Freeze Asset Request

Example

Last Updated: August 2023

Freeze-Asset Request

01: FUND LOCK REQUEST SUMMARY

Based on the evidence of this report, we request that the following addresses have their digital assets frozen:

0x2C40ce8D12dB859C3197BCe60fB128e5fceaD9E6
- Chain: Ethereum
- Sent: 137 ETH into the Binance wallet 0x09..B7

02: PROOF OF CRIME

(Provide description and evidence that the digital assets were stolen in a crime.)

What Happened? (1 sentence):

Upbit experienced a large transaction of 342K ETH (approx. $48.1 million) that went out from the exchange wallet to an alleged attacker wallet.

Details:

- **Total Value Lost (in USD)**: *$48.1 million USD*
- **Digital Assets taken**: *342,000 ETH*
- **Victim Protocol (type)**: *Upbit (CEX)*
- **Crime Date**: *2019-11-27*

This is a Crime Because:

- The attacker stole the private key of the exchange to transfer money to themselves from the exchange. This money did not belong to them.
- The Upbit team reported the transfer as a security breach the following day

Evidence:

—

ITEM: On-chain transaction

Chain: ETH

Transaction:
https://etherscan.io/tx/0xca4e0aa223e3190ab477efb25617eff3a42af7bdb29cdb7dc9e7935ea88626b4

What does this prove?

Security breach resulting in funds of 340,000e being transferred from the Upbit exchange wallet (0x5E032243d507C743b061eF021e2EC7fcc6d3ab89) to the attacker wallet (0xa09871AEadF4994Ca12f5c0b6056BBd1d343c029)

—

ITEM: Public announcement

https://upbit.com/service_center/notice?id=1085

What does this prove?

Proves that Upbit considered this transfer a theft, caused by the attacker stealing Upbit's private keys.

03: TRACE OF STOLEN ASSETS

(Provide description and evidence that stolen digital assets moved from the criminal to the exchange or organization that can freeze the assets.)

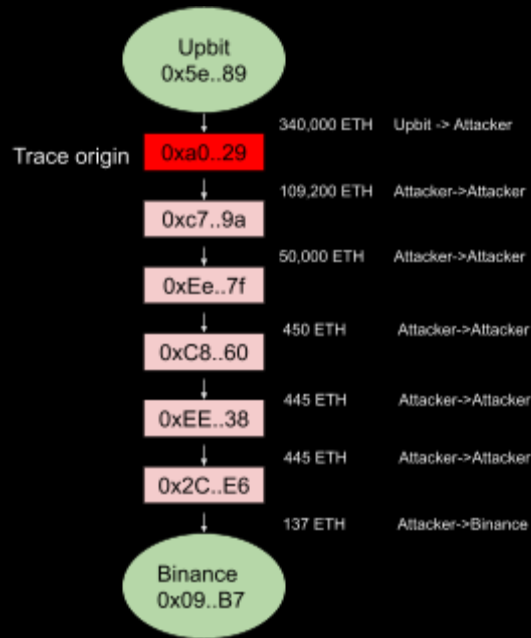The following image details the entire flow of digital assets for the incident

340,000e transferred from Upbit exchange wallet (0x5E032243d507C743b061eF021e2EC7fcc6d3ab89) to attacker wallet (0xa09871AEadF4994Ca12f5c0b6056BBd1d343c029)

First the attacker successfully steals money from Upbit 0x5e..89 and puts the stolen funds into 0xa0..29. After that the attacker moves the money to different attacker-controlled wallets to obfuscate funds (0xc7..9a, 0xEe..7f etc) until finally trying to move money from their 0x2C..E6 into the Binance wallet 0x09..B7.

Diagram

Upbit
0x5e..89

↓ 340,000 ETH   Upbit -> Attacker

Trace origin   0xa0..29

↓ 109,200 ETH   Attacker->Attacker

0xc7..9a

↓ 50,000 ETH   Attacker->Attacker

0xEe..7f

↓ 450 ETH   Attacker->Attacker

0xC8..60

↓ 445 ETH   Attacker->Attacker

0xEE..38

↓ 445 ETH   Attacker->Attacker

0x2C..E6

↓ 137 ETH   Attacker->Binance

Binance
0x09..B7

Transactions:

[Upbit -> Attacker]

[Attacker -> Attacker]

[Attacker -> Attacker]

[Attacker -> Attacker]

[Attacker -> Attacker]

[Attacker -> Attacker]

[Attacker -> Binance]

04: ADDITIONAL INFORMATION

(Provide speculative evidence about the attacker's identity, next moves, other ongoing or pending investigations, or anything else relevant to the request to freeze assets.)

None.

05: REPORTING & VERIFICATION

Reported By

- **Full Name**: *John Smith*
- **Email**: *johnsmith@jimbo.com*
- **Phone**: *+1 (555) 123-4567*
- **Country**: *United States*

Police Report

A police report is necessary for the incident request to be considered

- **Police Department Name and Address**: Silverwood Police Department (24 Maple Street, Silverwood, USA)
- **Country**: United States
- **Report ID or Reference Number**: PD-2023-XYZ789
- **Point of Contact**: Officer Mark Johnson
- **Email**: markjohnson@silverwoodpd.com
- **Phone**: +1 (555) 123-4567

Verified By

- **Organization Name**: CertiK
- **Date of Verification**: 2023-07-03
- **Point of Contact**: Brian Lee
- **Email**: brian.lee@certik.com
- **Phone**: +1 (555) 123-4567
- **Country**: United States
- **Comments**: None