Terrific Finance - Post-incident review

- Batasm team, 30 Apr 2022 -

On **26 Apr 2022**, the Batasm team was approached by 2 team members from Terrific Finance with a partnership proposal between both projects. Terrific team's lead dev and community manager posted this on Batasm Finance's discord, It was responded to by one of our team members shortly after. While an approach like this would always seem questionable, the Terrific Finance team was partly represented by a trusted person from the crypto space and community, which made this seem credible.

The proposal was for both teams to collaborate and initially to cross-promote the launch of Terrific on **28 Apr 2022 10PM UTC**. Since their project was a fork of Fantasm but being on the Avax chain, both teams agreed that it wouldn't be in competition with each other. The main pitch for this fork was a new lottery mechanism which would burn and reduce the supply of the protocols' native emission token. The Batasm team concluded that it could be a good opportunity to share, learn and connect with another team in the same space.

The Batasm team proceeded to consult our investors next. It was agreed that while this collaboration could be mutually beneficial, it would be in our best interest to do as much due diligence before we proceed with next steps.

Here's what the Batasm team did as part of the review/due diligence:

- Reviewed the forked contracts; contracts were of FSM v2 and had no changes.
- Identified that there was a new contract for the new lottery mechanism.
- Identified that front end was not available, due to the site not being deployed yet.
- Checked if Rugdoc review was filed or requested, and found that the lead dev has just requested it a few hours earlier.
- Found launch entry on ApeOClock.
- Confirmed the Terrific's lead dev's comment that they had already approached FSM team about this new fork; we found a message posted on FSM's partnership-request channel on discord.
- Reviewed their social presence on twitter and discord, they had a sizable number of followers.

All the findings above presented no major red flags to the Batasm team, and no indication to stop moving ahead.

On launch day morning, the Batasm team member was asked by the Terrific's lead dev if the agreed cross-project postings were still going ahead. By then, their dApp has been deployed 2 hours before, it was live and running, however without any emissions. The Batasm team jumped onto Terrific's discord and it was a lively chatter with the Terrific team actively engaging with the community.

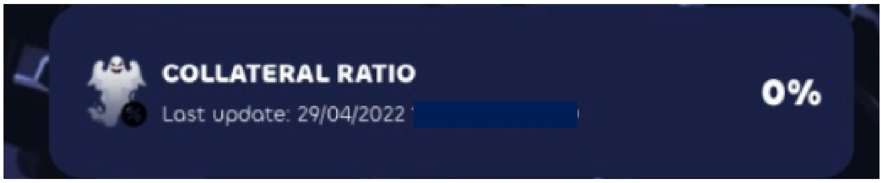
Nothing unusual was suspected at this point in time.

The Terrific Finance emissions eventually went live at **28 Apr 2022 10PM UTC**.

The Batasm team had been actively monitoring the dApp, Dexscreener charts, discord chats and on-chain transactions just in case things went south.

At around **29 Apr 2AM UTC**, Terrific's discord lively chatter appeared to have died down.The #general channel had a 5 min slowmode activated (might've had a reason for this which we are unsure of). At the same time, there was no active mod on discord and Terrific team members seemed unusually quiet at this point.

It was then when someone on their discord mentioned that the Collateral Ratio was showing 0% on the dApp. This was probably the last response from the Terrific lead dev, whom stated it was a UI issue and it was being fixed right then.

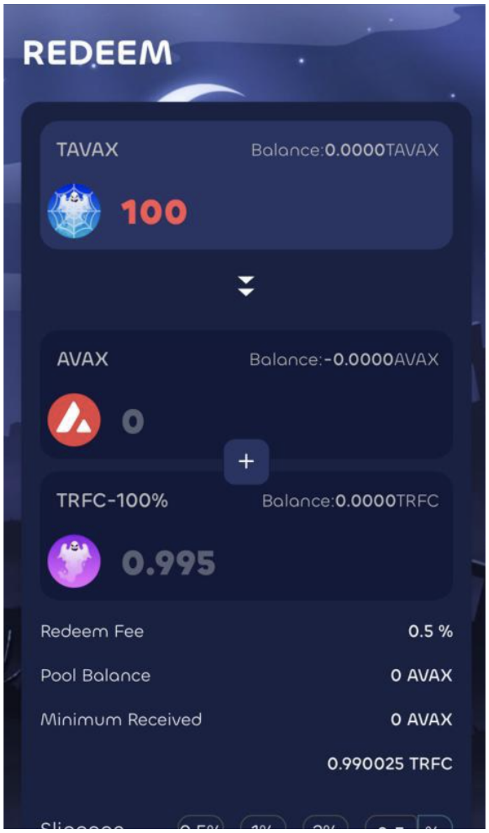


COLLATERAL RATIO

Last update: 29/04/2022 [redacted]

0%

Between **29 Apr 2022 3AM - 4AM UTC**, the Batasm team started noticing strange numbers showing on the Terrific dApp. Team was unable to tell if it was a UI issue or something worse, as the protocol is reporting a TVL of approx. $2.6M on the dashboard at this time.



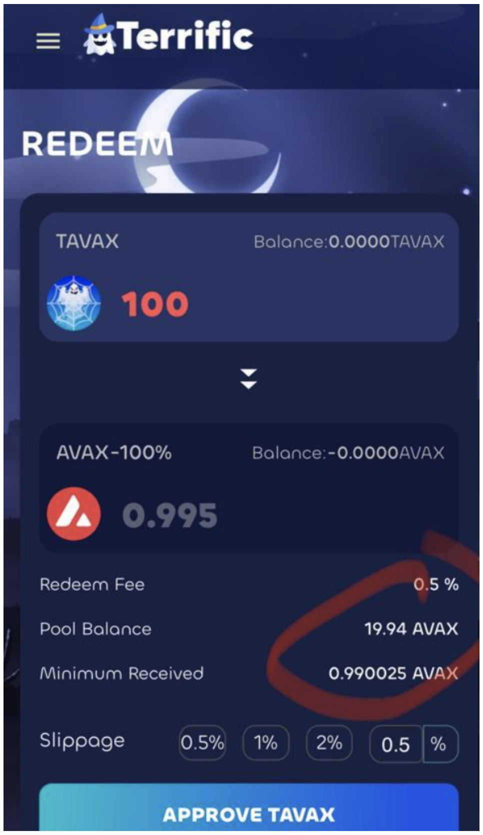
REDEEM

TAVAX Balance:0.0000TAVAX
100

AVAX Balance:-0.0000AVAX
0

TRFC-100% Balance:0.0000TRFC
0.995

Redeem Fee 0.5 %
Pool Balance 0 AVAX
Minimum Received 0 AVAX
0.990025 TRFC



REDEEM

TAVAX Balance:0.0000TAVAX
100

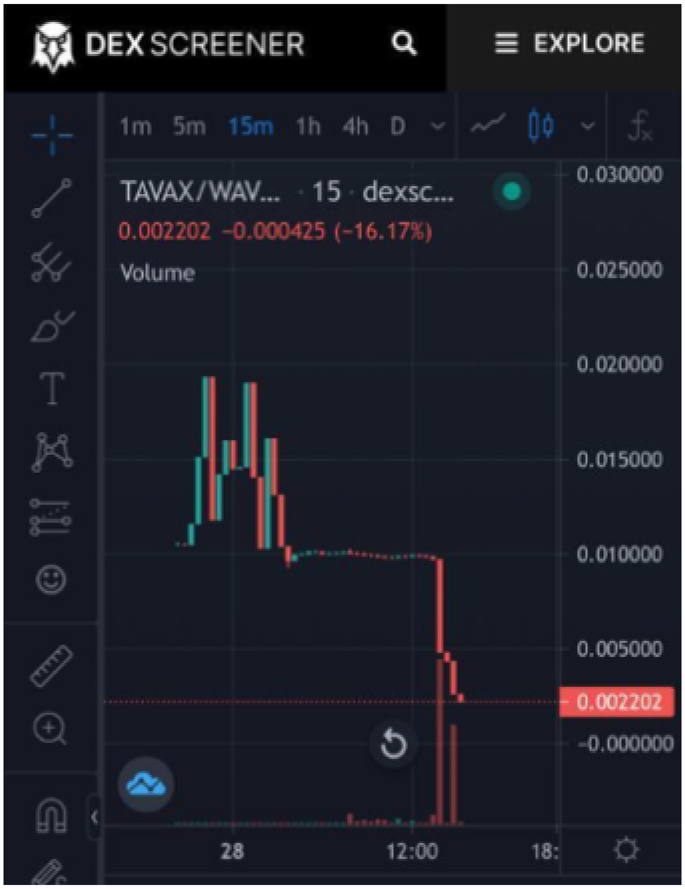
AVAX-100% Balance:-0.0000AVAX
0.995

Redeem Fee 0.5 %
Pool Balance 19.94 AVAX
Minimum Received 0.990025 AVAX

Slippage 0.5% 1% 2% 0.5 %

At this point, the Batasm team noticed that there were calls to the contract invoking reduceExcessCollateral() function (transfer accumulated fee to treasury) and requestFund() from Terrific's treasury wallet to it's dev wallet.
https://snowtrace.io/address/0x125b6276bdc31af709a6d1809db17f828bbb481b

At the same time, TAVAX price was indicating a sharp drop on the charts, indicative of an exploit or potentially someone draining the pool.



After seeing multiple similar transactions occurring between the Terrific treasury wallet to dev wallet, the Batasm Team was fairly confident that a malicious event has taken place. Within minutes, some of the Batasm community members had mentioned that Terrific's discord, Telegram, Twitter and dApp were shutting down or being removed.

Terrific's lead dev still appeared to be online but isn't responding and eventually went offline.

Assumptions based on interactions with the Terrific Team:

1. The Terrific lead dev is familiar with FSM and its related fork scene, and were very familiar with the steps and processes needed to launch a project.
2. The Terrific dev social engineered his way into teams to gain their trust, leveraging the credibility of other teams and members within the same space for ill intent.

Approximately 9000 AVAX was drained from the pool.
3543 AVAX: https://snowtrace.io/address/0x17e10121ca5116a270ccc6161811e40bf3d853bb
5000 AVAX: https://snowtrace.io/address/0x09ccbcd71a14997c6be26d9ff3b8be0e16747e56

Wallet Initialisation for the Terrific Finance contract funded by Tornado Cash
https://snowtrace.io/tx/0x6d7cc6c52f08646f86982b313e63a05c33d861f83980bad824efad711caf7d26

Final snowtrace of activity from Terrific moving to Tornado Cash
https://snowtrace.io/address/0x09ccbcd71a14997c6be26d9ff3b8be0e16747e56

There was an emergencyWithdraw function that some users might have been able to use to withdraw from the liquidity pool
https://snowtrace.io/address/0x31a7fc9625a37d2f026b9b6070cfe05553245bdf#writeContract

What the Batasm team has learned:

1. Ensure that there is a timelock masterchef and pool contracts
    - If a timelock with reasonable delay was in place, there might've been sufficient time for investors/community to react.
2. Renounce ownership
    - removes all possibilities for devs to make any changes or mint new tokens.
3. emergencyWithdraw() function
    - Only callable by users and provides a way to call into contract if the dApp is no longer available.

Trust is hard to navigate within this space as projects and teams tend to stay anonymous. In this scenario, the Terrific dev's social engineered and leveraged trusted community members to carry out their ill intentions. Therefore, we think that KYC'ing with the right authority is of utmost importance, as this provides that additional vector of trust for the community and partners.

The Batasm team is kyc'd with The Tulip DAO.