Subject:

Urgent Request to Freeze Malicious Addresses Involved in Stolen stETH Funds

To:

Lido Governance and Security Team

Date:

2024-12-18

Summary:

I am submitting an urgent request to freeze the following addresses due to their involvement in the theft of stETH tokens from my wallet through phishing attacks. Immediate action is required to prevent further withdrawals and secure user funds.

Malicious Addresses:

1. 0x2588C8170fcb77367b5A44C941d8aA91D0F6E8b4
2. 0x5400F716F97a294B75c5Db0C37D432231485e426

Incident Overview:

- Nature of Attack:

Phishing scam targeting stETH holders.

- Affected Party:

Victor Yeung (Wallet holder address: 0xc02039eC1e6c382F99EE4391B0492Ea2eD5234d2).

- Funds Stolen:

5.2 stETH.

Transaction Reference:

- Etherscan Links:
- [0x2588C8170fcb77367b5A44C941d8aA91D0F6E8b4]
- [0x5400F716F97a294B75c5Db0C37D432231485e426]
- [0x2588C8170fcb77367b5A44C941d8aA91D0F6E8b4]
- [0x5400F716F97a294B75c5Db0C37D432231485e426]
- Transaction Hash:

0x72ee6ede114f8569a55f0bc06e72bda144db7386f6032df265d05c61b96b2ce1

Requested Action:

1. Immediate Freezing:

Freeze the specified addresses to prevent any further withdrawals or transfers of ETH.

Justification:

Allowing withdrawals from these addresses could enable the attacker to launder stolen funds, causing irreversible damage to the victim and tarnishing Lido’s platform reputation.

Conclusion:

We trust that Lido’s governance and security teams will act swiftly to protect the interests of the community and affected users. Please confirm receipt of this request and inform us of any next steps.

Sincerely,

Victor Yeung

[

](/cdn-cgi/l/email-protection#0963686a62303f38393830496e64686065276a6664)