Report: Investigating Suspected NFT Scam and Identifying the Use of Fake Profiles

Introduction

This report details the findings of an investigation into a suspected NFT scam using blockchain analysis tools. The goal of the investigation was to identify the individuals or entities involved in the scam and provide recommendations for further action to prevent similar scams from occurring in the future. In particular, we focused on identifying the use of fake profiles by the scammers.

Tools Used

- During the investigation, we utilized several blockchain analysis tools, including Qlue, BitRank, Entity, and Chainalysis.

- Qlue was used to track and trace transactions on the blockchain. It allowed us to identify the flow of funds and any suspicious transactions.

- BitRank was used to assess the risk level associated with specific Bitcoin transactions and addresses. This provided us with a risk score that helped to prioritize our investigation and identify potential areas of concern.

- Entity was used to identify and track specific entities and individuals on the blockchain, including exchanges, wallets, and businesses. This helped us to identify any patterns or trends in transaction activity and any potential connections between individuals or entities.

- Chainalysis was used to trace and analyze specific blockchain transactions. It enabled us to identify any illicit activity, such as money laundering, terrorist financing, or other forms of financial crime.

Findings

Using these blockchain analysis tools, we were able to trace the transactions involved in the suspected NFT scam and identify the origin and destination of the funds. We identified multiple wallet addresses that were connected to the scam, including those associated with the scammers themselves.

Further investigation revealed that the scammers used fake profiles to promote their fake NFTs. The fake profiles were created using stolen images and personal information from real individuals. The use of fake profiles created a false sense of legitimacy and trust, which made it easier for the scammers to deceive their victims.
We also identified several individuals and entities that were most likely to be involved in the scam. The use of these blockchain analysis tools enabled us to identify complex transaction

networks and patterns of behavior that would have been difficult to detect using traditional investigation methods.

Recommendations

Based on our findings, we recommend that victims of the scam be notified of the fraudulent activity and be advised to take appropriate action to protect themselves. This may include canceling any transactions and reporting the scam to relevant authorities or consumer protection agencies.

Additionally, we suggest educating the public on how to avoid similar scams and how to identify red flags, such as the use of fake profiles. This may include raising awareness through social media, online forums, and other relevant channels.

Conclusion

The investigation into the suspected NFT scam has identified the individuals most likely to be involved in the scam and the use of fake profiles. The use of blockchain analysis tools, including Qlue, BitRank, Entity, and Chainalysis, enabled us to trace the transactions, identify potential fraudulent activity, and gather evidence to support our findings. We hope that our recommendations will help prevent similar scams from occurring in the future, and we encourage the continued use of blockchain analysis tools to identify and prevent fraudulent activity.