

DEFCON at DEVCON

A TABLETOP EXERCISE





Peter Kacherginsky



Heidi Wilder

More than **\$620M** were stolen
from DeFi projects across **277**
incidents so far in **2024**.

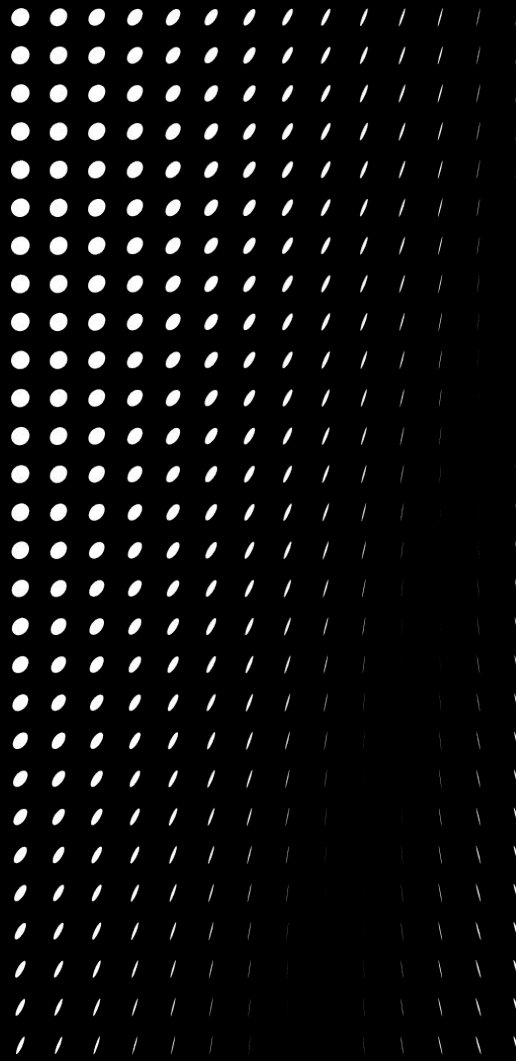
Average time to steal most of your
assets: **15 min**

Average time for projects to
respond to incidents: **1 hour**

In **27** instances fast actions of **whitehats** helped return **\$150M**.

You too can save millions by practicing **incident response** in a safe and controlled environment.

1 The Tabletop



TTX

A tabletop exercise is a method of **practicing** response to a simulated **scenario**.

Goals

- Practice **Incident Response** handling.
- Learn about DeFi **threats** and **exploitation tactics**.
- Bring back **practical experience** to your project.

Ground Rules

- Participation is encouraged (Slido).
- **Suspension of disbelief** at times.
- It will **not be perfect**, but we will learn together!

Terms

- **Injects** - time based learnings.
- **Artifacts** - incident facts.
- **Discussion** - IR prompts.

Logistics

- **Facilitator** will provide **injections** and help avoid rabbit holes.
- **5 min** break midway.
- **Post-mortem** after the exercise.

Slido



Slido #5551555

Let's begin...



FounderMode DAO

`_founderMode`

- **\$150M TVL** on **Mode** chain
- **\$FUMO** governance token
- Invests into other nascent DeFi projects by requiring them to create a **\$FUMO** token pair
- **80%** of all projects on Mode hold **\$FUMO** or some derivative

You were just hired by **FounderMode DAO**, by
a friend you met at **Devcon 2022!** 🎉

Team is **fully remote** and consists of **5 people**.
Everyone uses their **real names**...

You just finished onboarding and reading developer docs, when suddenly...

Inject 1: Security Alert 🚨

It's 3am.

Your phone is blowing up — Telegram, Signal, Discord, X — all are saying **your project just got rekt.**

Your team is panicking and begging you to sign off on a quick protocol upgrade.

What do you do?

→ How do you respond?

→ What happened?

→ How did it happen?

→ How would we triage?



Slido #5551555

DeFi Attack Kill Chain



1	Reconnaissance	Test exploit transactions. Public discussion of vulnerabilities.	Unknown
2	Resource Development	Initial funding to pay for the attack.	2024-09-20 19:18:59 - Received eth to pay for gas
3	Preparation	Helper contract deployment, configuration, testing.	2024-09-20 19:21:59 - Exploit Deployed
4	Exploitation	Active exploitation.	2024-09-20 19:30:59 - Two exploit txs
5	Laundering	Bridging, Swapping, Mixing stolen assets.	2024-09-20 19:35:47 - Swapping

DeFi Incident Lifecycle



1	Detection	Continuous analysis of security-related signals (e.g. on-chain alerts, social media, logs, etc.)	2024-09-20 20:31:00 - Chaofan tweet
2	Triage	Determine if there is a security incident , severity, and scope.	2024-09-20 20:55:00 - Announcement
3	Containment	Stop the bleeding first (e.g. pause the protocol, shut down the Dapp, etc.)	2024-09-21 00:49:47 - Pools paused
4	Mitigation	Fully eliminate and/or mitigate the root/cause of the incident.	2024-09-20 22:23:35 - Negotiating 2024-09-21 03:06:23- Funds returned
5	Recovery	Restoring normal operations.	TBD

Inject 2: Malicious Insider

Online sleuths (ZachXBT) point out that one of the funding addresses for the attack has an ENS name with the same Telegram handle as a recently hired contractor.

→ What are our immediate security concerns?

→ How should we investigate this situation?

→ How can we respond - internally & externally?



Slido #5551555

Case Studies

→ On September 15, **DeltaPrime** was hacked for \$6M due to a compromised admin key.



DeltaPrime ✓
@DeltaPrimeDefi

...

1 What's the status... on the attack vector? **1**

While we know one of the founder's computers was compromised, the investigation has not yet yielded definitive results as on how.

The key was not leaked on-chain and no malware was found. Computers will now be thoroughly examined by a digital forensics company.

4/9

4:05 PM · Sep 25, 2024 · **1,685** Views

Inject 3: Users drained 🚨

Multiple reports of users' wallets being drained on Mode network. All compromised users have previously interacted with the FounderMode contract.

→ What could be causing these wallet drains?

→ How should we respond to protect users?

→ What is the overall impact to the protocol / ecosystem?



Slido #5551555

Case Studies

→ On October 16, 2024 **Radiant Capital** lost \$53M after its developers were tricked into signing a malicious upgrade.

→ Following the initial drain, bad actors targeted user wallets that previously approved funds to the compromised contract.

Break for 5 minutes...



Inject 4: Laundering 🌀

Attacker starts swapping moving funds to various EVM chains.

- Can devs do something?
- What actions can we take?
- Who can help us stop this?
- How do we warn everyone?



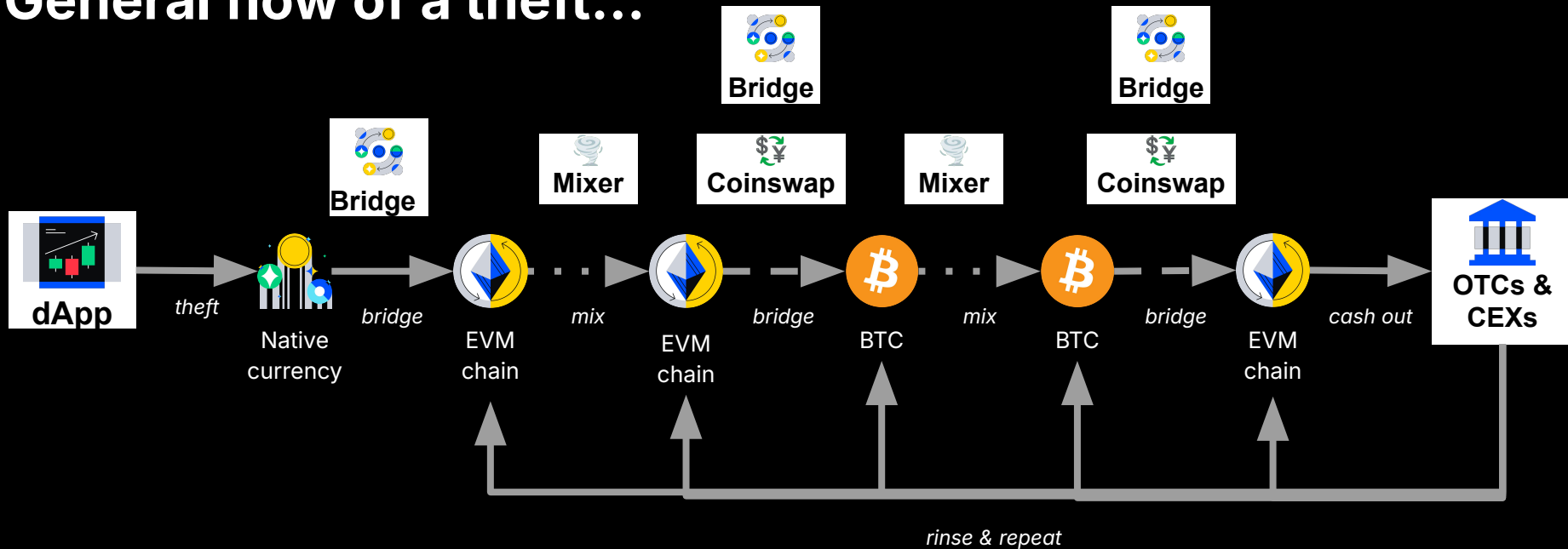
Slido #5551555

Case Studies

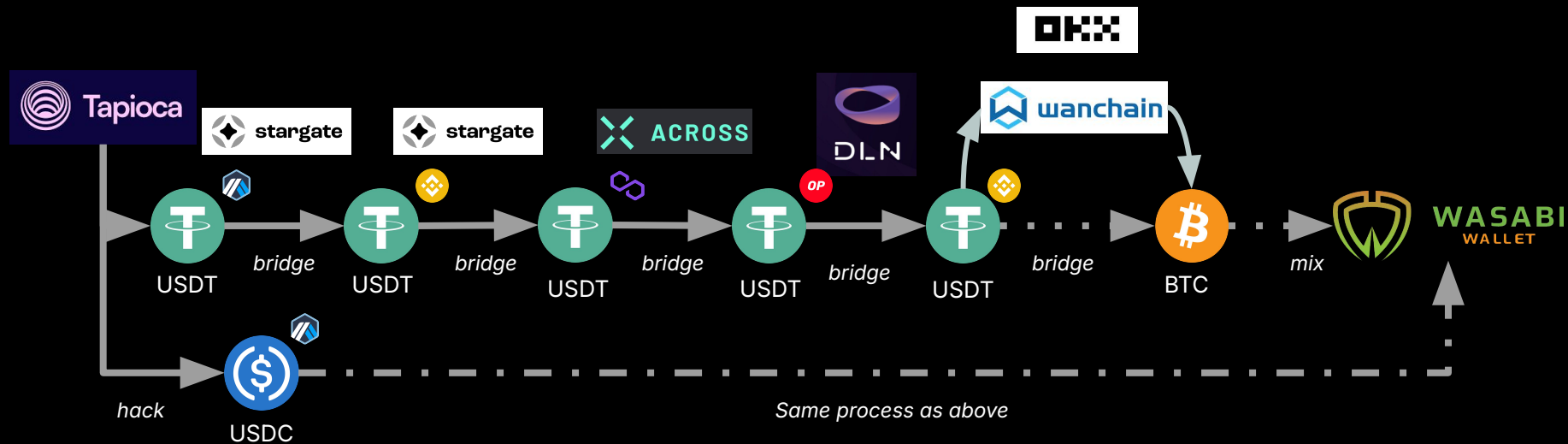
→ **Generally**: Use of mixers, bridges, coinswap services, CEXs

→ **Tapioca**: Increased use of bridges as mixing services

General flow of a theft...



Tapioca DAO Theft



Inject 5: Negotiations 🤝

The team is getting increasingly panicked that there is no way to get funds back.

The team founder is begging to start outreach to the attacker.

→ What would your message read?

→ What are you negotiating for?



Slido #5551555

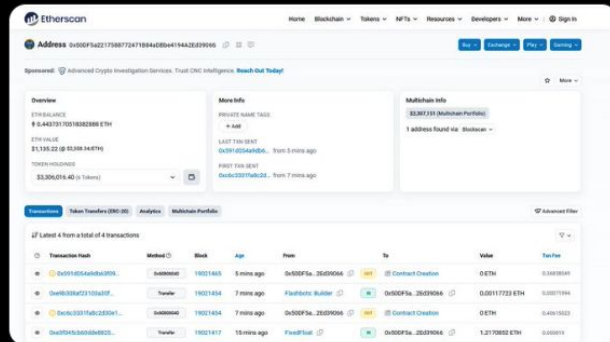
Case Studies

→ On January 16, 2024 **Socket** was hacked for \$3.3M



Spreek
@spreekaway

Socket/Bungee approval being exploited rn. several million already gone.
attack is ongoing



Etherscan Home Blockchain Tokens NFTs Resources Developers More Sign In

Address 0x00F5a2217380722471894C804414A3209906 Buy Exchange Pro Security

Sponsored: Advanced Crypto Investigation Services. Trust DMC Intelligence. [Reach Out Today!](#)

Overview

ETH BALANCE
\$ 5,440,791.100 (808,888 ETH)

ETH VALUE
\$1,135.22 @ \$0.208 (14,679)

TOKEN HOLDINGS
\$3,300,076.40 (3 Tokens)

More Info

Private Note: 1235
+ 1460

LAST TXN SENT
0x00F5a2217380722471894C804414A3209906 - 5 mins ago

RECENT TXN SENT
0x00F5a2217380722471894C804414A3209906 - 7 mins ago

Multichain Info

0x00F5a2217380722471894C804414A3209906 (Multichain Profile)

1 address found on Blockchain

Transactions | Token Transfers (20/30) | Analytics | Multichain Profiles | Advanced Filter

27 Latest 4 from a total of 4 transactions

Transaction Hash	Method	Block	Age	From	To	Value	Gas Fee
0x00F5a2217380722471894C804414A3209906	Initiate	19021405	8 mins ago	0x00F5a2217380722471894C804414A3209906	Contract Creation	0 ETH	0.00000000
0x00F5a2217380722471894C804414A3209906	Transfer	19021404	7 mins ago	Flashbots Builder	0x00F5a2217380722471894C804414A3209906	0.00117723 ETH	0.00000000
0x00F5a2217380722471894C804414A3209906	Initiate	19021404	7 mins ago	0x00F5a2217380722471894C804414A3209906	Contract Creation	0 ETH	0.00000000
0x00F5a2217380722471894C804414A3209906	Transfer	19021417	15 mins ago	Flashbots	0x00F5a2217380722471894C804414A3209906	1.2170802 ETH	0.00000000

11:19 AM · Jan 16, 2024 · 735.5K Views

我们了解您是 Socket 的攻击责任方。 我们想跟你讨论一项赏金，并将大部分资金退还给被影响的用户。 通过 blockscan 聊天联系我们。 你有 12 个小时。

We understand you are responsible for the Socket attack. We would like to discuss a bounty with you and return most of the funds to affected users. Contact us via blockscan chat. You have 12 hours.

please contact me by email:qwesdaffghg@proton.me

Hello White Hat.

You got an email from incident@socket.tech. Let's work together on returning the funds.

Socket/Bungee Explo...	OUT	GnosisSa...8_0820	495 ETH
------------------------	-----	-------------------	---------

Socket/Bungee Explo...	OUT	GnosisSa...8_0820	5 ETH
------------------------	-----	-------------------	-------

Hello White Hat,



We confirm receipt of 500 ETH. We agree that this is a white hat operation. Once we have received the remaining 531.22 ETH, this white hat operation would not be prosecuted. We are grateful for the white hat's help in preventing further harm to our users.

Socket/Bungee Explo...	OUT	GnosisSa...8_0820	532 ETH
------------------------	-----	-------------------	---------

Case Studies

→ On November 22, 2023
KyberSwap was hacked for \$48.8M



 Urgent 

Dear KyberSwap Elastic Users,
We regret to inform you that KyberSwap Elastic has experienced a security incident.

As a precautionary measure, we strongly advise all users to promptly withdraw their funds. Our team is diligently investigating the situation, and we commit to keeping you informed with regular updates.

Thank you for your understanding and cooperation during this challenging time.

3:52 PM · Nov 22, 2023 · 1.3M Views

We have reached out to law enforcement and cybersecurity on this case. We have your footprints to track you.

So it's better for you if you take the first offer from our previous message before law enforcement and cybersecurity track you down.

If the situation is not Fixed, a bounty offer will Float to the community instead.

If you don't return 90% of the funds you took from users to 0x8180a5CA4E3B94045e05A9313777955f7518D757 by 10am UTC, 27 November, we will also initiate a public bounty program to incentivize anyone who provides additional information to support law enforcement and cybersecurity in your arrest and the recovery of users funds.

To discuss in private, email vutran54@proton.me.

Dear Kyberswap Executives, Employees, Token Holders and LPs,

I said I was willing to negotiate. In return, I have received (mostly) threats, deadlines, and general unfriendliness from the executive team. That's ok, I don't mind.

I have prepared a statement concerning our (potential) treaty. I plan to release it on Nov. 30 at Noon UTC, sharp.

Under the assumption that I am treated with further hostility, we can reschedule for a later date, when we all feel more civil. You need only say the word.

If not, we proceed as planned on Nov. 30.

Thank you.

To ALL relevant and/or interested parties,

I thank you for your attention and patience during this uncertain time for Kyber (the protocol/DAO) as well as Kyber (the company). Below I have delineated a treaty for us to agree to.

My demands are as follows:

- * Complete executive control over Kyber (the company)

- * Temporary full authority and ownership over the governance mechanism (KyberDAO) in order to enact legislative changes. My current wallet address is fine for this.

This is my best offer. This is my only offer.

I require my demands to be met by December 10, otherwise, the treaty falls through.

Additionally, should I be contacted by agents from any of the 206 sovereignties, concerning the trades I placed on Kyber, the treaty falls through. In this case, rebates will total to exactly 0.

Kyber is one of the original and longest-running DeFi protocols. No one wants to see it go under.

To assist with this transition of leadership, I may be contacted on telegram: @Kyber_Director

Thank you.

– Kyber Director

Inject 6: Attacker responds

Attacker responds with an encrypted message and a link to download a library for encrypted chat.

Decrypt with the private key of **fundermode.eth**
(<https://github.com/LimelabsTech/eth-ecies>).

bLKELKDSx1KDFJkd2opfLpdkdjflsdlk/+
GIVX9YYekdkmzz/EXsNzldjekjtkeiio9
4ncGS+j1wudkkZKjdkx02Py13K5SW3f/nz
t96To3kxN5Bb

- What is this?
- Are there any risks?
- Should we respond?
- Who is the attacker?



Slido #5551555

→ On March 13, 2023 **Euler Finance** was hacked for \$200M.

Case Studies



March 17: Donation to Lazarus

From:	0xb66cd966670d962C227B3EABA30a872DbFb995db (Euler Finance Exploiter 2)
To:	0x098b716b8aaf21512996dc57eb0615e2383e2f96 (Lazarus Group: Ronin Bridge Exploiter (OFAC Sanctioned)) (Ronin Bridge Exploiter)
Value:	100 ETH \$265,938.19

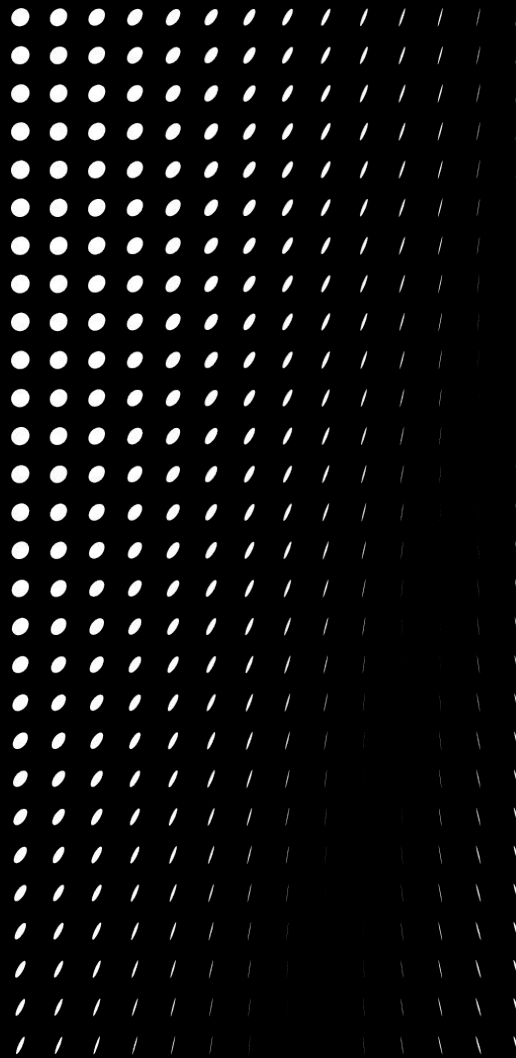
March 21: Lazarus Responds

From:	0x098b716b8aaf21512996dc57eb0615e2383e2f96 (Lazarus Group: Ronin Bridge Exploiter (OFAC Sanctioned)) (Ronin Bridge Exploiter)
To:	0xb66cd966670d962C227B3EABA30a872DbFb995db (Euler Finance Exploiter 2)
Value:	2 ETH \$5,318.76

Decrypt with the private key of 0xb66cd966670d962c227b3eaba30a872dbfb995db (<https://github.com/LimeLabsTech/eth-ecies>).

bKsKXCyxB1QjY2opF1BVGQQRnjzy67s6xFc/+GIvX9YeGakmzz/EXsNZ1AUhF37Q8RjVBn3DRVJP94ncxGS+j1wu5dLo4RRXrKS1rZzceoqVZ2pvsx02Py13K5SW3Yf/nzt96To3K0xN5sQqJZkfH6+RwWc+KoTAmomW1FNVWhlwV9UqKuuLwEo5heFmSFgBSJYNztvAEzZ/8Ra1BWu9P10zBbmX67W0/2DdDMAK31tX

2 Post-Mortem



What happened?

→ Malicious insider performed an unauthorized upgrade of the FounderMode DAO which drained locked funds.

→ Following the initial attack the attacker started draining user wallets that previously approved funds to the compromised address.

What happened?

→ The attacker started swapping stolen funds and bridging them everywhere until they were laundered through a Bitcoin mixer

→ The team attempted to negotiate with the bad actor, but instead received a link to potential malware.

Post-mortem 🤔

- What went well?
- What could be improved?
- What's left?



Slido #5551555



Slido #5551555

Questions?



Peter Kacherginsky
blockthreat.io
[@_iphelix](https://twitter.com/_iphelix)



Heidi Wilder
unlone.ly/app/channels/h3idi
[@h3idilao](https://twitter.com/h3idilao)

Thank you.