallets **withdrawing smaller amounts** has been observed. Their subsequent behaviors illustrate a clearer portrait of the fund flow.

A second observation of importance: **the 0.03 ETH lead, which led to a never-before discussed pattern of transactions directly linked to the exploit funder wallet,** and expanded upon below.

TornadoCash's classic contracts act as **withdrawal points** for users to redeem encrypted hash keys in clean wallets for funds received through relayers. For a more technical breakdown, please visit Coincenter.org.

The most noteworthy fund movements Intelligence on Chain followed out of TornadoCash began to leave **approximately 2 weeks** after the flash loan exploit.

This document represents **the summary of the investigation, to-date,** with regard to flow of funds following the Beanstalk Exploit.

Sensitive information has been redacted from this report, including specific wallet addresses linked to the Significant ERE pattern described below, to maintain the integrity & security of ongoing investigations by law enforcement.

3. What Happened: how was the money taken?

On 17 April 2022, a sophisticated combination of flash loans and governance proposals was used to hijack the decentralized stablecoin protocol known as Beanstalk.

Using the flash loans, the attacker was able to push a malicious proposal through Beanstalk's on-chain governance processes, draining their liquidity and withdrawing the funds to TornadoCash's "classic" contracts as ETH.

The Beanstalk exploit was widely reported on by numerous media outlets covering DAO's and the cryptocurrency ecosystem, including the *New York Times.* Participants in the project suffered losses measurable in tens of millions.

As of this publication, **the culprit remains at-large.**

4. Technical details of the exploit

Phalcon's breakdown of the fund flow is located here.

Certik's breakdown comes additionally recommended.

Overall, the attacker managed to send a sum total of **24,849.1 ETH** into TornadoCash contracts. Of this amount, the **100 ETH contract received 24,700 ETH.**

Our investigation **remained focused on the 100 ETH contract.**

5. Following the funds, post-TornadoCash

From April 2022 to April 2023, **727,600 ETH** was withdrawn from the 100 ETH TornadoCash contract.

Some noteworthy points of data on TornadoCash withdrawals from the 100 ETH contract during this period include:

- **~368,300 ETH** was withdrawn to wallets **in batches of over 500 ETH**
- **~141,000 ETH** was withdrawn to wallets **in batches of between 200 ETH and 400 ETH**
- **~218,300 ETH** was withdrawn to wallets **in batches of 100 ETH**

Due to the sheer volume of funds exiting TornadoCash, it is possible that some funds are from other exploits, and not originating from Beanstalk.

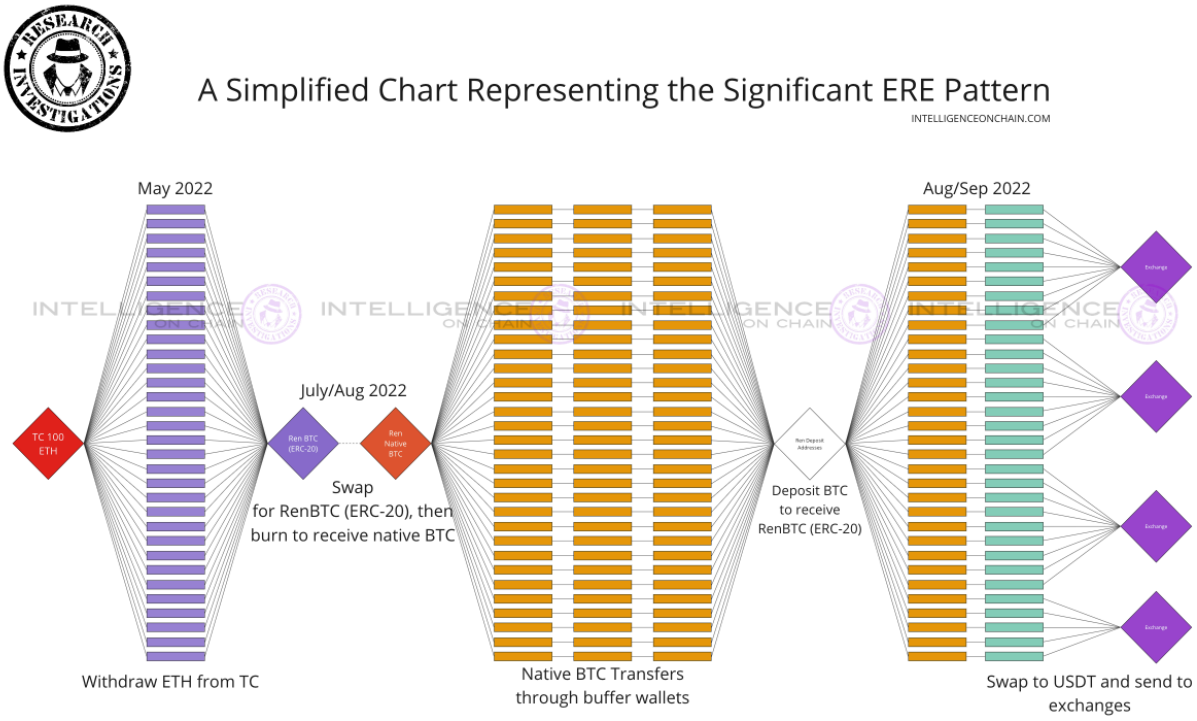
Over the past year, 164,800 ETH, in total, would enter RenBTC from TornadoCash's 100ETH contract. The funds Intelligence On Chain sought **represented a mere 15% of the volume** of this particular movement. This volume entering the RenBTC Protocol makes it **the largest singular recipient of TornadoCash withdrawals** by leaps and bounds within the studied timeframe.

No large quantity of TornadoCash withdrawals added perfectly up to 24,700 ETH. However, certain clues and patterns did emerge.

Intelligence on Chain has managed to locate a **24,400 ETH withdrawal pattern[1].** Whether that pattern represents the stolen Beanstalk funds **remains indeterminate.**

The Significant ERE withdrawal pattern from TornadoCash began **3 May 2022 and continued through 13 May 2022.**

The funds follow the path below:



[1] Referred to as the Significant ERE withdrawal pattern. See also Appendix A.

Although TornadoCash is perceived to be **THE PRIMO OPTION** for anonymizing ETH transactions, due to **the OFAC sanctions alongside the focus of investigators** on the 100 ETH contract, the volume leaving TornadoCash was lower.[2]

Other leads have surfaced, but **the sheer volume of ETH leaving TornadoCash** gifted investigators with a clear pattern leading to a key pillar in the money laundering effort: **The RenBTC Protocol.**

6. The Primary Pattern – How the Money Moves

The exploiters' ETH is first deposited in batches into classic TornadoCash contracts.

From the 100ETH TornadoCash contract, the ETH assets (minus relayers' fees) are sent to fresh wallets and converted into RenBTC, which is then subsequently burned at the Ren Protocol to be redeemed for native BTC.

For a majority of the funds, the launderers[3] ***bridged the native BTC*** **back to ERC-20 RenBTC.** This overall trend of **ETH > RenBTC > BTC > RenBTC > ETH** is repeated across numerous wallets **(sufficient to demonstrate the Significant ERE pattern)**.

After leaving TornadoCash, the funds **suspected** to belong to the exploiter likely proceeded along the Significant ERE pattern.

This took on the following sequence:

- ETH is withdrawn from TornadoCash in early May 2022
- ETH is traded for RenBTC in late July & early August 2022
- RenBTC is burned for native BTC, in batches throughout August 2022
- BTC follows **a complex series of moves** before bridging back to ETH through RenBTC, once again, throughout August and early September 2022

Upon returning to the ETH blockchain, a large amount of the funds were converted to USDT and sent to centralized exchanges, **presumably** for sale.

Beyond this point, Intelligence On Chain **cannot definitively prove beyond a reasonable doubt** what occurred with the funds upon receipt at centralized exchanges.

[2] Where other investigators have identified withdrawal wallets relating to exploits such as Harmony and Nomad, we have successfully ruled them out (with respect to Beanstalk).
[3] We refer to them as "launderers" here, rather than "exploiters," as we have not conclusively proven the funds' provenance, and remain open to the possibility that the launderers and exploiters are separate individuals or groups; however, we believe the amount and pattern remains of significant interest.

Regardless of the provenance of the funds, **the pattern** of the funds **makes it abundantly clear** that this remains a **comprehensive money-laundering effort across no less than two blockchain protocols,** and that the operators of this fund-flow network **represent a significant illicit presence emanating from TornadoCash.**

It remains probable that the Beanstalk funds left TornadoCash **in the immediate 30 days following the exploit on 17 April 2022. It would later proceed along the RenBTC trajectory in the subsequent months,** with each batch moving in shifts over a period of hours (due to the 1h settlement time of native BTC).

7. Speculative Suspect Details - The Exploiter & the Nature of the Funds

This section is *entirely speculative, and hypothesized.*

The Beanstalk exploiter has an excellent understanding of smart contract design[4], and intimate knowledge of the design and implementation of the Beanstalk DAO structure.[5] They were mindful of the developments leading up to that moment, and aware of the environment afterward, both locally within the Beanstalk community and globally within the market, as the fund-flows post-TornadoCash suggest a necessary market awareness of the ETH-BTC exchange rate.[6]

Having stolen the funds and deposited them into TornadoCash, the exploiter needed **only to wait** to make the trail harder to follow. However, as Appendix C illustrates, the 30% market drawdown in ETH-BTC exchange rate would have cost the attacker a massive amount to make that trade at the time of TornadoCash withdrawal, in service of their money laundering.

The market volatility **forces the launderer's hand.** They withdraw from TornadoCash, but even having taken custody of the funds, they could not commence the next phase of laundering until such time as the market exchange for ETH-BTC comes closer to the market exchange at the time of the exploit.

[4] See Coinmonks, "The Beanstalk Exploit: A Simplified Post-Mortem Analysis": "The attacker was able to identify and exploit flaws in the governance design."
[5] See infinitesn4ke.eth, "Governance Hacking: Swallowing Your Own Poison Pill": "While the governance structure of Beanstalk was relatively simple, these BIPs could be very complex. The BIPs follow the EIP-2535 standard which uses a diamond analogy to describe a methodology for modifying smart contracts over time after initial deployment. That summary is a gross oversimplification as EIP-2535 is, by no means, simple. The attack is very complex - and yet elegant - from an understanding of both EIP-2535 and Beanstalk's governance model."
[6] See Appendix C - ETH-BTC exchange rate on TradingView.

That exchange rate would be reestablished in July and early August, and also would have corresponded with Beanstalk's anticipated protocol relaunch scheduled for 6 August 2022.[7]

Upon withdrawing, the launderer would have needed to sit in *either ETH, or BTC*.

As BTC was their primary laundering node, the chain data suggests that the launderer waited for the prices to correspond to their desired exchange rate, and that a majority of these funds were sold for USDT and cashed out via centralized exchanges.

With respect to the Significant ERE pattern, which represents 24,400 ETH leaving TornadoCash from 3 May to 13 May 2022... the question remains: **why circulate the funds in this manner?**

8. The 0.03 ETH Lead

During the aftermath from the exploit, Certik flagged this wallet (0x71a7) on Arbiscan, noting it as having been involved in maneuvering the 101 ETH from TornadoCash into position.

However, this **funder wallet** sent ~0.03 ETH to another wallet on Ethereum Mainnet, which Intelligence on Chain refers to as the **Beanstalk receiver.**

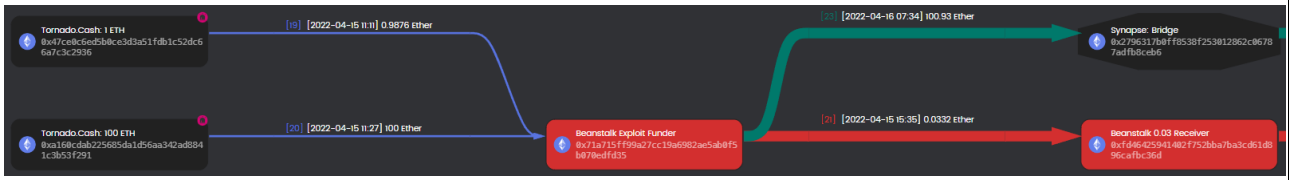
The Beanstalk receiver wallet sent the ~0.03 ETH within five minutes of having received it to a third wallet Intelligence On Chain refers to as **"0x55d6."**

Millions of dollars in USDT and ETH have passed through 0x55d6, and **the specific ETH received by a send action initiated by the exploit funder ended up at Kraken.** Intelligence On Chain is releasing this wallet with the expectation that white hats and other investigators may find it helpful in looking for connections.

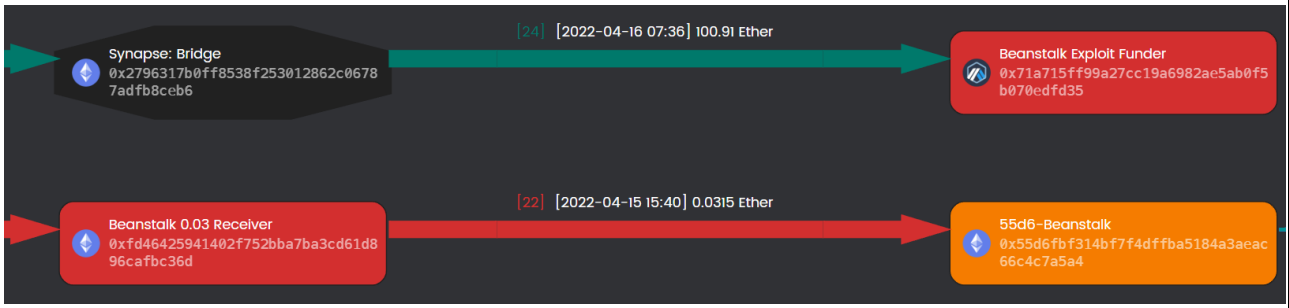
A Bitquery analysis shows the fund flow for the 0.03 ETH originating from the Beanstalk exploiter, traveling through the receiver, arriving at 0x55d6, then finally to Kraken:

Precisely **why** the exploit funder wallet sent the 0.03 ETH is not clear. Intelligence On Chain believes that this may have been **a mistake, possibly a crucial one.**

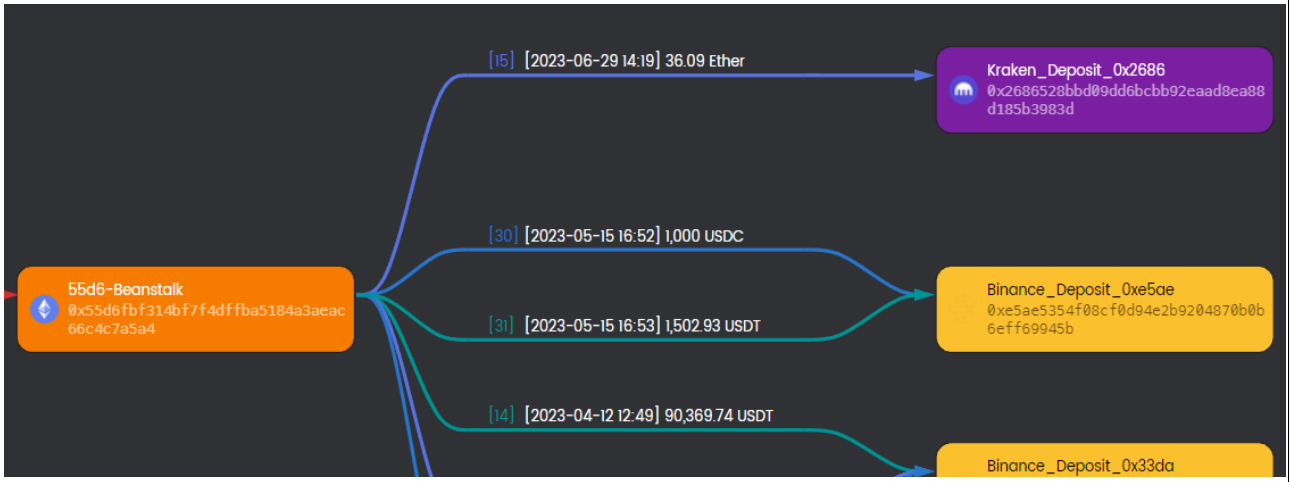
[7] See Decrypt, "Beanstalk Celebrates Anniversary with 'Safe Replant and Unpause'"



The exploit funder wallet can be observed, above, sending this 0.03 ETH. The receiver then sends the ETH to 0x55d6. The receiver wallet ceased all activity after the 0.03 ETH was withdrawn, though it also had a multi-year history. Our suspect's funds are in red; the original attack is in green, and is shown for reference:[8]



0x55d6 is an active wallet with a multi-year history. Our specific 0.03ETH target sum most likely arrived **at Kraken-created 0x2686.** Other sums may be observed, as well:



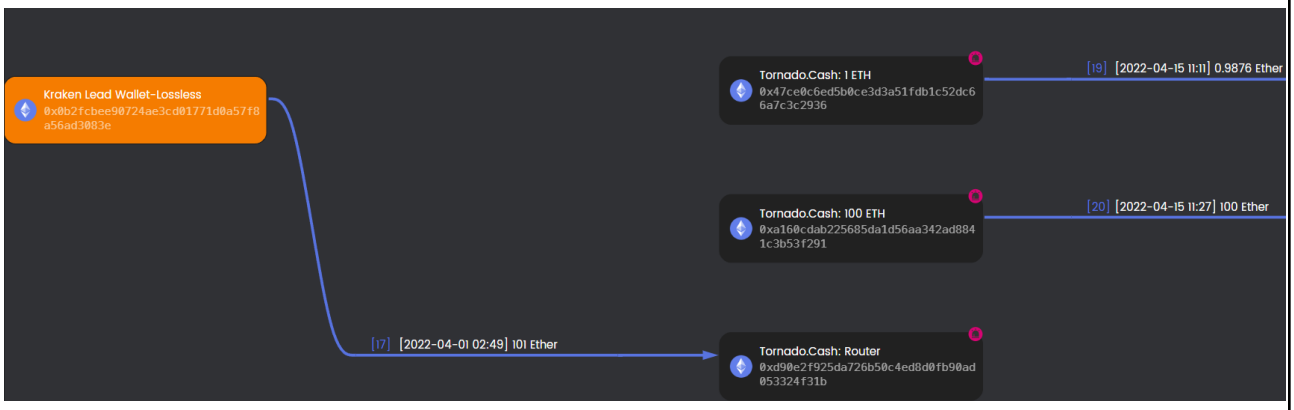
[8] This Metasleuth chart has been made available to the public for 1 year.

Two key similarities exist between the behavior of the 0.03 ETH wallets and some behaviors identified as part of a RenBTC money laundering effort:

- a coordinated movement of small amounts of ETH (~0.03) as needed to facilitate fund flows
- a roughly 2-week gap between the deposit of funds into TornadoCash and the withdrawal of funds from TornadoCash is presumed, similarly occurring both before the exploit (see below) and during the Significant ERE laundering effort

Assuming that the money launderers utilizing the Significant ERE pattern are the same as the exploiter, then the behavior is **very similar** in that the individual is accustomed to regularly transferring amounts nearing 0.03 ETH in size.

Additionally, the 2-week time gap between activities regarding TornadoCash occurs both in the lead-up to the Beanstalk exploit (**presuming further** that the Lossless-flagged Kraken Lead wallet[9] is valid), and after the withdrawal of ETH from TornadoCash, post-Beanstalk exploit (and according to the Significant ERE pattern).

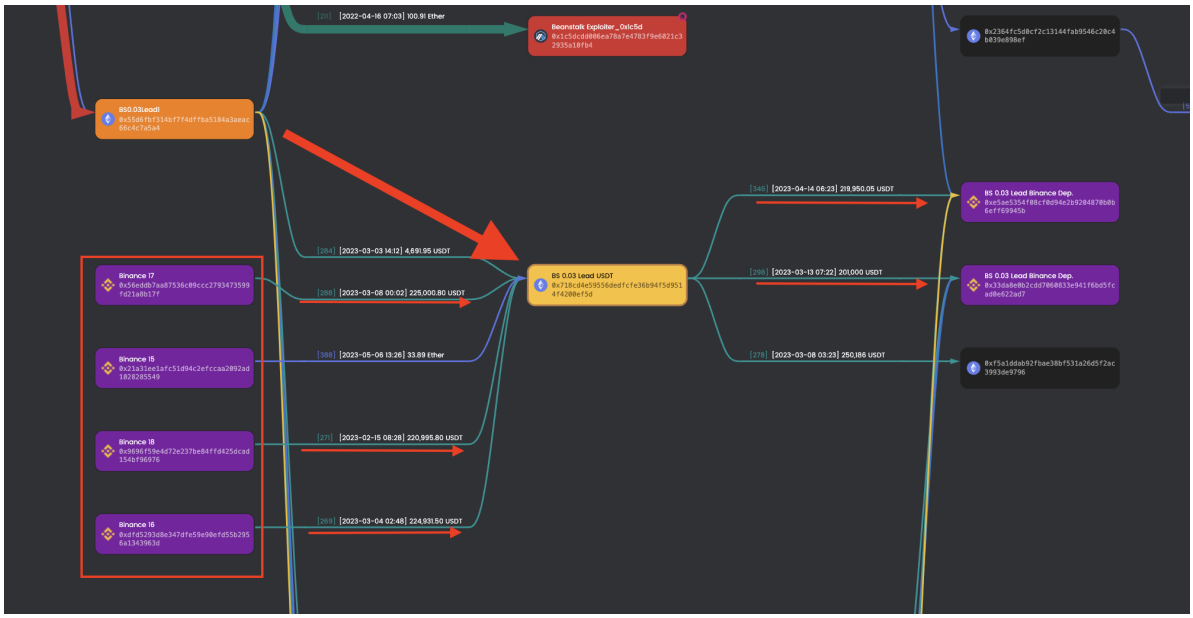


While many aspects of this trail of funds **may seem presumptuous,** the one certainty is **the 0.03 ETH transfer from the exploit funder arriving surreptitiously in 0x55d6, and inevitably making its way to Kraken.**

[9] See Appendix B - The Kraken Lead.

Worth noting: 0x55d6 sends funds to a subsequent wallet (0x718cd) which in turn receives **significant amounts of USDT from Binance and proceeds to send these funds back to a Binance Deposit wallet.**

This behaviour, the type of cryptocurrency and the amounts are **somewhat similar to the Significant ERE pattern, once the BTC is bridged back to Ethereum and converted to USDT:**



9. Recommendations: What did law enforcement receive?

Comprehensive MetaSleuth analyses in which investigators have followed each TornadoCash withdrawal to RenBTC redemption, along with detailed fund-flow analyses, have been provided to law enforcement.

Intelligence On Chain recommended law enforcement **exercise subpoena powers** in obtaining customer information related to those specified & flagged deposit addresses.

Key wallets have already been targeted for alert & monitoring. Any insights gained will be of importance for tracking and tracing future developments in the movement of stolen funds, and shared with law enforcement and the public, **where applicable**.

10. Conclusions & Future Monitoring

Regrettably, the Intelligence On Chain team **did not explicitly uncover the specific culprit.** However, the **trail of monies** that investigators unveiled speaks to the gravity of the illicit fund network.

Law enforcement agencies, investigators, and anyone interested in the more thorough version of the report **may appeal to the Federal Bureau of Investigation** for information derived from this report, where applicable. However, it should be noted that it is standard policy **not to comment on an open investigation.**

Wallets tied to this illicit network of financial activity have been thoroughly documented and compiled, having already been provided to law enforcement.

Intelligence On Chain recommends **a minimum of six months worth of monitoring** to commence following the publication of this public form of the Beanstalk Report.

11. Contact Details

Were you, someone you know, or a project or DAO you know was the victim of a flash loan exploit attack, cryptocurrency-oriented fraud, or similar-such events?
Do you have details on a massive theft of digital assets?
Do you believe you have more information to add to the context of the Beanstalk Report?

DO NOT HESITATE to contact Intelligence On Chain.

*The blockchain is **FOREVER. No ledger erasure is POSSIBLE.***

*The evidence remains, and **theft (from petty to grand) is illegal in every local, city, and state jurisdiction on this planet.***

Visit us at the Intelligence On Chain Discord server, and intelligenceonchain.com

12. Appendices & Speculative Notes

Appendix A - Validated Transactions for the Significant ERE pattern
[redacted]

Appendix B - The Kraken Lead
Intelligence On Chain presented to the Beanstalk community on 30 March 2023 regarding the value proposition of an investigation.

During that call, Publius (the founders of Beanstalk) disclosed that another analytics firm (Lossless) had flagged a wallet of interest to the exploit on 25 April, 2022, and shared this information with them, and members of the Beanstalk Farms team.

This information **was not previously disclosed** to the community-at-large until the Intelligence On Chain presentation.[10]

Afterward, the Beanstalk Farms team shared the message they received from Lossless on 25 April, noted below [sic]:

Quick heads-up; I deciphered all the TORN deposits over the last 1.5 month. There is one address that deposited exactly the 101 ETH amount into TORN which have been withdrawn later by the attacker: [[located here]]. This address got funded via Kraken. Ofc I'm using here the assumption that the attacker used the same EOA for the initial TORN deposit. I don't have connection to Kraken, but this is definitely a trace that should be looked at if possible we have a connection to Kraken.

Subpoenas executed toward the goal of obtaining this customer information **may yield some information** toward identifying the source of the exploiter wallet's funding. Unless proven otherwise, **the Kraken lead may be a sheer coincidence.**

[10] A YouTube recording of this call is available.

Appendix C - Exchange Price Charts & Explaining Fund Movements

ETH-BTC exchange, 1d, BINANCE (captured 20 August 2023)
The exchange rate from Ethereum to Bitcoin at the time of the exploit.

The red arrow is the point at which the exploit occurred on 17 April 2022, and stolen funds entered TornadoCash.

The orange arrow is the point, approximately 2 weeks after the hack starting on 3 May 2022, when Intelligence On Chain suspects the exploited funds began to exit TornadoCash via the Significant ERE pattern.

The green arrow is the point at which Intelligence On Chain suspects that the launderers began to convert the ETH into BTC starting in late July 2022, **possibly even at a profit in BTC** compared to the time of theft.

BTC - USDT exchange, 1d, BINANCE (captured 28 August 2023)

In the weeks following the Beanstalk attack, **the exchange rate of the stolen funds into BTC from ETH suffered a 30% drawdown in market exchange price,** likely pushing the launderer to withdraw the funds from TornadoCash in early May 2022.

Because the **ETH-BTC trading pair** was a **key node** in the money-laundering operation, the market turbulence caused by the Celsius and TerraLuna collapses (occurring coincidentally around the same time) may have forced their hand.

They could have waited comfortably in TornadoCash, sitting on their ETH deposits, as long as they felt comfortable (the platform would not be sanctioned formally by OFAC until 8 August 2022), and the longer they waited to withdraw, the less likely it would be to tie their funds back to the origin. The question remains as to **why they felt the need** to **begin withdrawing within weeks,** rather than months.

It could be a part of their 2 week waiting time pattern, or it could have simply been the chaos of volatile exchange rates occurring at that time.

It remains a testable hypothesis to suggest that the market turbulence in May 2022 led the launderers to **expedite their laundering process** and rush into some elements of their plan.

It is presumed the Beanstalk exploiters likely withdrew their ETH from TornadoCash in the early part of May 2022, but the laundering network **did not convert to RenBTC until July/August 2022,** presumably waiting for the market conditions on the ETH-BTC trading pair to swing in their favor.

At the time of the suspected laundering, although the USD value of both BTC and ETH was far lower than at the time of the exploit, the significance of the ETH -> BTC trade for the money laundering network remains an object of note.

The **tedious nature of conducting these transactions,** combined with a downwardly volatile market, may have led the launderers to inadvertently reveal connections they otherwise would not have revealed, **had they waited more patiently** to withdraw from TornadoCash.

Their wait would have led them to the **OFAC sanction event on 8 August 2022,** directly, and that event in and of itself spurred its own **flurry of exits from TornadoCash contracts.**

Coincidentally, that final flurry of fund bridging suspected to belong to this laundering network occurred **the same day as the sanctions announcement.**

13. Other Patterns

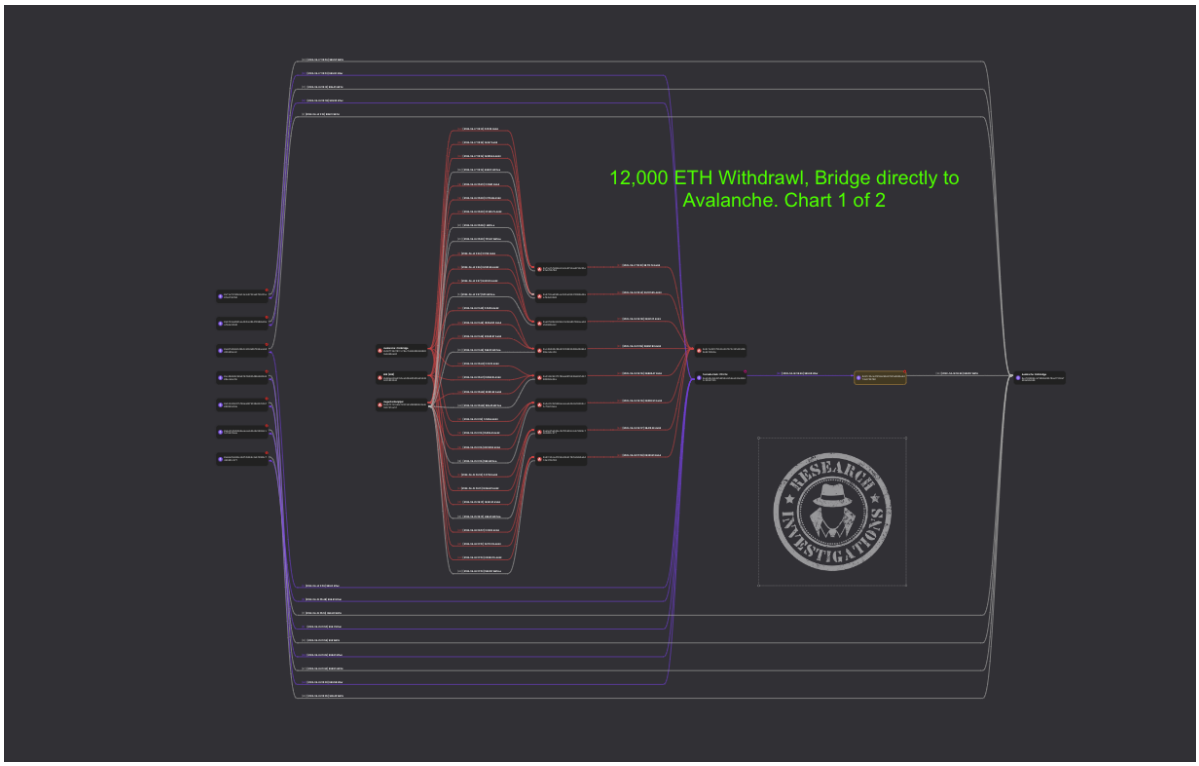
Our work has consisted of reviewing each of the wallets used to withdraw ETH from the 100ETH Tornado Cash contract.

There are notable patterns throughout the year from April 2022 to April 2023 which, based on our experience, **appear to be somewhat illicit,** given the amount of obfuscation thereafter.

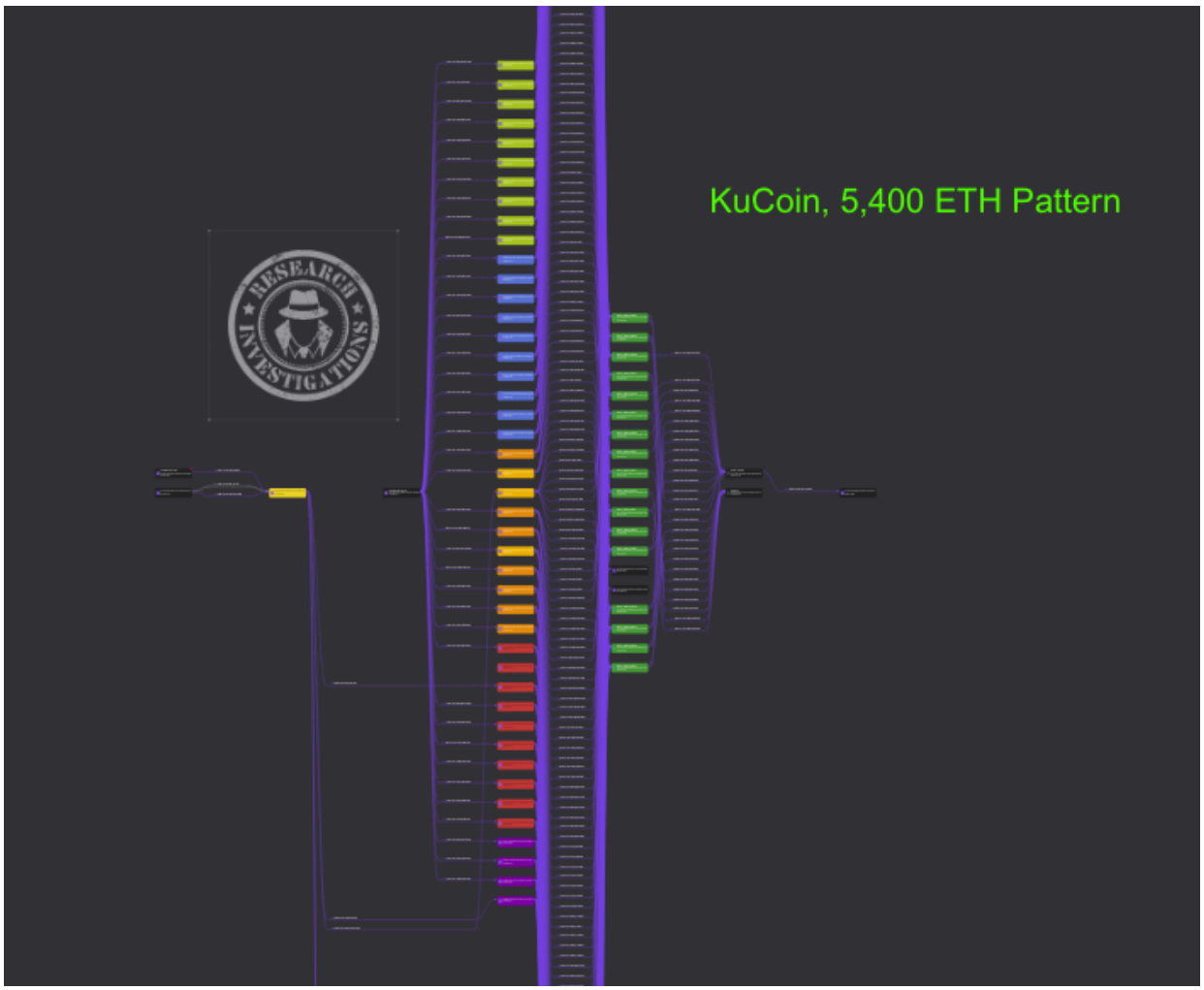
If you think any of these can be attributed to a particular exploit, **please get in touch!**

NOTE: The charts below represent only a small number of patterns.

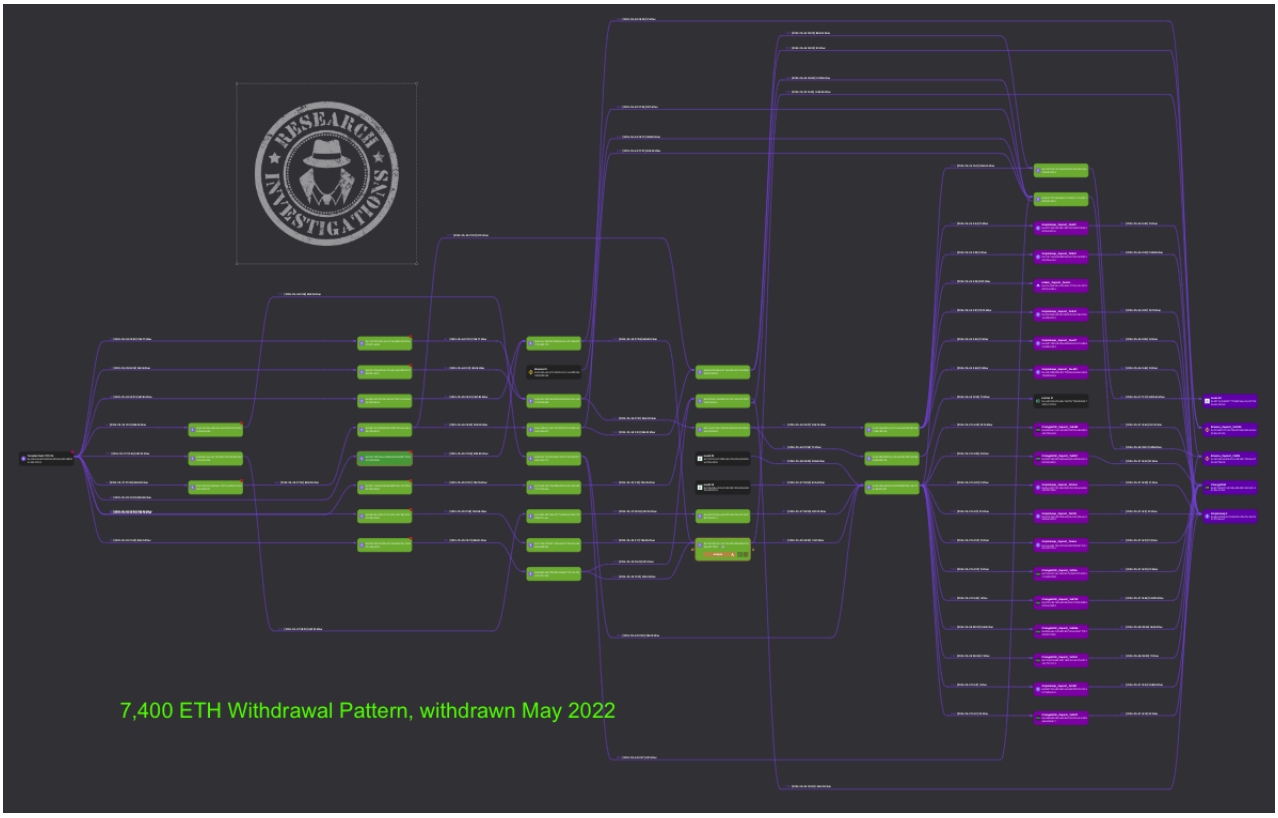
- **12,000 ETH, bridged directly to Avalanche and held in wallets**
    - This pattern is actually spread over two different charts. The chart below represents 72% of this pattern's funds; the secondary chart shows the exact same pattern.
    - Part of this pattern predates the Beanstalk exploit.
    - This pattern is highly specific, and unlikely to be related to Beanstalk.



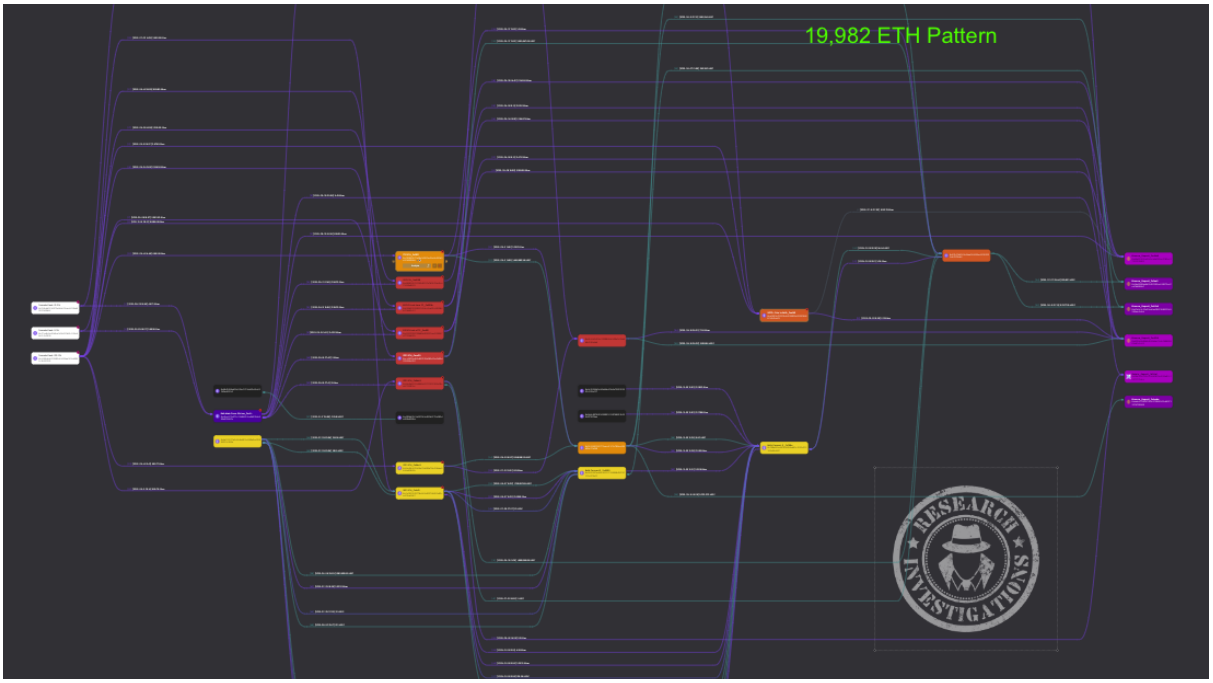
- **Withdrawal of 5,400 ETH out to KuCoin**
    - Most of the wallets in this pattern withdraw 100 ETH each and subsequently all end up in KuCoin.
    - It starts off with one withdrawal of 100 ETH split into several deposits. Each deposit address is linked to other ETH withdrawals from TC and this monster pattern continues to grow



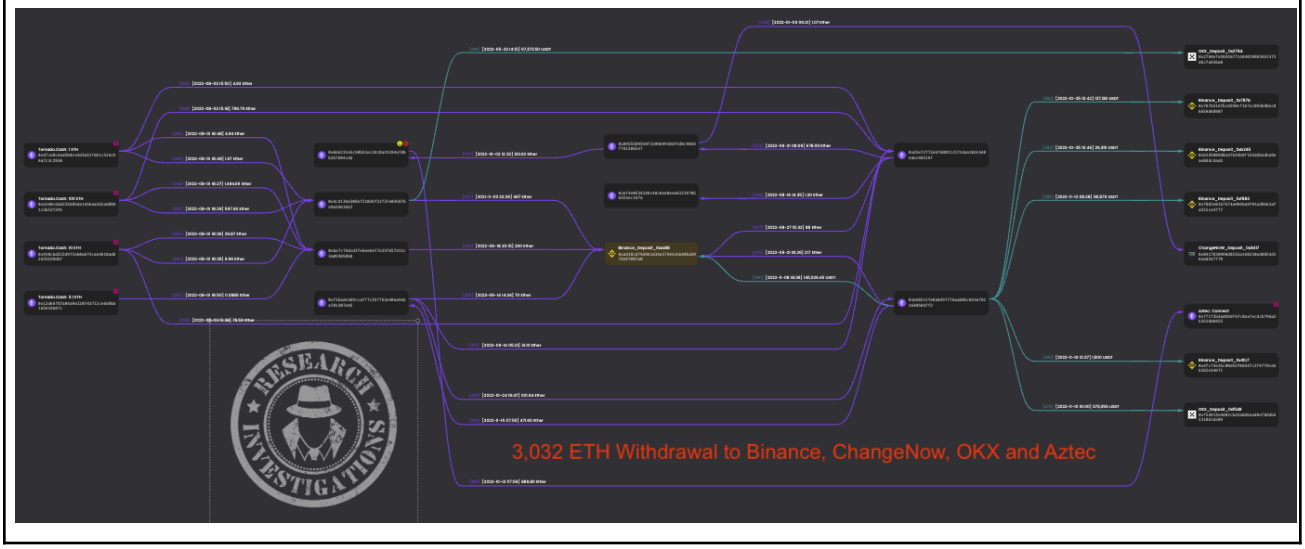
- **7,400 ETH Withdrawal, heading out to SimpleSwap, Kraken, Binance, KuCoin, Huobi and ChangeNow**
    - This pattern uses a lot of buffer wallets to try to obfuscate further, but their transactions merge into the same wallets at multiple points throughout this pattern.



- **The 19,982 ETH Pattern to Binance and Gate.io**
  - This pattern is actually spread over a couple of years and seems to be a common path.
  - There are three main trails which are all interlinked with one another totalling this massive amount of ETH. ~10,000 ETH pre-dates Beanstalk and therefore **we ruled this one out.**



- **3,032 ETH withdrawn and sent to Binance, ChangeNow, OKX and Aztec.**
  - This withdrawal pattern uses the 100 ETH, 10, 1 & 0.1 ETH TC contracts.
  - These funds were withdrawn from TornadoCash in August 2022.



- **3,016 ETH to Binance and FTX.**
  - This pattern occurred between May and August of 2022.
  - This chart shows the obfuscation used to try to hide the origins of these funds.