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 (£): 74.63 (real time value)
Inflation rate: 2.26 (default exponential)
Coins in circulation: 8994092 (real time value)
Total of honest masternodes: 4881 (real time 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: 4881
Masternodes required for net 10% over honest: 5371
Attack budget (£): cost of realise target of 5371 masternodes
Therefore, target total masternodes: 5371
Excluding those already under control or bribe, total: 0
Finalised total of masternodes to acquire: 5371

Coins in circulation before purchase: 8994092
From which coins frozen for required collateral: 4881000
Therefore, coins remaining available to acquire: 4113092
These are enough for this number of masternodes: 4113
Which as percentage out of the total possible masternodes is: 45.7%

ATTACK PHASE TWO: EXECUTION

FIRST PURCHASE ATTEMPT FOR 5371 MASTERNODES

PURCHASE OUTCOME: IMPOSSIBLE

REASON

Because the remaining coins in circulation are not enough for 5371 masternodes but for a maximum of 4113, still capable for an effective cyber sabotage

HYPOTHETICAL REALISATION

Dash price before attack initiation (£): 74.63
Estimated Dash price after purchase (£): 86.77
Estimated total cost with inflation (£): 433440309.609

Coins in circulation after purchase: 8994092
From which coins frozen for required collateral: 10252000 <--- (Problematic metric)
Therefore, coins remaining available to acquire: -1257908 <--- (Problematic metric)
Theoretical total active masternodes after purchase: 10252
From which malicious: 5371 (52.3% of total masternodes)

SUMMARY

Number of masternodes required for malicious majority: 5371
The available coin supply was enough to buy this amount of masternodes: 4113
The attempted purchase was for: 5371 masternodes <--- (Problematic metric)

SECOND PURCHASE ATTEMPT FOR 4113 MASTER NODES

PURCHASE OUTCOME POSSIBLE

ANALYSIS

Dash price before attack initiation (£): 74.63

Estimated Dash price after purchase (£): 83.93
Estimated total cost with inflation (£): 326071920.597

Coins in circulation after purchase: 8994092
From which coins frozen for required collateral: 8994000
Therefore, coins remaining available to acquire: 92
Total active masternodes after purchase: 8994
From which malicious: 4113 (45.7% 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:1598.93 (£134198.19)
Monthly Dash expected from masternode block reward:48511.5 (£4071570.2)
Yearly Dash expected from masternode block reward:583608.99 (£48982302.53)
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: 5371
Available supply was enough for this amount of masternodes: 4113
Estimated total cost with inflation (£): 326071920.597
Total active masternodes after purchase: 8994
From which malicious: 4113 (45.7% 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: 4113
Least honest votes required for net majority: 4526

(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: 4113
Least votes required for net majority against maximum malicious: 3738

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: 2929
Therefore, total malicious masternodes needed for net majority: 3223

INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 47.5%
Total ever coin supply: 18900000
Remaining ever coin supply: 9905908
Corresponding masternodes: 9905

EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)
Available masternodes: 492

09/2021:10160671 (53.7% of total ever)
Available masternodes: 1166

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