REPORT FOR DASH DECENTRALISED GOVERNANCE ATTACK SIMULATOR

FILES TO BE GENERATED

default.csv, default.html, default.pdf

VALUES PROCEEDING WITH

Attack budget (£): unspecified (cost estimated in phase two)
Dash price (£): 85.4 (real time value)
Inflation rate: 2.26 (default exponential)
Coins in circulation: 8777516 (real time value)
Total of honest masternodes: 4840 (real time value)
Honest masternodes already under control or bribe: 800
Target total masternodes: 1000 (user defined value)

ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Active masternodes before purchase: 4840
Masternodes required for net 10% over honest: 5325
Attack budget (£): cost of realise target of 1000 masternodes
Therefore, target total masternodes: 1000
Excluding those already under control or bribe, total: 800
Finalised total of masternodes to acquire: 200

Coins in circulation before purchase: 8777516
From which coins frozen for required collateral: 4840000
Therefore, coins remaining available to acquire: 3937516
These are enough for this number of masternodes: 3937
Which as percentage out of the total possible masternodes is: 44.8%

ATTACK PHASE TWO: EXECUTION

FIRST PURCHASE ATTEMPT FOR 200 MASTERNODES

PURCHASE OUTCOME: POSSIBLE

HYPOTHETICAL REALISATION

Dash price before attack initiation (£): 85.4
Estimated Dash price after purchase (£): 85.85
Estimated total cost with inflation (£): 17125206.362

Coins in circulation after purchase: 8777516
From which coins frozen for required collateral: 5040000
Therefore, coins remaining available to acquire: 3737516
These are enough to acquire more masternodes, specifically: 3737
Which as percentage takes this share from total possible masternodes: 42.5
However, 55% guarantees success in any governance attack
Theoretical total active masternodes after purchase: 5040
From which malicious: 200 + 800 = 1000 (19.8% of total masternodes)

SUMMARY

Number of masternodes required for malicious majority: 5325
The available coin supply was enough to buy this amount of masternodes: 3937
The attempted purchase was for: 200 masternodes
Estimated total cost with inflation (£): 17125206.362
Total active masternodes after purchase: 5040
From which malicious: 1000 (19.8% of total masternodes)

INSIGHTS: WHAT PROBLEMS CAN WE CAUSE RIGHT NOW?

(1) PREVENT HONEST PROPOSALS TO GO THROUGH

EXAMPLE

Monthly salary of Dash Core Developers or other beneficial investments

DESIGN VULNERABILITY

Proposals are not partially funded and remaining governance funds are burnt.
Therefore, if attacked proposal is not in top rankings, it will be rejected.

SUCCESS LIKELIHOOD: HIGH

Because even if net 10% is achieved there is no funding guarantee.
Funding is granted to the top X proposals based on net percentage.

METHODOLOGY

By down-voting proposals so that the net 10% margin is not achieved

EXPLOITATION

Total votes of malicious masternodes: 200
Least honest votes required for net majority: 704
Maximum malicious masternodes based on available circulation: 3937
Least honest votes required for net majority: 4332

(2) MALICIOUS PROPOSAL PASSES BY NEGLIGENCE

EXAMPLE

Malicious proposal up-voted from malicious masternodes and abstention is high

DESIGN VULNERABILITY

Votes are never questioned therefore if a proposal is accepted, no censorship exists

SUCCESS LIKELIHOOD: MEDIUM

The controversy of a malicious proposal is expected to unite honest owners

METHODOLOGY

Malicious proposal starts to be up-voted as close as possible to the closing window

EXPLOITATION

Total votes of malicious masternodes: 200
Least honest votes required for rejection: 0
Maximum malicious masternodes based on available circulation: 3937
Least votes required for net majority against maximum malicious: 0

HISTORIC DATA

Maximum votes ever recorded for funding a proposal is: 2147
At the time, this as percentage towards total masternodes was: 44.44%
Assuming a higher percentage this time due to unity from controversy: 60%
Which equals this number of honest masternodes: 2904
Therefore, total malicious masternodes needed for net majority: 3196

INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 46.4%
Total ever coin supply: 18900000
Remaining ever coin supply: 10122484
Corresponding masternodes: 10122

EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)
Available masternodes: 709

09/2021:10160671 (53.7% of total ever)
Available masternodes: 1383

08/2029 (74.41%), 03/2043 (90.23%), 05/2073 (98.86%), 04/2150 (100%)