REPORT FOR DECRED DECENTRALISED GOVERNANCE ATTACK SIMULATOR

FILES TO BE GENERATED

decred-default.csv, decred-default.html, decred-default.pdf

VALUES PROCEEDING WITH

Attack budget (£): unspecified (cost estimated in attack phase two)
Decred price (£): 19.99 (real time value)
Decred ticket price (£): 119.3 (real time value)
Inflation rate: 2.26 (default exponential)
Coins in circulation: 9722961 (real time value)
Ticket pool size: 41015 (real time value)
Tickets already under control or bribe: 0
Target total tickets: unspecified (defaults to 60% over honest tickets)

ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Ticket pool size before purchase: 41015
Tickets required for malicious 60% over honest tickets: 24609
Attack budget (£): cost of realise target of 24609 tickets
Therefore, target total tickets: 24609
Excluding tickets already under control or bribe, total: 0
Finalised total of tickets to acquire: 24609

Coins in circulation before purchase: 9722961
From which coins frozen for tickets: 4893089.5
Therefore, coins remaining available to acquire and freeze: 4829871.5
These are enough for this number of tickets: 40960
While this attack will proceed with purchasing: 24609
However, this amount is high to be purchased straight away as there exist constraints in tickets supply analysed below.

ATTACK PHASE TWO: EXECUTION

PURCHASE ATTEMPT FOR 24609 TICKETS

PURCHASE OVERHEAD ESTIMATION: 17 DAYS

REASON

Because 5 (honest) tickets per block will be used to vote and immediately expire which leads to 5 new spots for malicious tickets to take over. While this is the case for on-chain votes that vote towards PoW block validity, this is not to be confused with off-chain votes for proposals and consensus rules which is our focus in this simulation. Luckily, the right to vote for governance proposals remains valid during the entirevoting window as long as tickets were part of the initial proposal quorum(contextually: snapshot of ticket pool at the time where the voting started).

The number of days required is because Decred blocks are solved every five minutes which equals 288 blocks per day, therefore 1,440 expired tickets per day able to be replaced by 20 biddable tickets per block that equals 5,760tickets as candidates to replace those 1,440.

HYPOTHETICAL REALISATION

Decred coin price before attack initiation (£): 19.99
Estimated coin price after purchase (£): 31.11
Decred ticket price before attack initiaton (£): 119.3
Estimated ticket price after purchase (£): 130.42
Estimated total cost with inflation (£): 125764016.447
Cost includes competent bidding with high transaction fees to increase chances of ticket bids being picked by miners and placed in ticket pool.

Coins in circulation after purchase: 9722961
From which coins frozen for tickets: 5349176
Therefore, coins remaining available to acquire: 4373785
Ticket pool size after purchase: 40960
From which malicious: 24609 (60.0% of total tickets)

SUMMARY

Number of tickets required for malicious majority: 24609
This will take this number of days to be realised: 17 DAYS
Estimated total cost with inflation (£): 125764016.447
Ticket pool size: 40960
From which malicious: 24609 (60.0% of total tickets)

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: 24609
Least honest votes required for net majority: 27071
Maximum malicious masternodes based on available circulation: 40960
Least honest votes required for net majority: 45057

(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: 24609
Least honest votes required for rejection: 22370
Maximum malicious masternodes based on available circulation: 40960
Least votes required for net majority against maximum malicious: 37235

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: 9811

Therefore, total malicious masternodes needed for net majority: 10794

INFORMATION FOR THE FUTURE

Percentage of current circulation against total ever: 46.2%
Total ever coin supply: 21000000
Remaining ever coin supply: 11277039
Corresponding masternodes: 11277

EXPECTED CIRCULATION PER YEAR

09/2020: 9486800 (50.14% of total ever)
Available masternodes: -237

09/2021:10160671 (53.7% of total ever)
Available masternodes: 437

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