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 (£): 125.17 (real time value)
Inflation rate: 2.26 (default exponential)
Coins in circulation: 8891963 (real time value)
Total of honest masternodes: 4926 (real time value)
Honest masternodes already under control or bribe: 0
Target total masternodes: unspecified (defaults to net 10% over honest)
Masternode block reward: 1.55DASH

ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Active masternodes before purchase: 4926
Masternodes required for net 10% over honest: 5420
Attack budget (£): cost of realise target of 5420 masternodes
Therefore, target total masternodes: 5420
Excluding those already under control or bribe, total: 0
Finalised total of masternodes to acquire: 5420

Coins in circulation before purchase: 8891963
From which coins frozen for required collateral: 4926000
Therefore, coins remaining available to acquire: 3965963
These are enough for this number of masternodes: 3965
Which as percentage out of the total possible masternodes is: 44.5%

ATTACK PHASE TWO: EXECUTION

FIRST PURCHASE ATTEMPT FOR 5420 MASTERNODES

PURCHASE OUTCOME: IMPOSSIBLE

REASON

Because the remaining coins in circulation are not enough for 5420 masternodes but for a maximum of 3965, still capable for an effective cyber sabotage

HYPOTHETICAL REALISATION

Dash price before attack initiation (£): 125.17
Estimated Dash price after purchase (£): 137.42
Estimated total cost with inflation (£): 711621564.312

Coins in circulation after purchase: 8891963
From which coins frozen for required collateral: 10346000 <--- (Problematic metric)
Therefore, coins remaining available to acquire: -1454037 <--- (Problematic metric)
Theoretical total active masternodes after purchase: 10346
From which malicious: 5420 (52.3% of total masternodes)

SUMMARY

Number of masternodes required for malicious majority: 5420
The available coin supply was enough to buy this amount of masternodes: 3965
The attempted purchase was for: 5420 masternodes <--- (Problematic metric)

SECOND PURCHASE ATTEMPT FOR 3965 MASTER NODES

PURCHASE OUTCOME POSSIBLE

ANALYSIS

Dash price before attack initiation (£): 125.17

Estimated Dash price after purchase (£): 134.13
Estimated total cost with inflation (£): 514066619.132

Coins in circulation after purchase: 8891963
From which coins frozen for required collateral: 8891000
Therefore, coins remaining available to acquire: 963
Total active masternodes after purchase: 8891
From which malicious: 3965 (44.5% 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:768.22 (£103041.35)
Monthly Dash expected from masternode block reward:23307.76 (£3126269.85)
Yearly Dash expected from masternode block reward:280399.84 (£37610030.54)
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: 5420
Available supply was enough for this amount of masternodes: 3965
Estimated total cost with inflation (£): 514066619.132
Total active masternodes after purchase: 8891
From which malicious: 3965 (44.5% 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

Maximum malicious masternodes based on available circulation: 3965
Least honest votes required for net majority: 4363

(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

Maximum malicious masternodes based on available circulation: 3965
Least votes required for net majority against maximum malicious: 3603

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: 2956
Therefore, total malicious masternodes needed for net majority: 3253

INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 47.0%
Total ever coin supply: 18900000
Remaining ever coin supply: 10008037
Corresponding masternodes: 10008

EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)
Available masternodes: 594

09/2021:10160671 (53.7% of total ever)
Available masternodes: 1268

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