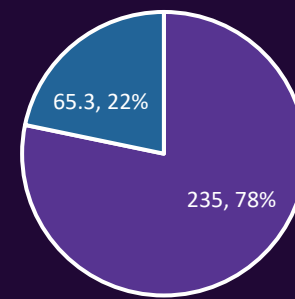
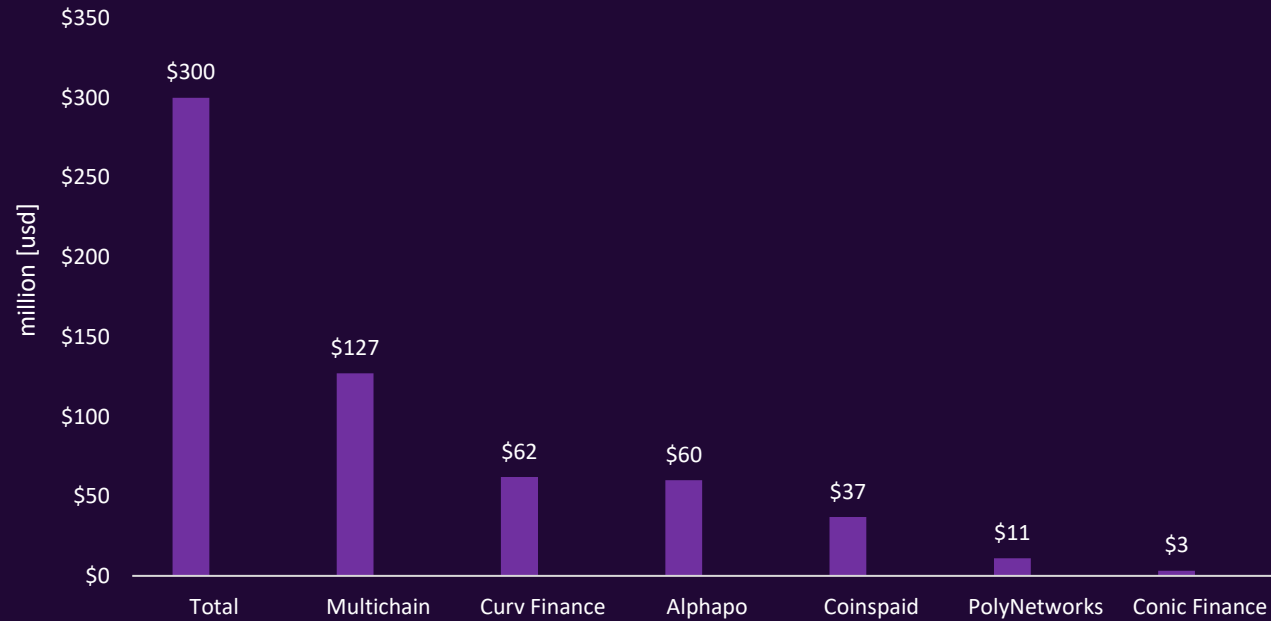


CoinsPaid Attack

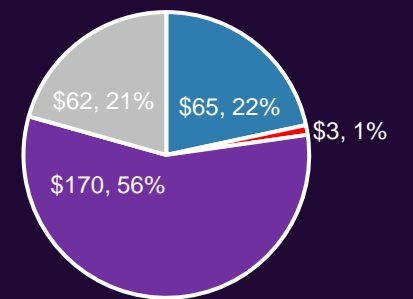




Major incidents in July 2023



Access Control Code Vulnerability



Thursday Friday Saturday Sunday



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

- 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.



March 23

Social engineering, DDos and BruteForce attacks

01

02

May 23

4 major attacks on CoinsPaid systems aimed at gaining access to the accounts of CoinsPaid employees and customers

03

June 23

A malicious campaign was carried out involving bribing and fake-hiring critical company personnel

04

July 07, 23

An attack was executed targeting CoinsPaid infrastructure. Over 150,000 different IP addresses were involved.

05

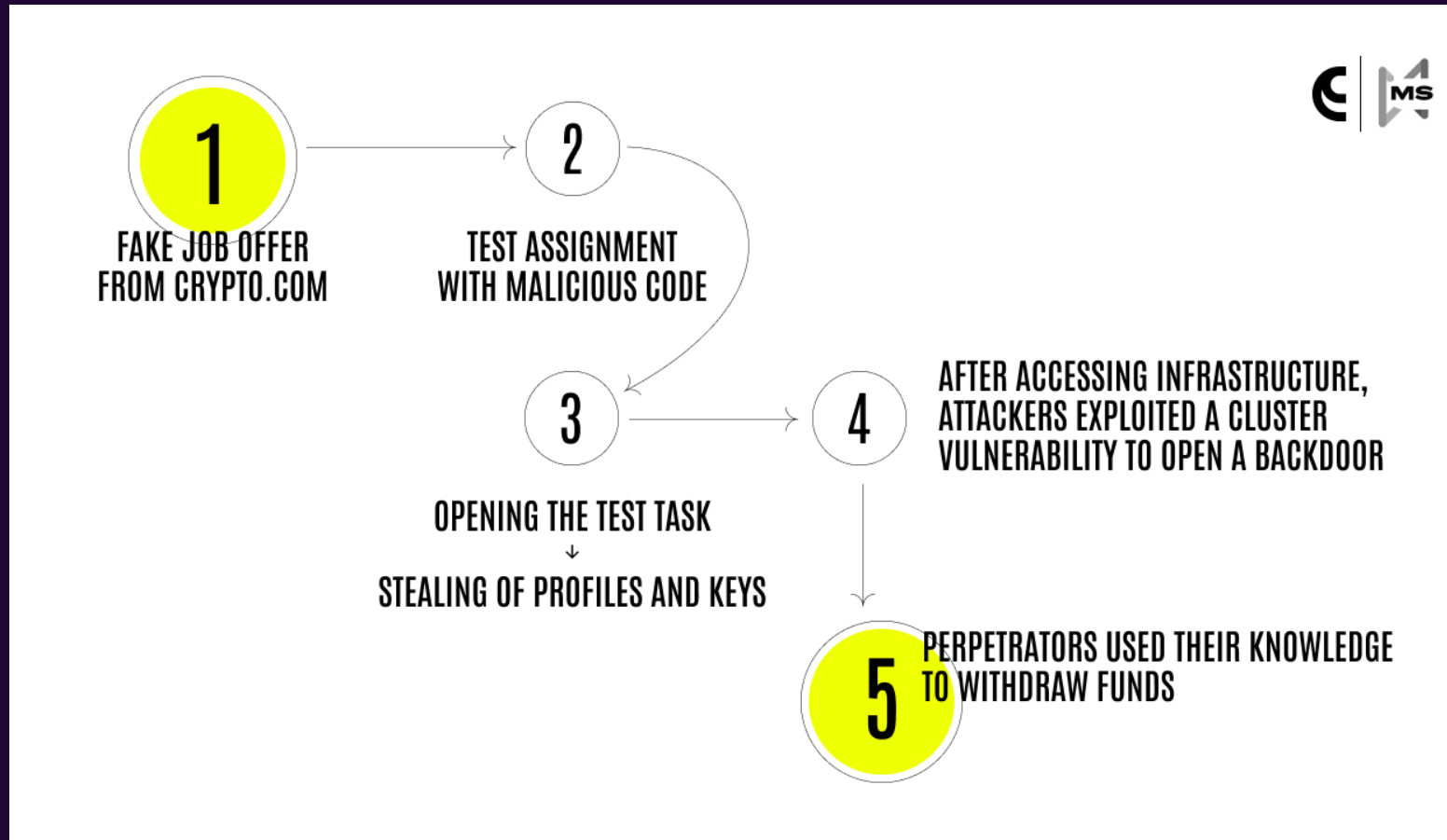
July 22, 2023.

Attacks launched Successful social engineering attack gained access to company infrastructure.

06

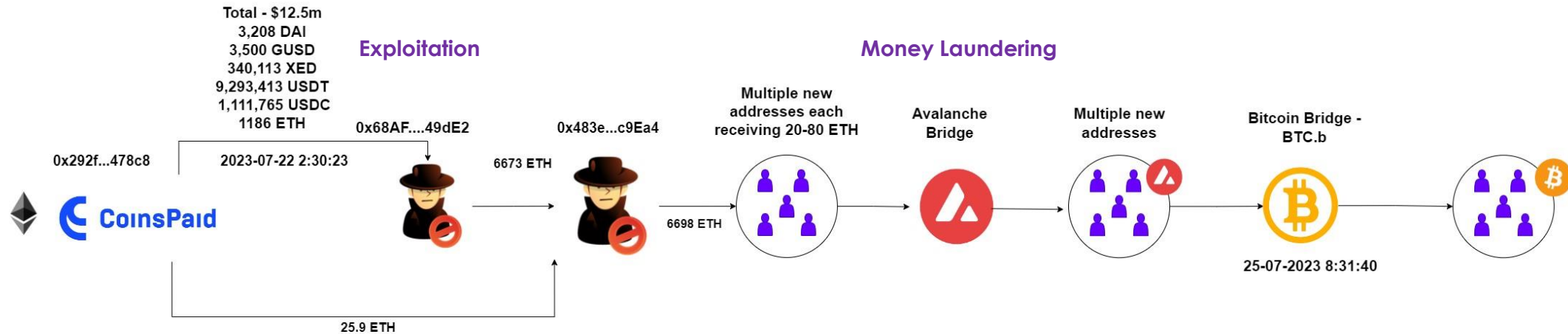
July 22, 2023.

Hackers withdraw \$37M from CoinsPaid hot wallets



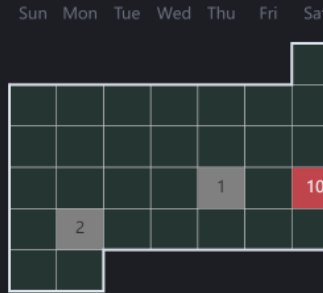


 **Total loss on ethereum:**
~12.5M \$





July 2023



Search by Tx / Address

- High** Tx hash: 0x04ff...d4d9 Suspicious address: 0xb118...49c0 Detection time: 22-07-2023 06:55:35 Value lost: \$6,429.78
- High** Tx hash: 0x5b08...3074 Suspicious address: 0xb118...49c0 Detection time: 22-07-2023 05:14:47 Value lost: \$25,530.01
- High** Tx hash: 0x0b67...1a7d Suspicious address: 0xb118...49c0 Detection time: 22-07-2023 04:39:11 Value lost: \$7,564.44
- High** Tx hash: 0xd845...dfb4 Suspicious address: 0xb118...49c0 Detection time: 22-07-2023 03:50:47 Value lost: \$9,455.56
- High** Tx hash: 0x14b7...70de Suspicious address: 0x68af...9de2 Detection time: 22-07-2023 02:36:23 Value lost: \$3,208.42
- High** Tx hash: 0xeb74...b6ab Suspicious address: 0x68af...9de2 Detection time: 22-07-2023 02:36:11 Value lost: \$3,499.23

- 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 Alerts @CyversAlerts

ALERT 📷 On July-22 Cyvers AI-Powered Threat Monitoring Platform detected 2 private key leakage attacks on @coinspaid and #Alphapo conducted by the same entity, funds were bridged to Avalanche and to the final destination, Bitcoin. Have a look at the screenshots from our system

The screenshots show a detailed transaction flow diagram for 'Alphapo and Coinspaid Private Key Leakage Attacks'. The diagram illustrates the flow of funds from initial transactions through various bridges (Avalanche, Bitcoin) to final destinations. Key events include 'Alphapo First Attack Transaction' on 22-07-2023 02:20:09 AM +UTC, 'Coinspaid Hacker Bridge to Avalanche' on 24-07-2023 03:27:35 AM +UTC, and 'Alphapo Hacker Bridge to Bitcoin' on 22-07-2023 08:20:18 AM +UTC. The dashboard on the right displays various metrics, charts, and a list of transactions.

Cyvers Alerts @CyversAlerts

ALERT 📷 Cyvers AI-Powered system has detected suspicious transactions on Alphapo.eth 0x6dfc34609a05bC22319fA4Cce1d1E2929548c0D7 Suspicious address has received \$100M in 7 transactions. Attacker: 0x040a96659fd7118259EBCD547771f6eCb9580d17 Private Key Leakage? [#CyversAlert](#)

10:43 PM · Jul 22, 2023 · 14K Views



Thank You
for your time

