REPORT FOR DASH DECENTRALISED GOVERNANCE ATTACK SIMULATOR

FILES TO BE GENERATED

dash-default.csv, dash-default.html, dash-default.pdf

VALUES PROCEEDING WITH

Attack budget (£): unspecified (cost estimated in attack phase two)
Dash price (£): 66.76 (real time value)
Inflation rate: 2.26 (default exponential)
Coins in circulation: 9007008 (real time value)
Total of honest masternodes: 2200 (user defined value)
Honest masternodes already under control or bribe: 0
Target total masternodes: unspecified (defaults to net 10% over honest)
Masternode block reward: 3.11 DASH

ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Active masternodes before purchase: 2200
Masternodes required for net 10% over honest: 2421
Attack budget (£): cost of realise target of 2421 masternodes
Therefore, target total masternodes: 2421
Excluding those already under control or bribe, total: 0
Finalised total of masternodes to acquire: 2421

Coins in circulation before purchase: 9007008
From which coins frozen for required collateral: 2200000
Therefore, coins remaining available to acquire: 6807008
These are enough for this number of masternodes: 6807
Which as percentage out of the total possible masternodes is: 75.5%

ATTACK PHASE TWO: EXECUTION

FIRST PURCHASE ATTEMPT FOR 2421 MASTERNODES

PURCHASE OUTCOME: POSSIBLE

HYPOTHETICAL REALISATION

Dash price before attack initiation (£): 66.76
Estimated Dash price after purchase (£): 72.23
Estimated total cost with inflation (£): 168250124.969

Coins in circulation after purchase: 9007008
From which coins frozen for required collateral: 4621000
Therefore, coins remaining available to acquire: 4386008
These are enough to acquire more masternodes, specifically: 4386
Which as percentage takes this share from total possible masternodes: 48.6
However, 55% guarantees success in any governance attack
Total active masternodes after purchase: 4621
From which malicious: 2421 (52.3% of total masternodes)

RETURN ON INVESTMENT

Money invested in this attack are not lost, just exchanged from GBP to Dash.
Daily Dash expected from masternode block reward: 941.16 (£67979.99)
Monthly Dash expected from masternode block reward: 28554.91 (£2062521.15)
Yearly Dash expected from masternode block reward: 343524.77 (£24812794.14)
Estimated profits should also take into consideration any potential increase in the highly volatile original coin price with which masternodes were acquired.

SUMMARY

Number of masternodes required for malicious majority: 2421
The available coin supply was enough to buy this amount of masternodes: 6807
The attempted purchase was for: 2421 masternodes
Estimated total cost with inflation (£): 168250124.969

Total active masternodes after purchase: 4621
From which malicious: 2421 (52.3% 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: 2421
Least honest votes required for net majority: 2665
Maximum malicious masternodes based on available circulation: 6807
Least honest votes required for net majority: 7489

(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: 2421
Least honest votes required for rejection: 2199
Maximum malicious masternodes based on available circulation: 6807
Least votes required for net majority against maximum malicious: 6187

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: 1320
Therefore, total malicious masternodes needed for net majority: 1454

INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 47.6%
Total ever coin supply: 18900000
Remaining ever coin supply: 9892992
Corresponding masternodes: 9892

EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)
Available masternodes: 479

09/2021:10160671 (53.7% of total ever)
Available masternodes: 1153

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