Hello Maker Community,

I was recently approached by a new community member, @compacter7366

, via Discord. They claimed to have evidence of an operational security breach involving the Aligned Delegate @truename.

Endgame Edge has implemented a protocol to protect the sensitive information of ADs. We requested that the informant and the AD establish a secure communication channel so that the evidence could be presented and discussed privately. After the evidence was sent to True Name, the AD asked us to review the evidence and apply our judgment to evaluate the situation.

The evidence, sent to me, consisted of on-chain transactions that showed a multisig, set up by True Name, that contained a signer who was also a signer of the multisig of one AVC Member, ACRE DAOs.

I involved @JanSky and @ldr to assist with the investigation, and we confirmed that the evidence was accurate. We verified that:

- The multisig was created by True Name's EA address on 7/4/2023.

- The signers of the multisig were True Name's EA address and one of the current signers of ACRE DAO's multisig.

- On the same day, 10 MKR were received from Coinbase and delegated to True Name.

- On 8/16/2023, the MKR were undelegated and transferred to Coinbase.

- The address was removed as a signer of the multisig by True Name's EA address on the same day the whistleblower sent the evidence to the AD.

- The signer shared by both multisig wallets was recently added to ACRE DAO's multisig on 2/2/2024.

We then asked True Name and ACRE DAOs to provide explanations. The explanations we received indicated that an external entity related to the AVC member, contacted the AD, offering to delegate MKR and asking True Name to set up a multisig where both could be signers. We verified that this multisig was indeed used to receive MKR and self-delegate it to True Name.

MKR delegation can be done completely anonymously and permissionlessly. There was no need for True Name to set up a multisig and handle MKR from an MKR holder. True Name should have been more cautious, as this is at least an operational security error or a failure to follow best practices. Under MIP101 Section 2.6.6, this situation requires the facilitator to immediately derecognize the AD. We also believe that this behavior could be considered against MIP101 Section 2.6.5.

At the time True Name created the multisig to receive the MKR, the sections of the Atlas were different, but the spirit of the sections was similar. For instance:

Section 2.6.5:

ADs are generally not allowed to engage directly with Ecosystem Actors and other counterparts to the DAO, or engage in other operational activities. They must remain focused on their job of using their physical voting power over the protocol to safeguard its alignment. Additionally, they must publicly provide governance information and research material to AVCs and can interact with ecosystem participants for this purpose. They are also not allowed to provide 'kickbacks' from their compensation to MKR holders that delegate to them. Any violation of these requirements constitutes breaching the Alignment Conserver requirements.

Section 2.6.6.1:

FacilitatorDAOs must err on the side of caution and act in case there is any kind of real possibility that the privacy of an AD is compromised.

Section 2.6.5.1:

If a FacilitatorDAO finds that an AD has performed a misaligned act or breached their requirements, they can derecognize the AD and confiscate their AD Buffer. The AD Buffer can be used as a whistleblower bounty in case an ecosystem actor provided useful data, information, or evidence that led to the derecognition of the AD. GOV6 must specify sufficient safety mechanisms around the payment of the whistleblower bounty.

However, as the purpose of these sections is to protect the protocol, we interpret that they must be applied retroactively in their current status

. This is because if the operational security of the AD was compromised before the introduction of the rule, it creates the same harm as if it were compromised afterward, resulting in an AD with poor operational security.

After carefully discussing the situation and considering the on-chain evidence and explanations from both parties, we (JanSky, Ldr, and VoteWizard) have unanimously decided that the situation warrants the derecognition of True Name.

We have also decided to issue an [official warning](#) to ACRE DAOs, as the address added as a signer to True Name's multisig was also a signer of ACRE DAOs' multisig. We have received and understood their explanation, which mentioned that this is a different legal person and not the same entity as ACRE DAOs. However, the address was connected to ACRE DAOs as it was the singer of its multisig, and we do not want to set a precedent in which an AVC member can collaborate with an AD to set up a multisig to handle MKR for them.

Whistleblower Bounty

As per [MIP101 Section 2.6.6](#), part of the AD's buffer is designated as a whistleblower bounty to the informant, under specific conditions. We believe that these conditions have been satisfied, but we will provide confirmation in a subsequent post.

To conclude, Endgame Edge extends our deepest gratitude to [@truename](#) for their invaluable contributions to MakerDAO