Guild Audits

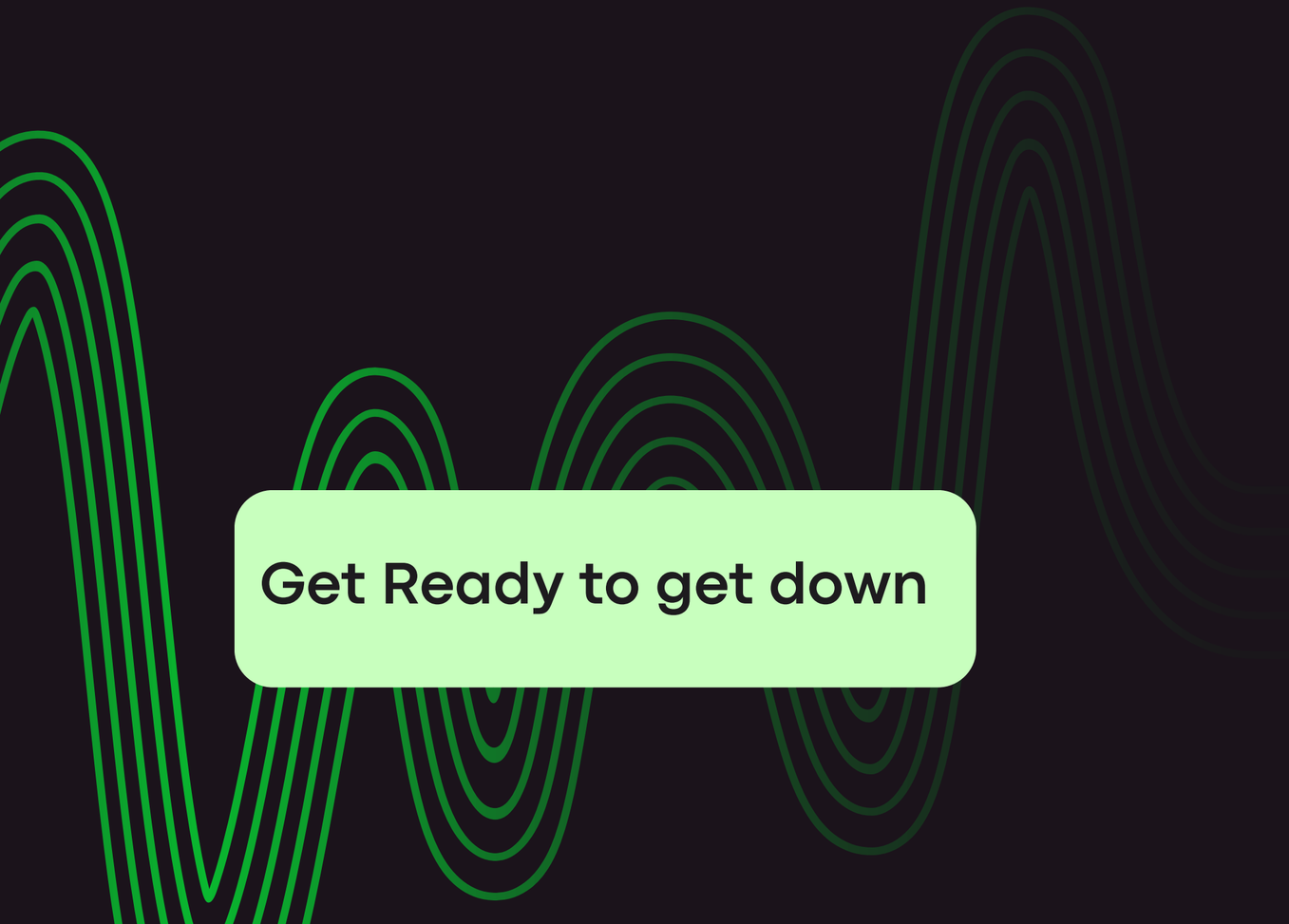
AN OVERVIEW AND ANALYSIS OF THE MIM-SPELL HACK

Reviewing how it went down , visualizing and getting into the mind of the hacker

Presented By @jaydhales @dev_pelz
@otaikisadiq @0xkenzman

MARCH 27TH 2024

AGENDA



Get Ready to get down

What is MIM-SPELL ? 3

Explaining Key-Words 5

The Attack 6

How it went Down ? 7

Code-time ! 8

Analysis and Mitigation 9

Conclusion 10

Guild Audits

What is MIM_SPELL ?

Abracadabra utilizes interest-bearing crypto assets as collateral to borrow its stablecoin, Magic Internet Money (MIM). It aims to provide users with a platform to leverage their assets into a stablecoin. With significant growth, $267.63 million total value locked, and an average APY of 15.58%, it's governed by its token SPELL and powered by Sushi's Kashi Lending technology.

MIM is created with yield-bearing assets, offering users a capital-efficient option to borrow stablecoins through whitelisted assets. It's a unique take on decentralized stablecoin design, providing users with a way to leverage their assets in a capital-efficient manner

Back to Agenda

Guild Audits

What is MIM_SPELL ?

MIM_SPELL is linked to the Abracadabra Money protocol, comprising Magic Internet Money (MIM) and SPELL tokens. MIM, pegged to the US Dollar, utilizes yield-bearing assets for collateral, offering capital efficiency. SPELL tokens act as the platform's governance token, granting holders governance rights and passive income through staking

Holding **SPELL** tokens also yields **sSPELL** tokens, which provide utility and earnings from the protocol. **MIM_SPELL** is commonly referenced in decentralized exchange trading pairs, where **MIM** and **SPELL** are exchanged against each other.

Back to Agenda

Explaining Key-Words

KeyWords you should take note of

ELASTIC VARIABLE

An elastic variable is one that responds significantly to changes in another variable

DEGENBOX

DegenBox is a strategic program created by Abracadabra Money. It's used to solve the issue of accepting non-interest-bearing tokens

ASSETS/ COLLATERAL

Assets in web3 refer to tokens , cryptocurrencies like ETH or BTC. Collateral on the other hand refers to digital assets users deposit to secure a loan (also tokens).

FLASHLOANS

Type of loan in the DeFi space where a user borrows assets with no upfront collateral and returns the borrowed assets within the same blockchain transaction

PRECISION AND ROUNDING

Precision concerns the closeness of measurements, assessing consistency. Rounding reduces significant digits for easier understanding and manipulation

CAULDRONS

In the context of Abracadabra Money, cauldrons refer to isolated lending pools on the Ethereum blockchain.

Magic Internet Money (MIM) is a stablecoin used in the Abracadabra protocol. It's backed by interest-bearing tokens (ibTKNs), making it a more capital-efficient option compared to other stablecoin designs

Back to Agenda

Back to Agenda

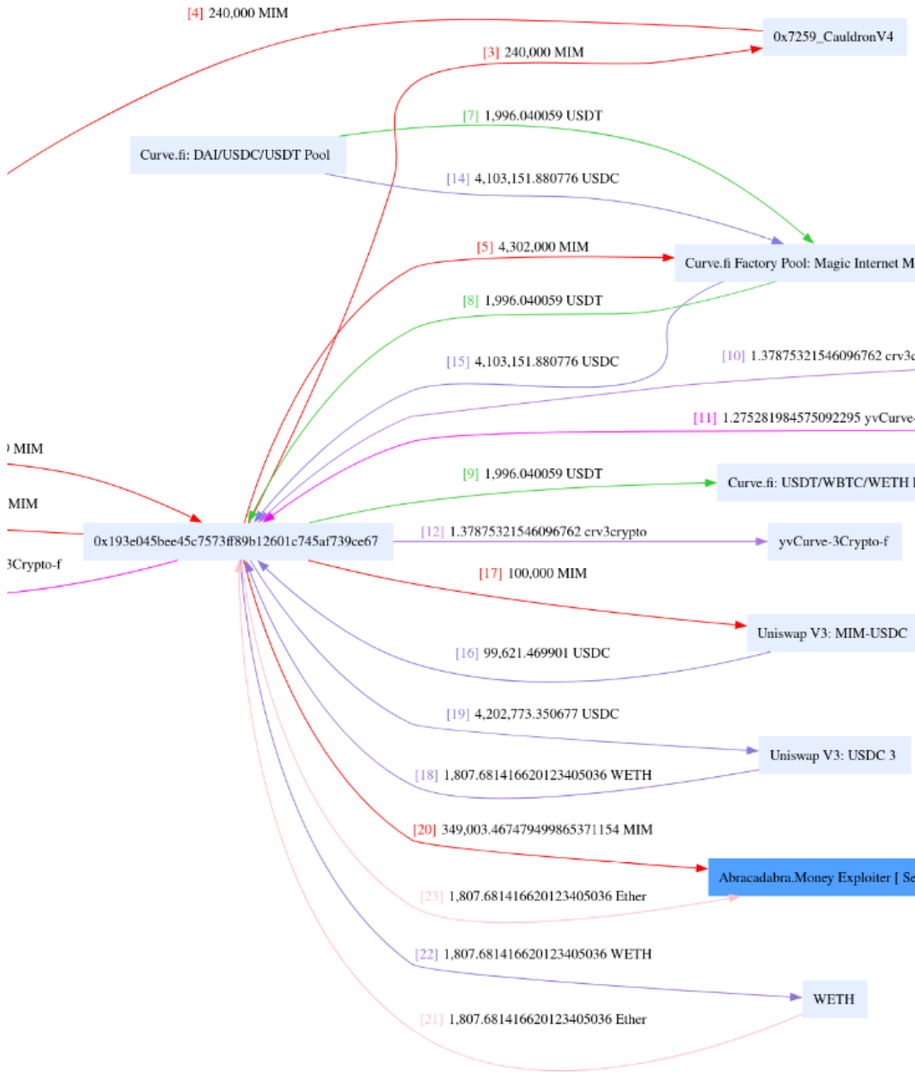
THE ATTACK

OVERVIEW

In January 2024, MIM_SPELL suffered a flash loan attack due to a precision calculation vulnerability, resulting in a loss of $6.5 million

PROPONENTS

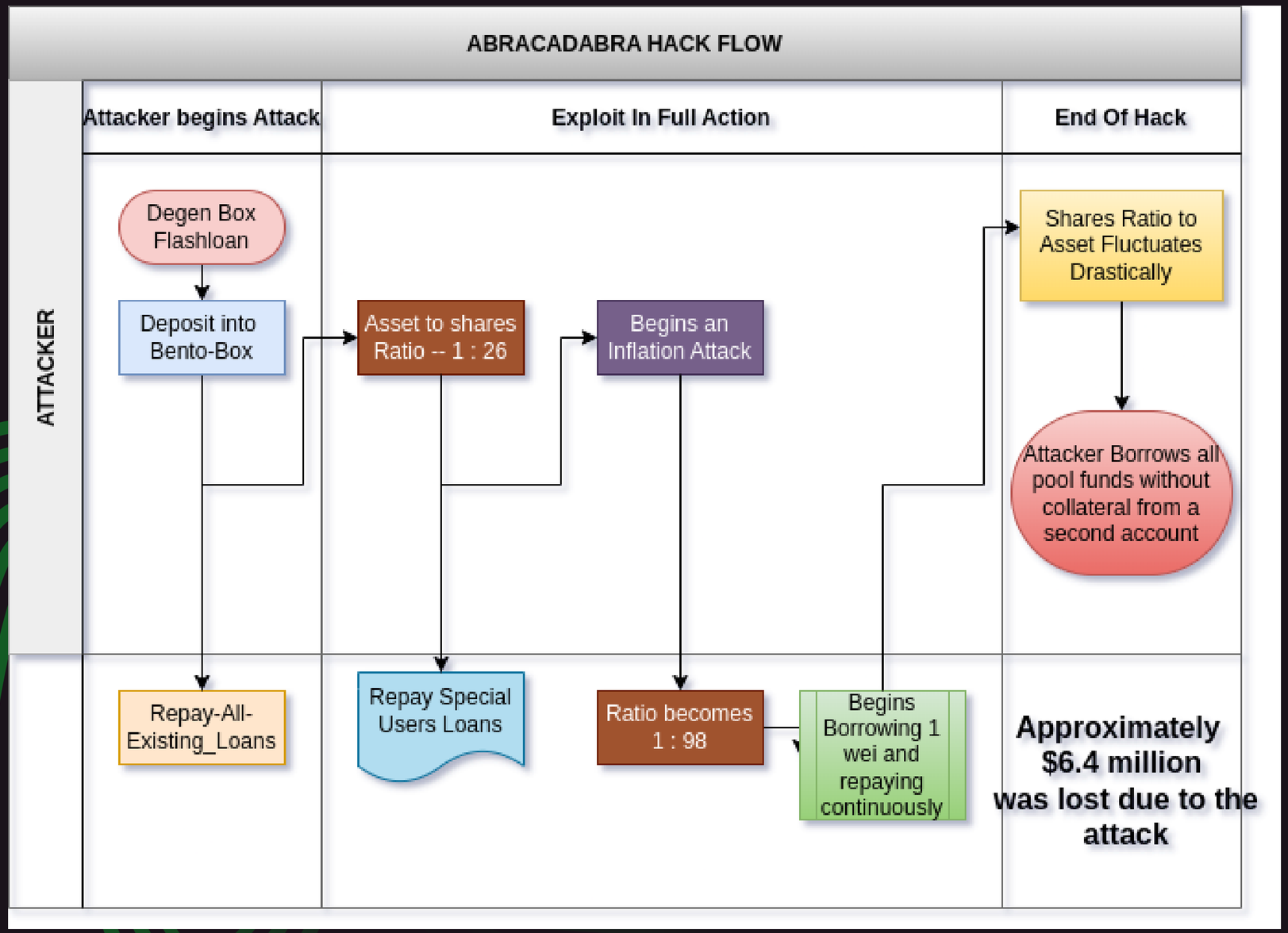
The essence of the attack was an accuracy problem when calculating loan variables, which caused key variables to be manipulated and proportions to be out of balance, resulting in excessive lending of MIM tokens.



Guild Audits

HOW IT WENT DOWN

Back to Agenda



C0D3 T1M3 !!!

Lets get into the cod3 and try to r3play the 4tt4ck that happen3d

Head over to https://github.com/jaydhales/MIM-Spell-Hack-Review

Back to Agenda

ANALYSIS AND MITIGATION

When developing logic related to precision calculation, carefully consider precision and rounding.

For lending protocols that use shares calculation to calculate owed interest, make sure there is no way to reduce totalBorrowShares less than totalBorrowAssets

Back to Agenda

Thanks!. Arigato!. Connect with us

JAYDHALES	https://twitter.com/jaydhales1
OT	https://twitter.com/otaikisadiq
PELZ	https://twitter.com/Pelz_Dev
KENZMAN	https://twitter.com/kenzman18

Guild Audits