

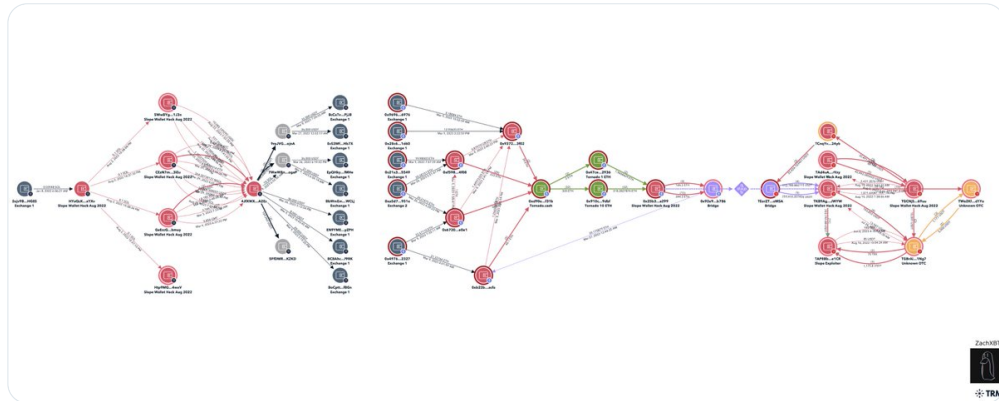


ZachXBT @zachxbt

Oct 10, 2023 · 9 tweets · [zachxbt/status/1711748033954590900](https://twitter.com/zachxbt/status/1711748033954590900)

1/ What happened to the funds from the @slope\_finance \$4M hack?


Here's my analysis tracing the latest movements in 2023 and where the stolen funds ended up going.



2/ TLDR: Slope Wallet (founded by Leal Cheung) was hacked in August 2022. After the hack their entire team disappeared.

Multiple Solana community members I reached out to confirmed this.


In May 2023 whoever ran the account fell for a prank and accidentally made a tweet.

 **Slope**  
@slope\_finance · Follow

Thank you again to @osec\_io + @SlowMist\_Team for their efforts assessing/reviewing the breach. They have now both published full reports (below):

- OtterSec - [osec.io/reports/slope-...](https://osec.io/reports/slope-...)
- SlowMist - [slowmist.medium.com/analysis-of-a-...](https://slowmist.medium.com/analysis-of-a-...)

We will also publish an internal Slope factsheet tomorrow.




slowmist.medium.com  
Analysis of a Large-scale Attack on Solana (Part 2)  
This article will only share staged investigations with community members.

4:42 PM · Aug 16, 2022

176 Reply Copy link

[Read 189 replies](#)

 **Slope**  
@slope\_finance

**Greed consumed me.**

I connected my wallet to a random site, signed a blind tx, handed over write perms for my Twitter.

This was The **\$GREED** Experiment.

Thank you @voshy for the wakeup call.

I will keep this on my timeline and own it.

**My full statement:**  
[voshy.medium.com/the-greed-expe...](https://voshy.medium.com/the-greed-expe...)

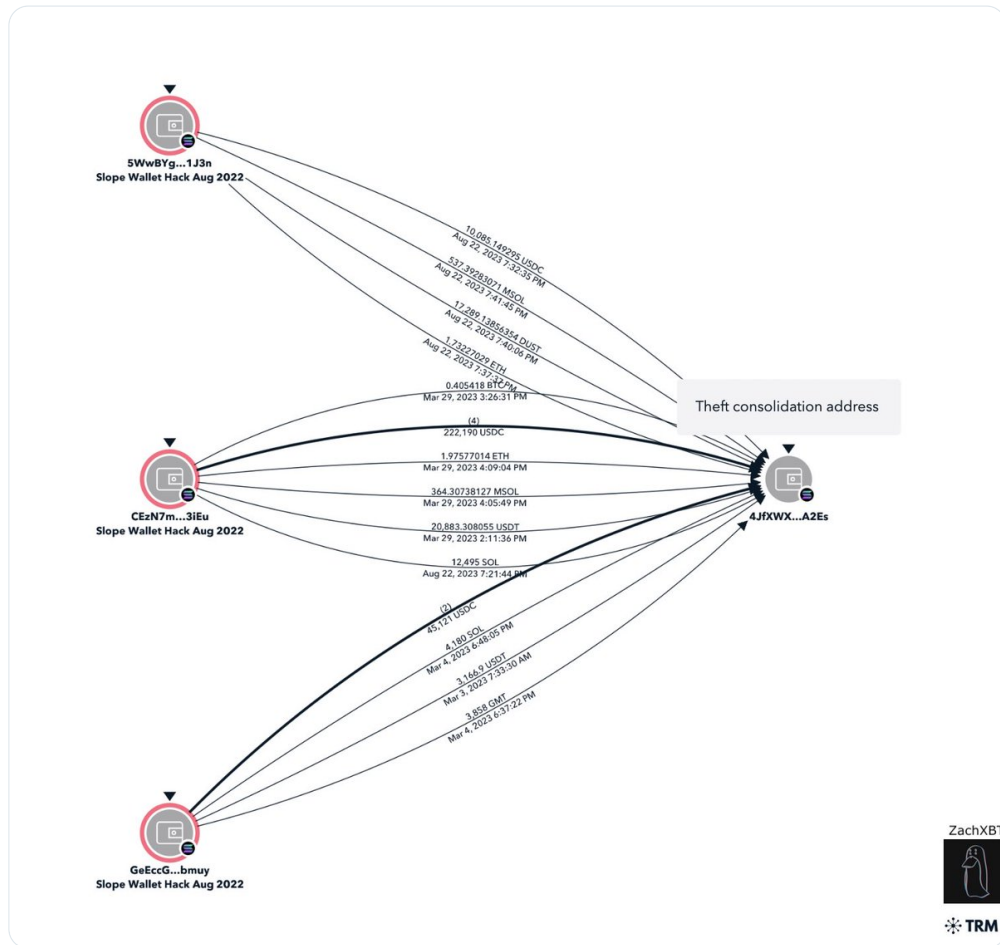
This is a short version of my story about greed and my learnings. For the full version please click the link in this same Tweet.

It started a few days ago when I heard about \$GREED. I failed to see this was an attempt at sarcastic social commentary and got caught up in the hype. Fear of missing out was stronger than my good judgement.

3/ In March & August 2023 the hacker was active laundering funds off of Solana from the original theft addresses.

SOL Consolidation address:

4JfXWXd2aenLncrdpJcryX8kZVJUSHyGPnc6HSyhA2Es



4/ The hacker used instant exchanges (Binance nested) to transfer funds from Solana -> Ethereum

Using timing analysis I was able to find the destination addresses as they were reused each time.

ETH destination address

0x9372e8fa0286e8aed82fe9f897bba1ae549f3f02  
0xf59880f2e434a0a7e598bbeab27ab2301cbc4f08  
0x67208653edc4f8bed74bdacc84f7251d7255e0e1  
0xb22b4f480a717505d37944a953bb60b4f741acfa

5/ From the ETH addresses above fun were deposited to Tornado Cash.

Tornado deposits (322 ETH total)

March 9 - 8 X 10 ETH  
March 27- 6 X 10 ETH  
July 14 - 6 X 10 ETH  
Aug 15 - 1 X 10 ETH, 2 X 1 ETH  
Aug 23 - 11 X 10 ETH

6/ I then demixed the Tornado withdrawals. For some reason the Slope hacker withdrew funds to only one address.





17:20–18:00

Panel: Challenges and Opportunities in the upcoming DID future

Chi FENG, Founding Partner, SevenX Ventures (Moderator); Wendy, PMO, HashKey DID; Yisi LIU, Co-Founder and CTO of Mask Network, Founder of Next.ID; James WEN, Co-Founder and CEO, Dmail Network; Xiao ZHANG, Founder, zCloak Network; Leal Cheung, Co-Founder, zkMe



Follow

**zkMe** 

@zkme\_

It's our vision to build the zk-credential layer of web3. zkMe verifies user credentials without disclosing any personal information to anyone!

 Science & Technology  [link3.to/zkme](https://link3.to/zkme)

 Joined September 2022

71 Following **59.2K** Followers



**LC**

last seen recently



**Info**



Username



**Notifications**

On



Add to contacts

**Groups**



**Aptos Builders**

1,221 members



**SOLSecurity Community**

235 members

