Identifying Shadow Owners in Safe Multisig

Guide based onbartek.eth X threads:1 ,2 ,3

Introduction

In Safe multisig wallets, besides the "public" owners visible in the UI, there can be "shadow" owners. These shadow owners are authorized to execute transactions but are not listed in thegetOwners() method, making them invisible in the Safe UI. This guide will help you determine if there is suspicion of shadow owners in the multisig.

Understanding Owner Structure

Safe maintains an [address] -> [address] mapping where each owner's address points to the next owner's address or a 'sentinel' (a dummy address indicating the end of owners list). This setup allows additional storage where owner addresses pointing to non-zero values might not be visible in the Safe UI. Owners added through this additional mechanism do not appear in the standardgetOwners() list.

Pic. source:bartek.eth

Adding a Shadow Owner

Safe allows additional delegateCalls during:

- setup()
- call
- executeTransaction()
- call
- executeTransactionFromModule()
- call

Any of these calls can modify arbitrary storage slots and add a shadow owner. The transaction might call another contract that adds a new owner to the multisig.

Pic. source:bartek.eth

Although the Safe UI will warn about unexpected delegate calls, it is not always malicious but should be viewed with suspicion.

Pic. source:bartek.eth

Detecting Shadow Owners

You cannot see shadow owners in the UI or directly determine their addresses. However, you can check for "dirty" storage, which might indicate the presence of shadow owners. Here's how to do it:

1AccessToken Flow Database

A login is required to access the database.

2Login and Query

- Use this query:https://app.tokenflow.live/studio/editor/66c451806875f9a936d548c9
- . This query is to check Safe multisig on Ethereum.
- Enter the address of the Safe in the query parameter
- Click "RUN"

NB : The query might take a while to run.

3Analyze Results

Smart contracts use storage slots written according to a specific layout. Let's see Safe storage layout:

Pic. source:bartek.eth

When you analyze the results of the query:

- The first two columns (MEM_HASH
- ,RAW_LOCATION
-) show the "raw" storage slots as seen by the EVM .
- TheLOCATION
- column is a decoded storage slot derived from the Safe smart contract storage layout.
- Look for storage locations that could not be decoded using the known storage layout. Such storage must have been set directly by anSTORE
- assembly call, indicating "dirty" storage.

Example below:

Pic. source:bartek.eth

- To check the value of such “dirty” storage you can usehttps://storage-slots.swiss-knife.xyz/
- , select “custom”, enter the multisig address and the storage slot in to the form and hit query button:
- Alternatively if you havebrownie
- installed, enter following commands in the console:
- brownie console
- from brownie import web3
- web3.eth.get_storage_at("{multisig address}", "{storage slot}")
- Results should look like that:
- Or if you have Foundry installed, you can use the following command:
- cast storage {multisig address} {storage slot}
- note
- In Safe0x6c9a6c4a39284e37ed1cf53d337577d14212a4870fb976a4366c693b939918d5
- storage slot by default is used to storefallback handler address
- , you can read more about ithere
- and find this address in theofficial documentation
- .

Next Steps if a Suspicious Multisig is Found

If your analysis reveals suspicious activity within a multisig, follow these steps to ensure security:

For New Multisigs :

1. Do not accept the multisig
2. . If the multisig shows signs of suspicious activity or dirty storage, do not proceed with using it
3. Investigate
4. . Conduct a thorough investigation into the source of the multisig and those who proposed its use

For Existing Multisigs :

1. Migrate to a new multisig
2. .
3. If a currently used multisig is found to be suspicious, create a new multisig with the same set of public signers and transfer all assets to it
4. Identify malicious actors
5. . Investigate and identify any individuals responsible for the malicious transactions

By following these steps, contributors can maintain security, ensuring that only authorized owners have control.Edit this page Previous Guide to being a signer at any Lido DAO multisigsNext Checking the evm script from Aragon vote