CYVERS

CoinsPaid Attack

meir@cyvers.ai

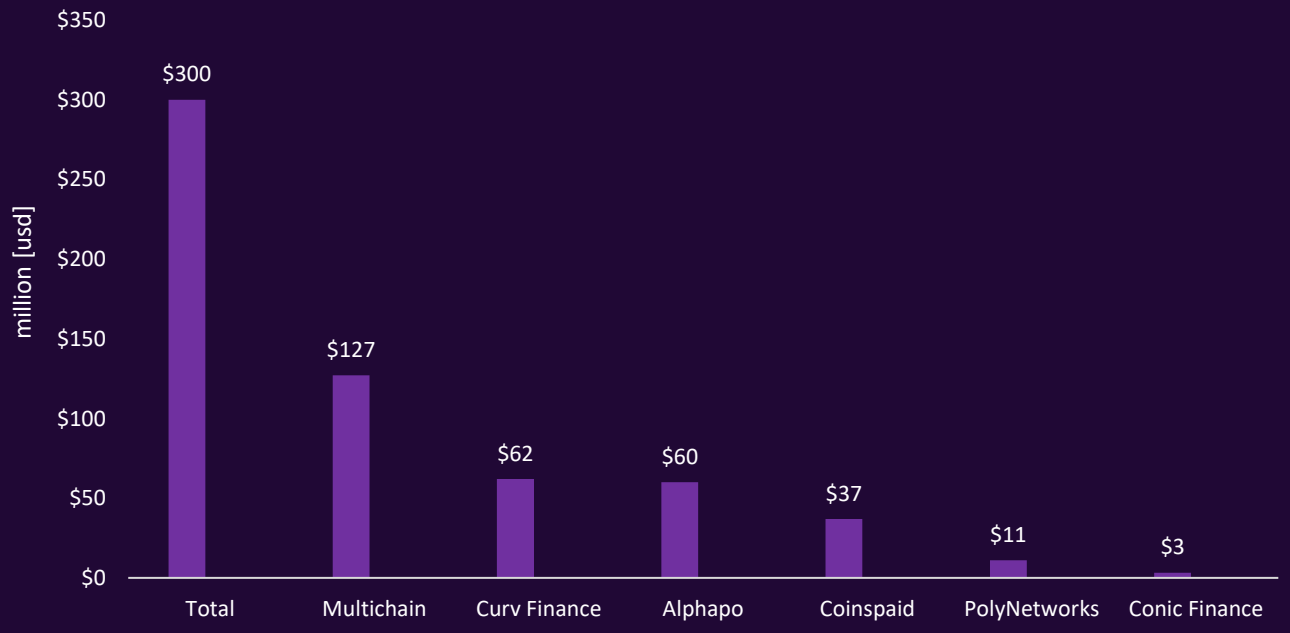
The Problem

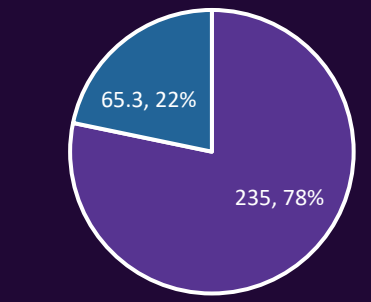
CYVERS

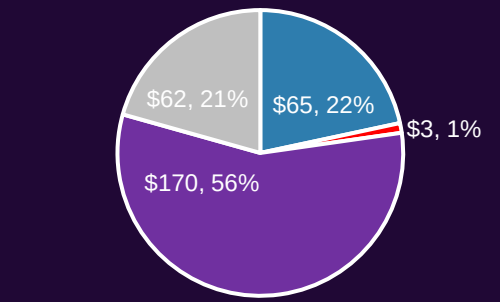
Source: Peter Kacherginsky, DSS 2023

Major incidents in July 2023

CYVERS

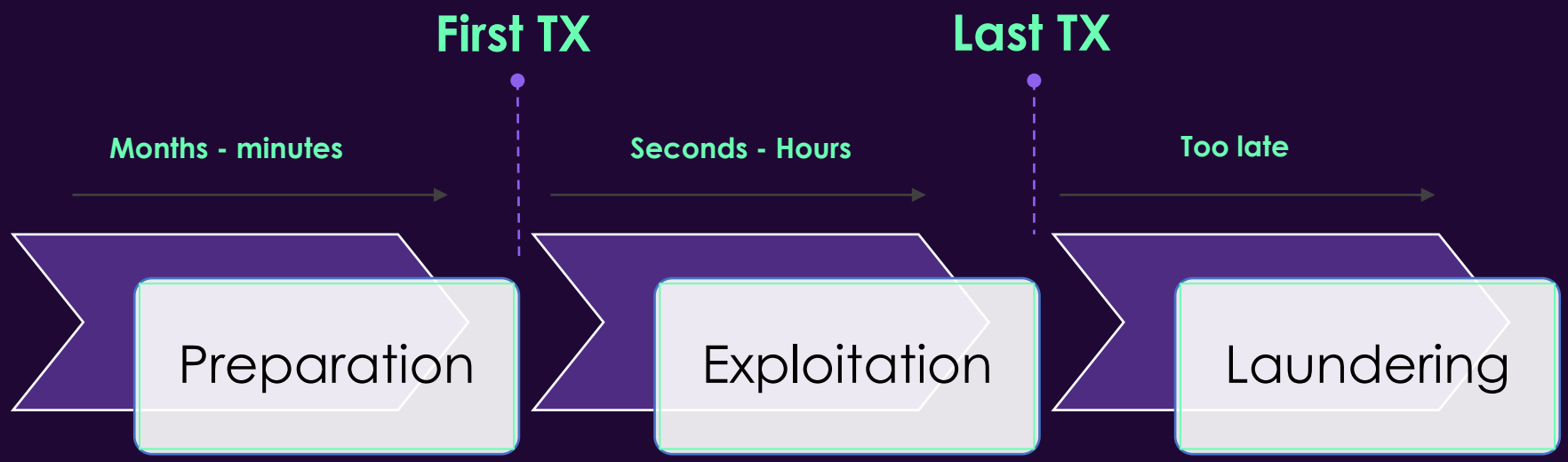






Web3 Attack Kill Chain

CYVERS



DeFi (Smart Contracts)

- Funding the attack
- Ownership Transfer
- Malicious contract Deployment

- Smart contract exploit transactions

Bridge, Swap and Cash out to CEX, DEX or Tornado Cash

CeFi (Wallets)

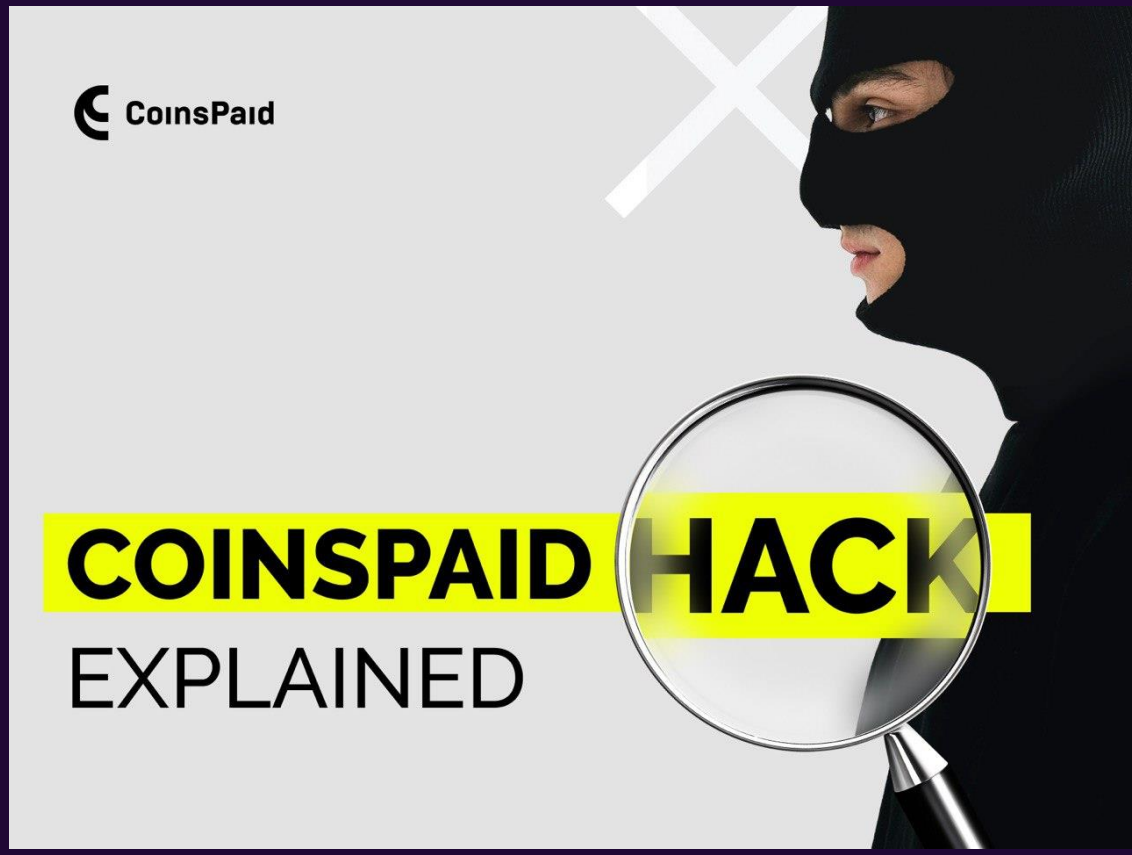
- Off-chain Web2 attack Preparation

- Private key leakage /access control transactions

CeFi – CoinsPaid attack 22.07.2023

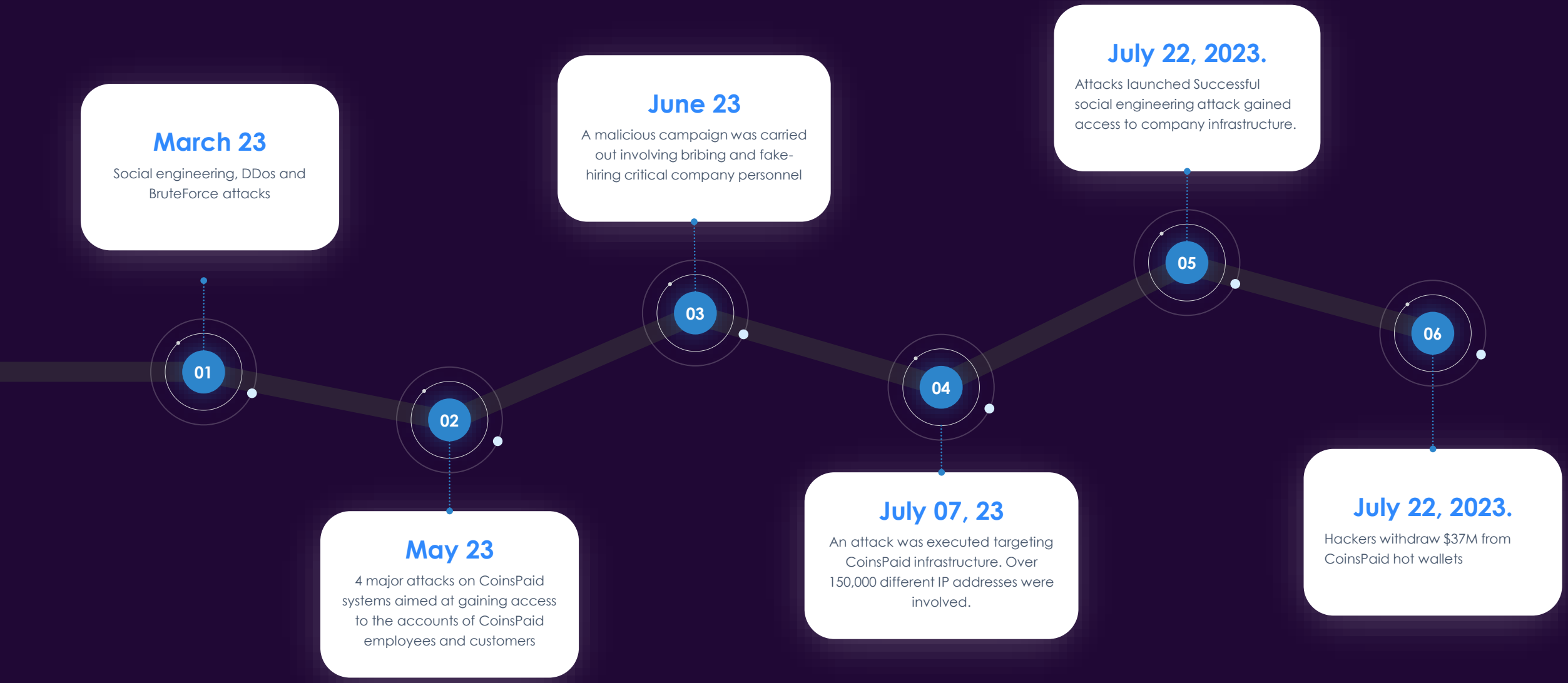
CYVERS

- CoinsPaid has processed €19 billion in crypto.
- On July 22, 2023, loss of $37.3 million on 3 different chains.
- Exploitation took around 4.5 hours, preparation 6 month.
- Suspects that Lazarus Group is behind the attack.

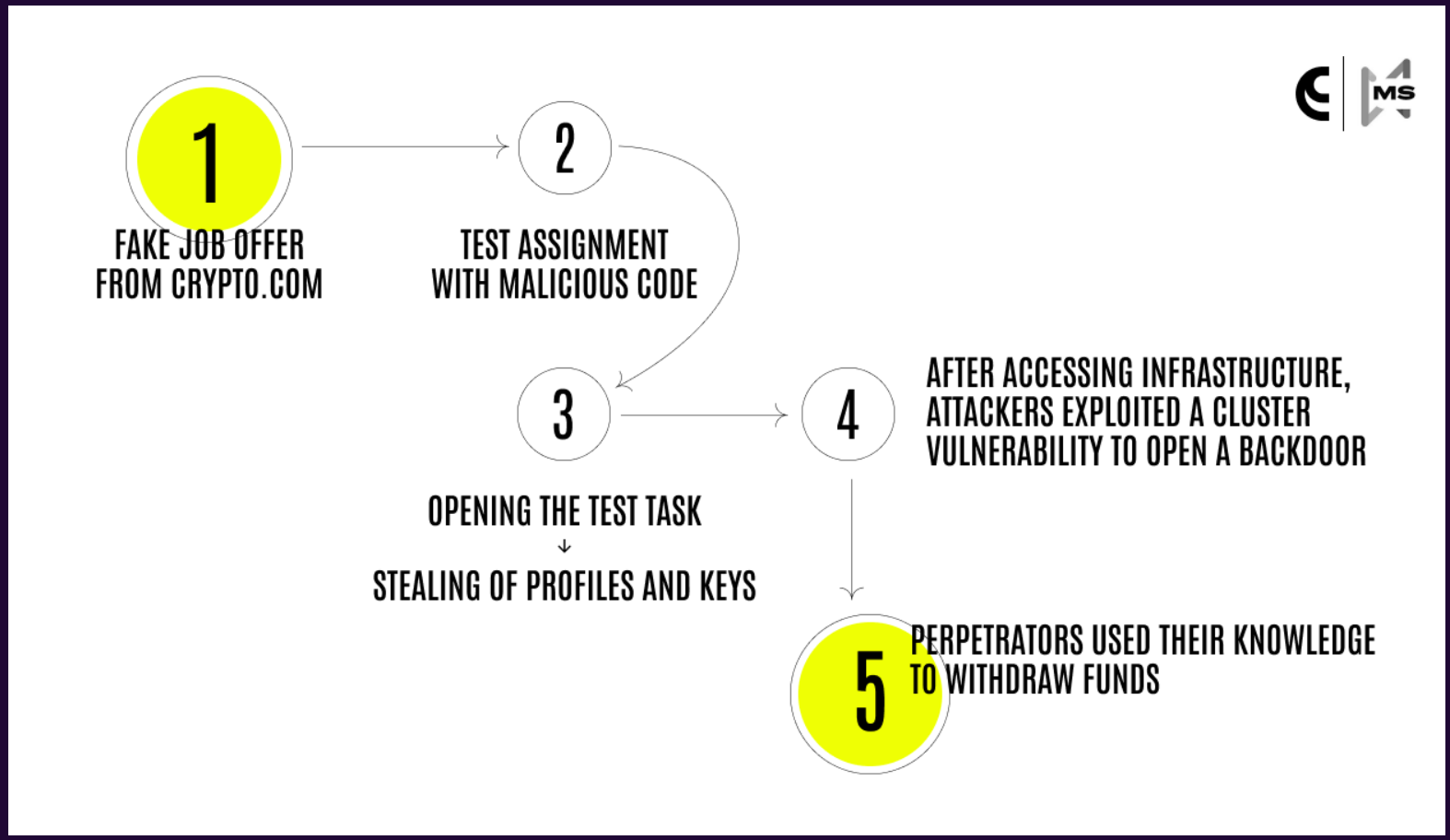


Attack Timeline

CYVERS



July 22 - off-chain attack analysis

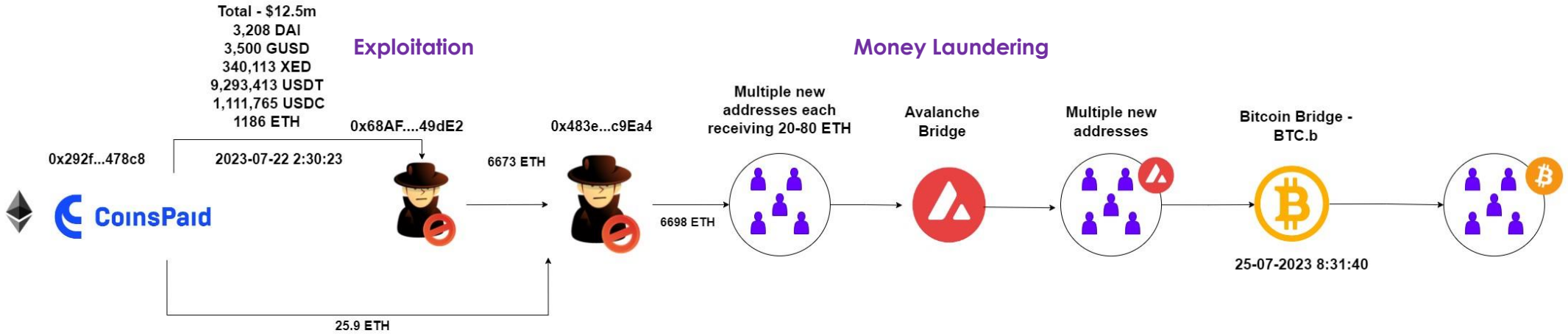


Source: CoinsPaid

July 22 - on-chain attack analysis

CYVERS

Total loss on ethereum:
~12.5M $

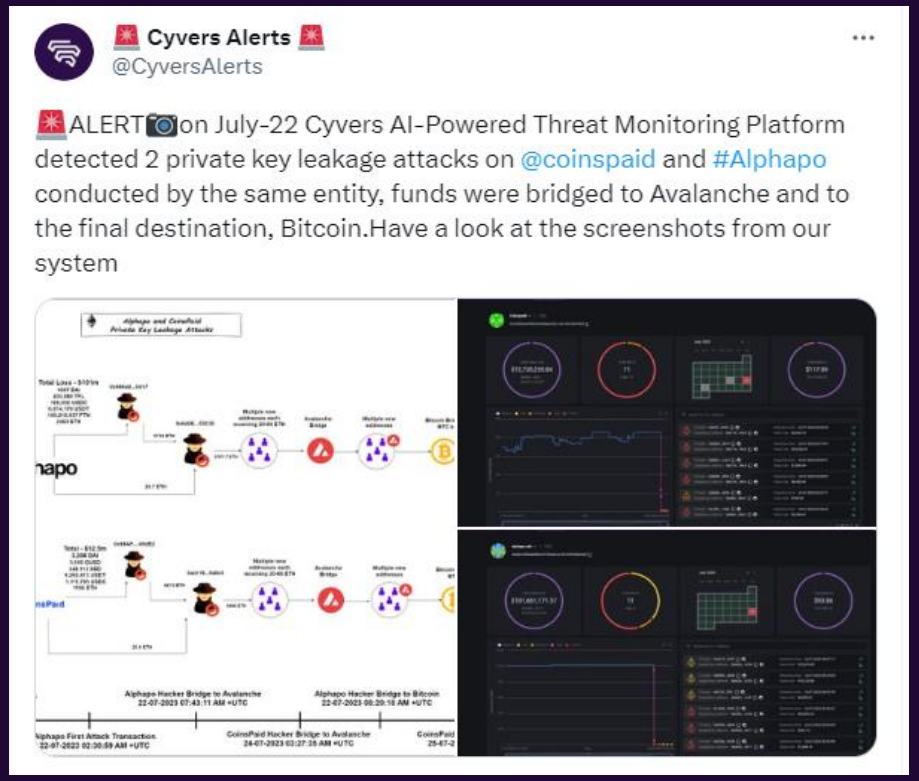


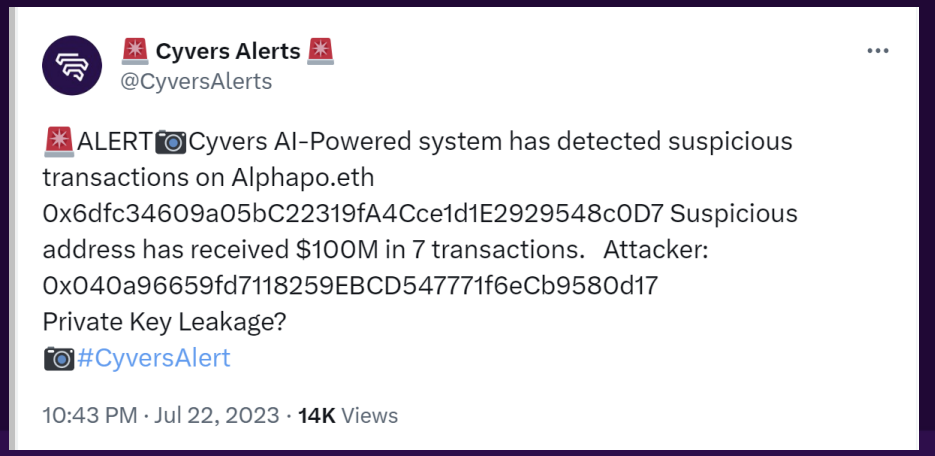
Coinspaid – Ethereum Hot Wallet

CYVERS

Conclusions

- Big attack surface Web2 + Web3
- Set up a monitoring systems also on Web3 infrastructure
- Attack are fast, automation of response needed.
- Current Blockchain AML scoring ineffective





CYVERS

Thank You

for your time