CLAUDIA

CUSTOMIZED KNOWLEDGE

COMPLIANCE REPORTING

Reporting Number: NR001 by the Compliance Desk.
Subject: Violation of "Code of ethical business behavior", Human Malevolence-attack (failure of responsibilities)
Incident: One governance parameter of DAO in testing is breached, "initclaudia" and ERC-20 token (CLD) at rinkeby in Aragon, ability without consensus.
Qualified: Natural Risk, Human risk.

Legal disclaimer: This is a compliance report from CLAUDIA´s Compliance Desk and it represents the experience of an incident management item with the response from the DAO and privacy respect for the old members of CLAUDIA. The term attacker is not, at any moment, considered in this report as offense to anyone, and it is limited for a generic analysis onto our incident mechanism responsiveness as elemental part of our minimal governance viability.

1. **ABSTRACT:**

Two members communicated to abandon the DAO in the last meeting. Transition process had consensus to start with.

Two phases, one per each member to give privacy and comfortability each of them with free will to decide their choice to abandon:

1. One of them managed two accounts at the reference DAO in testing
   0xa82B8fBFcE642128da94B79D98489F8d0382Ef26
   0x39ad97EbcEbC6Fb8c54C41B6f2162de8500B5fF0

2. The other manage one account at the reference DAO in testing
   0xEaB479C6625C4c4220a29e787C39F908f69e4810

The one who managed two accounts, one of the accounts was, formerly, authorized to perform events with various permissions and abilities. Note that one of the events that the malicious member wanted to do was rejected on 13th October 2019 (voting #20). This member did not respect the last meeting decisions and was doing on the member own with malicious actions on the DAO in testing. Various controversial and malicious actions on the DAO were unilateral performed over reference accounts ***0x229d09145c2D5d586fD2208036AdF06165b5ab25*** ***and 0xE15a1b7711F267607bAdeA7b41476Ae3903E8dF3*** which belongs to the Compliance department and CEO´s department of CLUADIA, this activity was getting under management control by the malicious member taking advantage of the Grants ability with the Role "Mint Tokens" and the ACL and revoked the member´s responsibility over

0xa82B8fBFcE642128da94B79D98489F8d0382Ef26 which was formerly the control agent at the DAO for that role. This decision was not agreed in the meeting for transition.

28th November 2019 DAO in testing was unilateral manipulated by the malicious member with success for the action which conclude within eleven minutes approximately.

Compliance department determined a "Prudential Measurement" and suggested to do not treat malicious member with revenge and allow member´s free will to complete member´s pretension. Suddenly member´s action involved the other exit member and complete the deletion correctly from the DAO in testing. Thanks to the traceability and immutability of the Blockchain where the DAO is in testing, CLAUDIA´s Compliance Department has identified interesting recommendations to take in place in the Governance of CLAUDIA about invoking Smart Contracts.

2. GOVERNANCE ANALYSIS:

a. Off-Chain:

One member in the off-chain was concern for continuing the personal relationship and helping the DAO in the transition, and the process was completed with fairness and respecting the "Code of ethical business behavior" signed by the member. CSO was the role of responsibilities within CLAUDIA.

The other member vaguely took care about the transition and did not take care about the DAO in testing hence confirmed that the member took by member´s own the decision to destroy the DAO in testing because he was the controller of the permissions, and it was his decision to do not respect his words on the last meeting. The process is not completed with fairness and the "Code of ethical business behavior" signed by the member is not respected. CTO was the role of responsibilities within CLAUDIA.

Compliance department signed termination for both members upon members' request, the documents with reference digital-asset evidences on Blockchain respectively are:

- ***d0c774fa1ae742dd1d714b69d9cfd04ff7fbdaf162c072fad57e17f6bf9a25d3*** for the CTO
- ***9145c2daae4ee9d3f92a463ed11f6dae6a8e7e76bb16249d50b254368f94867c*** for the CSO.

Whereas CLAUDIA as Startup the inception was incubated at University Program, respectful from the DAO was a principle and both members did as they wish to leave the CLAUDIA.

Whereas both members had responsibilities to deploy departments which are fundamentals for CLAUDIA.

Compliance department reacted with minimal damages for CLAUDIA although the relevance of the members for CLAUDIA are missing by the others, the community demonstrates robustness reorganizing the handling, controlling and management of both departments for a proper driving. Activation of decentralization with the advisors and mentors were key elements to maintain great resilience to the incident.

b. On-Chain:

Within other DAO in testing, we have tried many times the same malicious activity with different proposes and it was implemented from the same manner at ACL in Aragon with success, hence we have learnt a process which it was the goal of the malicious member, CLAUDIA does not condemn the malicious member, moreover received the gift of the modus operandi to be included at the “sanctions and prudential guidelines” that was approved to elaborate for CLAUDIA in previous meetings.

The events descriptions are not against the continuation of the DAO since the malicious member just transmitted permissions to the stable members and revoked the permissions from the member´s ability. However, the events were not fair implemented with transparency in advance and it had burnt other member´s tokens which imply that both exit members were under consensus because no complaint were announced to the CLAUDIA.

However, some relevant details are interesting to analysis within the on-chain activities, as we have known and tracking the rinkeby testnet (Ethereum), interesting discoverability had happened to take in consideration and recommendations in this Compliance Reporting:

1. The malicious activity was consummated with different events that had to be consecutively performed. The good faith disappears from the scenario at any moment because of the off-chain confirmation by the member.
2. The tool for Mint Tokens in Aragon has got a powerful ability to perform this kind of actions which can be interoperated also as embargo for Agents of the DAO for non-ethical behavior.

3. There is a breach of responsibilities with the trick that the malicious member made on the DAO in testing, because the deletion of the member by the member itself diluted the responsibilities in a black box space; on the other hands average and ratings on the DAO in the Aragon has to be very critical for the evolution thus why it is very important to understand in advance the configuration of the DAO and such parameters will determine the voting process of the decision making and participation.
4. Unilateral actions on a DAO in Aragon were performed which is in contradiction with the essential of the DAO and it is a clear approached by the two members agreement, with which one of them manipulated the other to perform the first action to be approved and serving to consummate the rest of the pretended events on the DAO in testing.

Deep analysis is able on rinkeby at Ethereum testnet for anyone who wants to extract their useful conclusions.

c. Cross-Chain:

There were no consequences for cross-chain due to the status quo of testing about the DAO that suffered the attack by the member.

3. ACTIONS:

During the attack:

No actions except observation were taken by CLAUDIA.

Actions took by the attacker:

1. Got the ability with advance in enough to proof and never trained the members about that, as part of the member´s responsibilities (voting#1 and voting #14). Authority enough to do it.
2. Burnt tokens from members' accounts. Authority enough to do it.
3. Gave permissions and ability to perform actions of role "Mint Tokens" to the remained members. Authority enough to do it.
4. Revoked its ability to perform actions of role "Mint Tokens". Authority enough to do it.
5. Burnt 5300000 (CLD) tokens from attacker account. (Vote #32). Authority enough to do it.

CLAUDIA

CUSTOMIZED KNOWLEDGE

Upon the 19th November 2019 minutes was approved by the DAO the attacker burnt 600000 (CLD) tokens from the DAO in testing which belongs to the members of DAO (one of them was attacker account), on 28th November 2019 started the attacked on-chain at 17:05 UTC (voting #27) and took 11 minutes interventions until 17:16 UTC.

Note by Compliance desk: appointed a note to calculate time of response and pretensions of attacker, but are not relevant due to the benefits obtains by the attack itself for CLAUDIA. And barriers over CLAUDIA were taking in place 19th November 2019 after the last regular meeting.

Post-attack:

No actions or events have been registered and good finance rate on the apps of the DAO in testing. Preliminary guidelines for Governance are under elaboration with Prudential Events and Responsibility definitions for roles.

Reputation is naturally neutralized because of the nature of the DAO, "in testing", whereby not all the attributes of CLAUDIA were implemented on that DAO in testing.

Due that the propose of that DAO in testing was precisely learning about the ACL and the Mint Token role and due to the malicious action, the goal of the testing DAO was achieved although in a non-orthodoxly way.

Which is the cause?

Human personality is the response that we have concluded in the Compliance department. There was no other intention behind the member, human beings are different made by the same material and personality has got different motivations and ingredients to perform events and actions that reflect our pureness and personality in essence. Attacker took advantage of its ability and permissions that the DAO in testing was agreed to be under member´s control and responsibility so the member was able to do it since the beginning and at the end all these rights or abilities were transmitted correctly to the other members which shall remain in CLAUDIA with no damage except off-chain and personal relationship.

The cause it was not the technology and the functional components used on the processing, technology did not fail, but it was the vehicle used to make a unilateral decision that affects other members without previous communication, lack of legitimacy for the authority and ability of the member´s rights, position abuse and violation of the "Code of ethical business behavior" of CLAUDIA.

4. CONCLUSIONS:

First conclusions are learnings, technical learnings and governance learnings which have to be applied in a DAO to maintain resilience and robustness against the demotivation, jealousy or other capitals sin that can arise selfishness or personality fears.

In resume:

a) Technology did not fail.
b) Violation of principles: Responsibility, Transparency, Loyalty and integrity (1, 2, 3, 4 of "Code of ethical business behavior", respectively)
c) No further actions will be taking by CLAUDIA. DAO in testing will be transformed and/or continuing testing with different experimentation.
d) No retaliation.

Final conclusion is that technical transition of members is completed and incident autonomously resolved within the registry of CLAUDIA. Pending some material.

We are CLAUDIA and our values and principles are part of our DNA we know working in a project is not a reason to disqualify any of our members, either exit members of our DAO, we thank them for their contributions during our common journey we are sure values are same and adventures different, but we are CLAUDIA and the project is more responsible than ever with the community and with technology so this are the result of this piece of our story in 2019.

Published by the Compliance Desk