REPORT FOR DASH DECENTRALISED GOVERNANCE ATTACK SIMULATOR

FILES TO BE GENERATED

default.csv, default.html, default.pdf

VALUES PROCEEDING WITH

Attack budget (£): 700000000.0 (user defined value)
Dash price (£): 84.22 (real time value)
Inflation rate: 2.26 (default exponential)
Coins in circulation: 8775963 (real time value)
Total of honest masternodes: 4500 (user defined value)
Honest masternodes already under control or bribe: 0
Target total masternodes: 8311 (capped due to budget)

ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Active masternodes before purchase: 4500
Masternodes required for net 10% over honest: 4951
Attack budget (£): 700000000.0 (enough to acquire 8311 masternodes)
Therefore, target total masternodes: 4951
Excluding those already under control or bribe, total: 0
Finalised total of masternodes to acquire: 4951

Coins in circulation before purchase: 8775963
From which coins frozen for required collateral: 4500000
Therefore, coins remaining available to acquire: 4275963
These are enough for this number of masternodes: 4275
Which as percentage out of the total possible masternodes is: 48.7%

ATTACK PHASE TWO: EXECUTION

FIRST PURCHASE ATTEMPT FOR 4951 MASTERNODES

PURCHASE OUTCOME: IMPOSSIBLE

REASON

Because the remaining coins in circulation are not enough for 4951 masternodes but for a maximum of 4275, still capable for an effective cyber sabotage

HYPOTHETICAL REALISATION

Dash price before attack initiation (£): 84.22
Estimated Dash price after purchase (£): 103.01
Estimated total cost with inflation (£): 699952457.571
Therefore remaining budget equals (£): 47542.429

Coins in circulation after purchase: 8775963
From which coins frozen for required collateral: 9451000 <--- (Problematic metric)
Therefore, coins remaining available to acquire: -675037 <--- (Problematic metric)
Theoretical total active masternodes after purchase: 9451
From which malicious: 4951 (52.3% of total masternodes)

SUMMARY

Number of masternodes required for malicious majority: 4951
The available coin supply was enough to buy this amount of masternodes: 4275
The attempted purchase was for: 4951 masternodes <--- (Problematic metric)

SECOND PURCHASE ATTEMPT FOR 4275 MASTER NODES

PURCHASE OUTCOME POSSIBLE

ANALYSIS

Dash price before attack initiation (£): 84.22

Estimated Dash price after purchase (£): 93.88
Estimated total cost with inflation (£): 380694961.504

Coins in circulation after purchase: 8775963
From which coins frozen for required collateral: 8775000
Therefore, coins remaining available to acquire: 963
Total active masternodes after purchase: 8775
From which malicious: 4275 (48.7% of total masternodes)

SUMMARY

Number of masternodes required for malicious majority: 4951
Available supply was enough for this amount of masternodes: 4275
Estimated total cost with inflation (£): 380694961.504
Total active masternodes after purchase: 8775
From which malicious: 4275 (48.7% 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: 4275
Least honest votes required for net majority: 4704

(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: 4275
Least votes required for net majority against maximum malicious: 3885

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: 2700
Therefore, total malicious masternodes needed for net majority: 2972

INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 46.4%
Total ever coin supply: 18900000
Remaining ever coin supply: 10124037
Corresponding masternodes: 10124

EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)
Available masternodes: 710

09/2021:10160671 (53.7% of total ever)
Available masternodes: 1384

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