Assignment 3

Computing Technology Innovation Project - COS30049

Members:

Nguyen Nam Tung 103181157

Xuan Dat Le 103487949

Abdullah Al Taskin 103793044

Table of Content

1. Introduction

In these modern days and ages, blockchain and cryptocurrency have become one of the most popular technology sections, offering endless innovative financial solutions and opportunities. However, with its increasing popularity and adoption, the security of those digital assets has also become a critical concern. As a result, this report will delve deep into a practical scenario within the realm of blockchain and cybersecurity, which is the analysis of a security breach incident that occurred at Deribit Exchange. Several mitigation measures and remediations will also be proposed to resolve the risks associated with the incident.

2. Incident Overview

2.1. Company Background

Deribit is one of the most popular companies in the cryptocurrency derivatives market, providing a range of offerings, including futures, perpetual swaps, and options for both Bitcoin and Ethereum. Additionally, the platform allows the trading of various other digital currencies, using USDC as collateral (Lielacher, n.d.).

Known for its professional trading interface, the exchange has gained popularity due to its high liquidity and minimal trade latency, establishing itself as a leading destination for crypto options trading. However, unlike several regulated crypto derivatives exchanges, Deribit operates in an unregulated space, which may pose regulatory concerns in the future. (Lielacher, n.d.)

2.2. Summary

The security breach at Deribit Exchange marked a significant event in the cryptocurrency landscape. This incident happened when an unknown cyber attacker successfully gained access to Deribit's infrastructure, compromising the security of the exchange's hot wallets. The consequences were profound, leading to the unauthorised withdrawal of cryptocurrencies with the value of 28 million dollars from these wallets (Somraaj, 2022).

2.3. Date and Time of the Incident

The incident took place on November 1, 2022, with the discovery of the breach occurring on the same day, which set off a chain of events that required critical attention and response.

2.4. Main Entities

There are two main entities involved in this incident:
Deribit Exchange: Deribit Exchange is a well-established cryptocurrency exchange platform known for its focus on cryptocurrency derivatives, including options and futures. It provides a marketplace for traders to execute digital asset transactions.

The attacker: The identity of the attacker remains unknown at this point. Their activities compromised the security of Deribit's hot wallets, leading to the unauthorised withdrawal of cryptocurrency funds.

2.5. Nature of the Suspicious/Illegal Activity

During the Deribit Exchange incident, the attacker exploited vulnerabilities within Deribit's infrastructure, gaining unauthorised access to the exchange's hot wallets. Subsequently, they executed transactions with the clear intention of withdrawing cryptocurrencies from these wallets without the requisite authorization.
These unauthorised actions not only violated established security protocols but also constituted a breach of legal standards. The consequences were substantial, resulting in the loss of digital assets and a significant decline of the exchange's standing and credibility within the cryptocurrency community.

3. Incident Details

A total sum of $28 million, which was seized during the incident, was divided among Bitcoin (BTC), Ethereum (ETH), and the stablecoin USDC. These assets remained dormant until November 5th, when they started being funnelled into the cryptocurrency mixer known as Tornado Cash, as reported in Deribit Insights in 2022.

In accordance with Somraaj's findings from 2022, the cybercriminal made off with 691 BTC and 9,111.59 ETH, comprising 6,967 ETH and 3,412,950.9 USDC, which were swiftly converted into Ethereum.

Deribit’s hot ETH wallet address: *0x58f56615180a8eea4c462235d9e215f72484b4a3*
Hackers ETH wallet addresses:

- *0xb0606f433496bf66338b8ad6b6d51fc4d84a44cd*
- *0x8d08aad4b2bac2bb761ac4781cf62468c9ec47b4*

Hackers BTC wallet addresses:

- *bc1q2dequzmk5vk8nmmrata8nq4y0zgqn4vc0n2h8y*
- *bc1qw5g8lw4kzltpdcraehy2dt6dqda8080xd6vhl4kg4wwsypwerg9s3x6pvk*

3.1. Tornado Cash

Tornado Cash provides a method for users to obscure their Ethereum transactions by employing a system of "pools" governed by smart contracts. These pools can be likened to banks that do not maintain individual records for each depositor but ensure that withdrawals do not exceed deposits.

Various pools have specific criteria for the type and quantity of tokens they accept. For example, one pool might exclusively accept deposits in increments of 0.1 ETH, while another could accommodate 100 ETH deposits. Since users depositing the same amount direct their ETH to the same pool, tracing the precise source of a withdrawal becomes a challenging task. All transactions are segregated into four distinct pools based on values: 0.1 ETH, 1 ETH, 10 ETH, and 100 ETH. Tornado Cash mixes the funds of different users and distributes the transaction into the pool storage with transactions of equivalent values from all users, making it intricate to connect an input transaction to an output transaction. This complexity adds to the difficulty of tracking stolen funds back to their origin, as noted by Arkham in 2023.

The Tornado Cash Mixer stack comprises the following components:

1. Web interface: The frontend of the decentralised application (DApp) provides user-specific buttons for interaction.
2. Relayer: This server retransmits transactions for users to safeguard on-chain nodes from privacy-sensitive data such as IP addresses, thereby enhancing user privacy.
3. Contract: It includes a Tornado.Cash Proxy contract that directs transactions to the appropriate Tornado pool based on the deposit or withdrawal amount. Presently, there are four pools catering to different deposit amounts: 0.1, 1, 10, and 100 ETH.

The user initiates a deposit or withdrawal through the Tornado Cash interface. The Relayer subsequently forwards this transaction to the Tornado Cash Proxy contract on the blockchain. This contract then directs the transaction to the relevant pool based on the amount, ultimately completing the deposit or withdrawal operation.

4. Transaction Analysis and Visualization

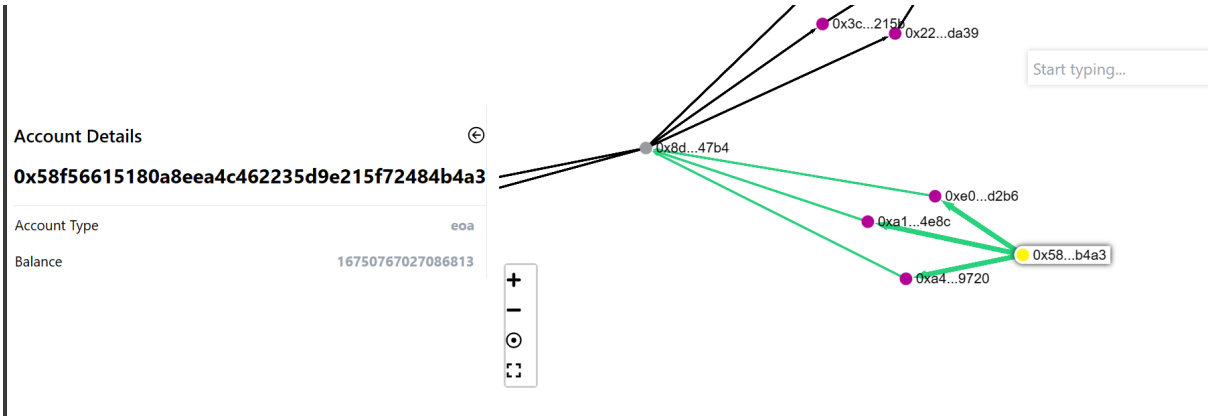

Figure 1: Transactions from Deribit's address to Hackers' first address

As the figure has shown, there are 3 transactions from the Deribit's address to the first address of the hackers.

The initial transaction took place on **Wed Nov 02 2022 10:57:11 GMT+1100 (Australian Eastern Daylight Time)**. During this transaction, 6,947 ETH was transferred from Deribit's hot wallet to the first address of the hackers, which can be identified as 0x8d08aad4b…68c9ec47b4. Subsequently, two additional transactions

occurred within two hours of the first one, involving 0.65 ETH and 20 ETH, respectively.

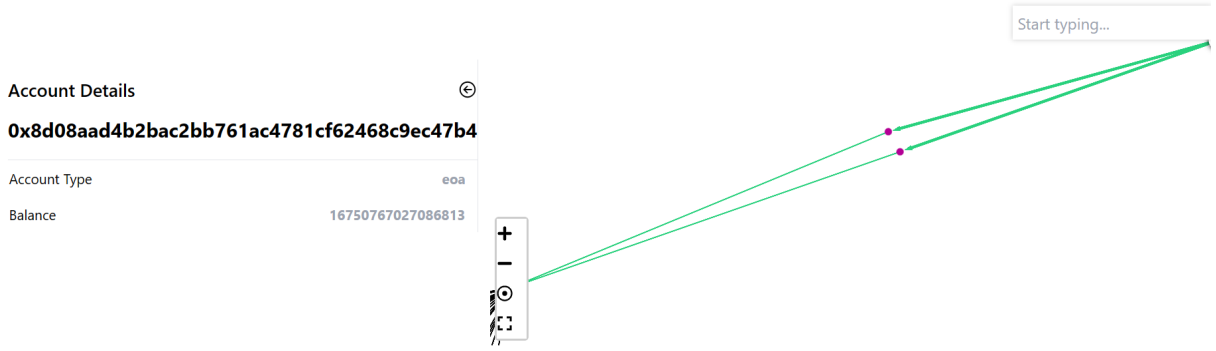

Figure 2: Transactions from hackers' first address to the second one

As it can clearly be observed through the given image, a total of both ETH and USDC amounting to 9,111.59 ETH were transferred to the second wallet at the address 0xb0606f…4d84a44cd. This transfer occurred through two separate transactions:

1. The first transaction involved 9,080.19 ETH and took place 30 minutes after the initial transaction from Deribit's wallet.
2. The second transaction, involving the remaining balance of 31.4 ETH, occurred 7 hours after the last transfer from Deribit, specifically at 8 a.m. on the following day.

Both of these transactions contributed to the accumulation of 9,111.59 ETH in the second wallet.

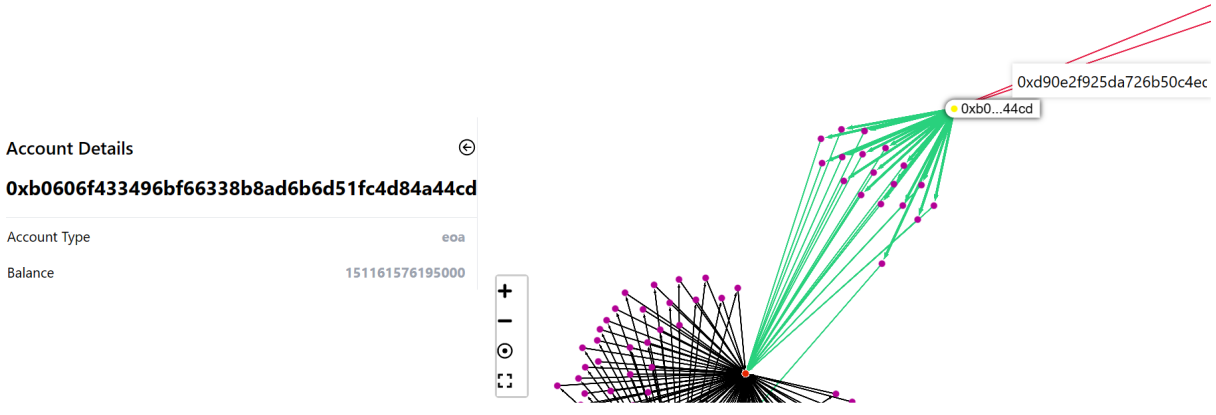

Figure 3: Transactions from the second Hackers' account to the Tornado Mixer

On November 5th, the stolen amount was funnelled into Tornado Cash. The transfer involved the following:

1. The hackers directly sent 1,610 ETH to the Tornado Cash smart contract through over 17 individual transactions.

2. The remainder of the stolen funds, which amounted to 7,499 ETH, was sent through an intermediate wallet with the address 0x3089df0…da10fe2d. This transfer was accomplished over the course of 3 hours and comprised a total of 92 individual transactions.

These actions were taken to obfuscate and mix the stolen funds through the Tornado Cash service, making it more challenging to trace their origin and ownership.

We can observe that all transactions sent to the Tornado Cash Mixer consist of 1 ETH, 10 ETH, or 100 ETH denominations. Additionally, these transactions include input data specifically designed for the Tornado smart contract. By utilising the provided Python code, we can gain a better understanding of this input data and its purpose.

```
web3 = Web3("https://mainnet.infura.io/v3/6725306487624c2e8da91c6f255f7865");

# Transaction hash you want to analyze
tx_hash = '0x1d05c33a840e11c887622934f1805f9bd32f32c6c0441c4b7c6f04953bfcb72d'

# Retrieve transaction information
tx = web3.eth.getTransaction(tx_hash)
```

Figure 4: Python code to get the transaction by Ethereum Node

```python
if tx:
    # Get the contract address and input data from the transaction
    contract_address = tx['to']
    input_data = tx['input']

    # Use Etherscan API to get contract ABI
    etherscan_api_key = 'input with appropriate API' # Change this accordingly to get the appropriate API
    abi_endpoint = f"https://api.etherscan.io/api?module=contract&action=getabi&address={contract_address}&apikey={et

    # Make a request to Etherscan to retrieve the ABI
    response = requests.get(abi_endpoint)
    abi_data = response.json()

    if abi_data['status'] == '1':
        abi = abi_data['result']
        contract = w3.eth.contract(address=contract_address, abi=abi)

        # Decode the function input
        func_obj, func_params = contract.decode_function_input(input_data)

        print(f'Function Object: {func_obj}')
        print(f'Function Parameters: {func_params}')
    else:
        print('Failed to retrieve contract ABI from Etherscan.')
else:
    print('Transaction not found.')
```

Figure 5: Get the transaction by Ethereum Node and Etherscan to get the ABI contract

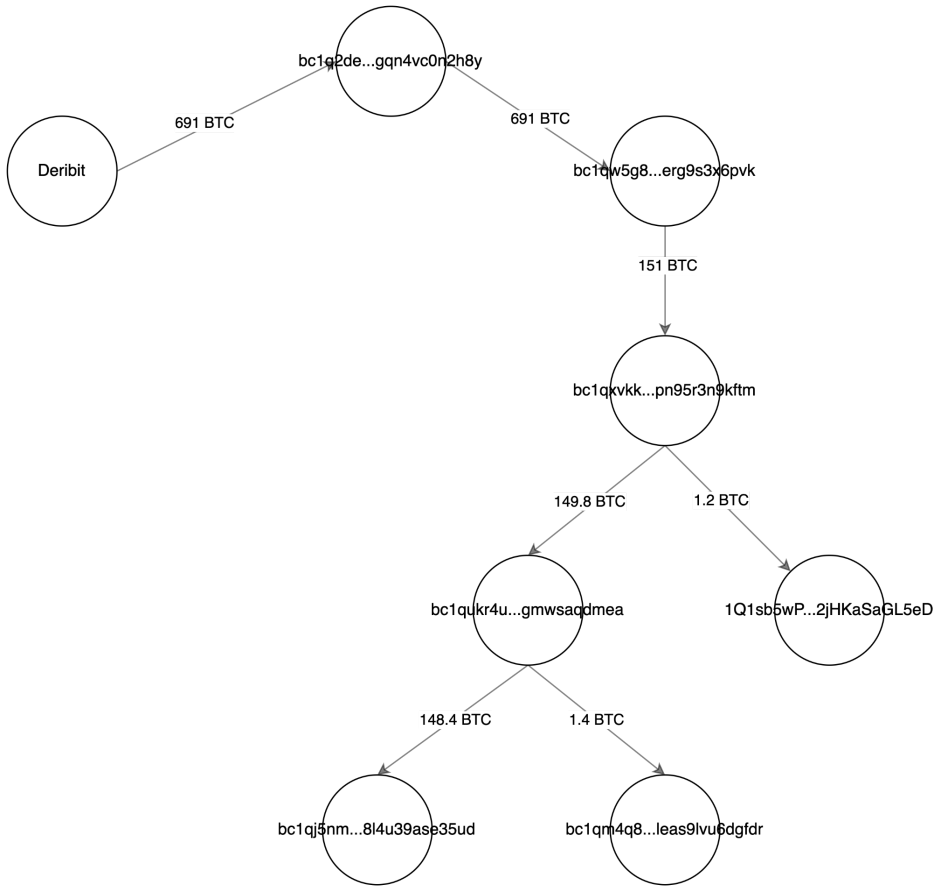

Figure 6: BTC transactions flow

The stolen BTC is currently spread across multiple wallets controlled by the hackers as of October 2023. Specifically:

1. 691 BTC was initially moved from Deribit's wallet to the address bc1q2dequzmk…y0zgqn4vc0n2h8y through 131 separate transactions. From there, it was further transferred to bc1qw5g8lw4kzltpd…wwsypwerg9s3x6pvk.
2. A total of 151 BTC was sent to the address bc1qxvkkl39…pkctpn95r3n9kftm and subsequently forwarded to several other addresses.
3. The remaining 540 BTC is currently held in the address bc1qw5g8lw4kzltpd…wwsypwerg9s3x6pvk.

This distribution strategy is being employed to obscure the origins and ownership of the stolen BTC.

5. Mitigation Measures and Remediations

In response to the security breaches like Deribit Exchange, a comprehensive strategy can be implemented to address the risks associated with suspicious and illegal activities.

5.1. Mitigating Risks Associated with Suspicious/Illegal Activity

Intermediate Incident Response

The first and foremost step is to take fast and decisive action. This includes suspending affected systems and accounts immediately to prevent any further unauthorised activities. This limits the scope of the breach and reduces potential financial losses. In the case of Debirit Exchange, right after the security breach, Deribit took immediate security measures, which, as a precautionary step, involved the temporary suspension of all withdrawal activities, including connections to third-party integrations such as Copper Clearloop, Cobo Loop, and Banxa. Additionally, new client verifications through external applications were also temporarily halted (Deribit, 2022).

Forensic Investigation

A thorough forensic investigation can be conducted to determine the extent of the breach. This involves identifying the entry points used by the attacker and any vulnerabilities exploited. Deribit has engaged the services of three expert firms to support the investigation of the security breach. (Deribit, 2022). This could help gain

insights into the tactics employed by the attacker to understand the methods and to prevent future incidents from happening.

5.2. Ongoing Monitoring and Remediation

Transition to Fireblocks

Deribit executed a strategic migration of its entire hot wallet setup to Fireblocks, encompassing BTC, ETH, and USDC, in addition to SOL, which was already integrated with Fireblocks. The transition process was conducted meticulously, ensuring that outdated hardware or technology was not utilized for the new configuration. This move provided Deribit with a fresh and secure foundation for managing hot wallet assets (Deribit, 2022).

Manual Confirmation for Withdrawals

As part of the heightened security measures, all withdrawal transactions now mandate manual confirmation by an administrator. While this adjustment may result in slightly extended withdrawal processing times, it introduces an additional layer of security and oversight to safeguard user assets (Deribit, 2022).

Continuous Threat Monitoring

Cryptocurrency platforms can implement real-time monitoring systems, which enables the rapid detection of suspicious activities and potential security threats. These systems closely monitor network traffic, system logs, and user activity, substantially reducing the risk of cybersecurity attacks.

Regular Security Assessment

Ongoing security assessments can be utilised to identify the potential weaknesses and vulnerabilities that could be exploited by criminals. This includes performing routine comprehensive security assessments and engaging in multiple penetration testing to simulate various attack scenarios, thereby enhancing the security systems for cryptocurrency platforms

5.3. Strengthening AML Processes and Control

AML (Anti-Money Laundering) processes and controls encompass the guidelines and actions established by organisations to detect money laundering, terrorist financing, and other financial misconduct. They are implemented to ensure that financial institutions and businesses adhere to legal and regulatory obligations and maintain the stability of the financial system (Corporate Finance Institute, n.d.).
To enhance AML processes and controls, there are several steps that can be taken:

Legal and Regulatory Compliance

In terms of legal and regulatory compliance, it's crucial to stay updated on the ever-evolving AML regulations and guidelines in the cryptocurrency industry, as these regulations may change over time. As a result, an effective way to enhance compliance is by designating a compliance officer. This individual will be responsible for monitoring and ensuring strict adherence to AML regulations, with a particular focus on those specific to the cryptocurrency sector. Their expertise in AML rules will play a key role in upholding the platform's commitment to regulatory compliance.

AML Training and Education

Prioritising AML training and education is a crucial element of a robust security strategy. This involves comprehensive employee training to equip them with skills and abilities to recognize AML red flags, understand the company's AML policies, and report any suspicious activities. Additionally, educating customers about AML requirements, their responsibilities, and the importance of adhering to AML regulations is also of paramount significance. This helps maintain the platform's security and integrity, therefore strengthening its cryptocurrency compliance.

AML Technology Integration

Cryptocurrency platforms can strengthen AML measures by integrating advanced technologies. Key components of this strategy involve the utilisation of blockchain analysis tools, which are instrumental in tracing the flow of cryptocurrency funds and identifying potentially suspicious activities, thereby enhancing overall security.

6. Conclusion

In conclusion, the Deribit Exchange security breach underscores persistent security challenges in the cryptocurrency industry. Unauthorised access and illegal withdrawals of cryptocurrencies highlight the need for strong security measures and protocols. Additionally, this incident also emphasises the significance of security monitoring, user education, and industry collaboration. Learning from this experience and proactively enhancing security practices will help bolster asset protection and user trust in this evolving landscape.

7. References

Lielacher, A. (n.d.). Deribit Review. [online] Investopedia. Available at: https://www.investopedia.com/deribit-review-5215948.

Somraaj, D. / S. (2022). Crypto Exchange Deribit Hacked for $28M in Bitcoin, Ethereum, USDC. [online] Decrypt. Available at: https://decrypt.co/113334/crypto-exchange-deribit-hacked-28m-bitcoin-ethereum-usdc

Deribit (2022). 1 November incident report and next steps. [online] Deribit Insights. Available at: https://insights.deribit.com/exchange-updates/1-november-incident-report-and-next-steps/.

Corporate Finance Institute. (n.d.). Anti-Money Laundering. [online] Available at: https://corporatefinanceinstitute.com/resources/career-map/sell-side/risk-management/anti-money-laundering/.