Solutions for the TinyMan v1.0 Hack and PeraWallet Verification

By Brian Haney
December 9, 2022

Introduction

Hipo Labs is the creator of TinyMan and PeraWallet. The company was founded by Kaan Eryilmaz and Taylan Pince. In January 2022, the TinyMan v1.0 protocol was hacked. As a result, several Choice Coin users who had provided liquidity in those pools lost assets. In March of 2022 the TinyMan Compensation Program was released promising all effected users would recover loss and would make assets available to users suffering loss.

However, as explained in this Report, no Choice Coin users were ever compensated for their loss. After the Hack, PeraWallet, which is also a product of Hipo Labs, removed Choice Coin's verification on the Algorand blockchain. This decision was made unilaterally and without any regard for the legitimacy of the project, its contributions to open-source software development, nor the value Choice Coin adds to the Algorand blockchain. The purpose for this Post is to encourage collaboration with Hipo Labs to properly compensate Choice Coin users as previously promised and appropriately funded.

The Hacks

The first attack was carried out by the following address.

MNN5MB3E7JSJPA6FRMCKUTK5V77GSJIALVWVCBXFZLEVAUEY5FUPGJUDPE

The first hacker funded the address with the following TXID from Binance.

3ES475ZKZPSCVJPZZNZZWJD2CVFMELRRI4K4SL4RHXMDOLT5YP3A

After the attack and relaunch of the TinyMan v1.1 protocol, the hacker swapped 501,300.37 Choice for various assets including Algo and YLDY. The second attack was carried out by the following address.

KFPIZAUTTOXIN5DGDGMMNSPVXYD6YGC7TEDPKZANIXYWBIFB445OTEY4N4

The second hacker funded the address with the following TXID from Okex.

UWW5KSPSPGV3J5XURM2SQFEKO4UYAVEHLTCSHWMVXSTEW2XZDCFA

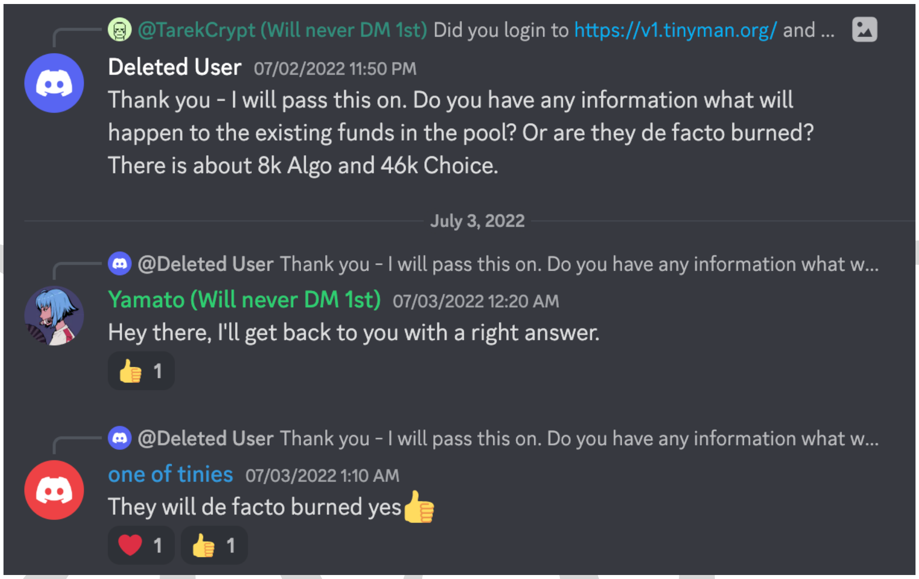
Both addresses were funded by centralized exchange accounts, which have access to the hacker's identity.

Existing Assets

The TinyMan v1.0 Choice-Algo pool is available at the following address.

4ADBL4JU6XRWT2DLWMNTQ7V7GLQUVVUQJ5NDWUNGXAJPRW3JGZ7HJUSC4I

As I was investigating the 2022 TinyMan Hack, I asked for information from the TinyMan team on Discord regarding the status of the attacked pool, my account GreenRex is now Deleted User. My assumption was that the v1.0 protocol was taken offline and that the remaining assets were burned, which was confirmed by the TinyMan Team on Discord.



@TarekCrypt (Will never DM 1st) Did you login to https://v1.tinyman.org/ and ...

Deleted User 07/02/2022 11:50 PM

Thank you - I will pass this on. Do you have any information what will happen to the existing funds in the pool? Or are they de facto burned? There is about 8k Algo and 46k Choice.

July 3, 2022

@Deleted User Thank you - I will pass this on. Do you have any information what w...

Yamato (Will never DM 1st) 07/03/2022 12:20 AM

Hey there, I'll get back to you with a right answer.

👍 1

@Deleted User Thank you - I will pass this on. Do you have any information what w...

one of tinies 07/03/2022 1:10 AM

They will de facto burned yes👍

❤️ 1 👍 1

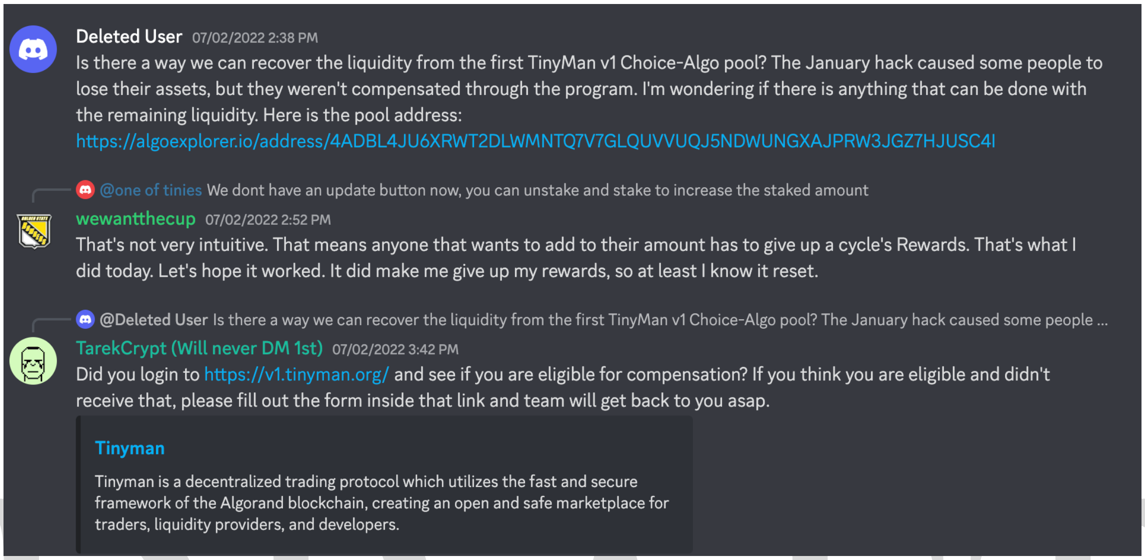
My assumption was verified by TinyMan, who wrote the assets will be de facto burned. However, in October of 2022, the same TinyMan v1.0 Choice-Algo pool was again attacked, and the attacker siphoned 5,650.775262 Algo from the pool. The transaction ID for the second attack is available at the following.

MTBGLTBMYCM7EUSFY6K7L6ONQ7AQN3V7C2NT3TZHEU3WXD2QDXVA

After discovering the additional attack, I reached out to the TinyMan team via email to find a solution for the problem and efforts are ongoing. In fact, the pool still contains 2,669.95 Algo and 65,243.91 Choice.

Compensation

I had received several complaints from Choice Coin users that they had not received compensation for their lost assets and inquired directly of TinyMan in July via Discord.



Deleted User 07/02/2022 2:38 PM
Is there a way we can recover the liquidity from the first TinyMan v1 Choice-Algo pool? The January hack caused some people to lose their assets, but they weren't compensated through the program. I'm wondering if there is anything that can be done with the remaining liquidity. Here is the pool address:
https://algoexplorer.io/address/4ADBL4JU6XRWT2DLWMNTQ7V7GLQUVVUQJ5NDWUNGXAJPRW3JGZ7HJUSC4I

@one of tinies We dont have an update button now, you can unstake and stake to increase the staked amount
wewantthecup 07/02/2022 2:52 PM
That's not very intuitive. That means anyone that wants to add to their amount has to give up a cycle's Rewards. That's what I did today. Let's hope it worked. It did make me give up my rewards, so at least I know it reset.

@Deleted User Is there a way we can recover the liquidity from the first TinyMan v1 Choice-Algo pool? The January hack caused some people ...
TarekCrypt (Will never DM 1st) 07/02/2022 3:42 PM
Did you login to https://v1.tinyman.org/ and see if you are eligible for compensation? If you think you are eligible and didn't receive that, please fill out the form inside that link and team will get back to you asap.

Tinyman
Tinyman is a decentralized trading protocol which utilizes the fast and secure framework of the Algorand blockchain, creating an open and safe marketplace for traders, liquidity providers, and developers.

I relayed the information to the complaining Choice Coin users, none of whom found they were determined to be eligible. This was although according to the TinyMan Attack Reports published on Reddit and by Headline, show at least worth of 121,936 Algo and Choice were affected by the attack.

The assets made available for effected users as part of the TinyMan Compensation program were stored in this Algorand address.

K3G7XHS3V4547EFGKMYXLVIEBEGG6ZYDU5IWM73D3U75RNIBPF2KPKRCWA

As evidenced by the address transaction logs, no Choice Coin users who suffered loss during the hack were compensated. The amounts below show the estimated total impact of loss suffered by attacks on the initial pool.

Choice Exploited	Algo Exploited
566,544.28 Choice	69,288.73 Algo

This amount does not include subsequent value loss suffered as a result of the hackers swaps on the TinyMan v1.1 protocol. The list of asset holders effected by the attack is available at the following asset ID for the TinyMan pool tokens.

359384389

PeraWallet Verification

Verification of assets on Algorand has always been a big problem for new projects and I've always advocated for solutions, starting in September of 2021. The PeraWallet team, then demanded that if Choice Coin wanted to receive its verification back, that I would personally be required to send them my government issued ID as required by the Pera ASA Verification. To be clear, I am not able to send PeraWallet my government issued ID for security reasons.

This is because my ID has sensitive personal information, and it is important that the information stays secure. At no time prior, had anyone ever said that getting an asset verified would require creators to disclose sensitive government information to a third-party platform. Still, I fought hard to get Choice verified. To be clear, I fully disclosed my identity as one of the co-creators of Choice Coin. But, at a certain point in my discussion with Taylan, it became clear that regardless of what else was true, Taylan would not verify Choice Coin without my personal government ID. I am still openly seeking a solution to this dilemma.

Solutions

1. I will continue to work with TinyMan to ensure that effected users receive compensation for lost assets. TinyMan should provide the appropriate amount of assets lost to all effected Choice Coin users as previously promised.
2. I will continue to work with Pera ASA to ensure they have the needed information necessary to validate the project and provide verification on Algorand. Despite, my inability to give away my government ID, PeraWallet should provide an alternative method to validate and verify Choice Coin.