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 (£): 20.84 (real time value)
Decred ticket price (in DCR): 117.8 (real time value)
Inflation rate: 7.48 (default exponential)
Coins in circulation: 9821215 (real time value)
Ticket pool size: 41147 (real time value)
Tickets already under control or bribe: 0
Target total tickets: unspecified (defaults to 60% over honest tickets)
Ticket reward per block: 5.36

ATTACK PHASE ONE: PRE-PURCHASE ANALYSIS

Ticket pool size before purchase: 41147
Tickets required for malicious 60% over honest tickets: 24689
Attack budget (£): cost of realise target of 24689 tickets
Therefore, target total tickets: 24689
Excluding tickets already under control or bribe, total: 0
Finalised total of tickets to acquire: 24689

Coins in circulation before purchase: 9821215
From which coins frozen for tickets: 4847116
Therefore, coins remaining available to acquire and freeze: 4974099
These are enough for this number of tickets: 40960
While this attack will proceed with purchasing: 24689
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 24689 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 5,760 tickets as candidates to replace those 1,440.

HYPOTHETICAL REALISATION

Decred coin price before attack initiation (£): 20.84
Estimated coin price after purchase (£): 22.69
Decred ticket price before attack initiaton (in DCR): 117.8
Estimated ticket price after purchase (in DCR): 119.65
Estimated total cost with inflation (£): 63801318.075
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: 9821215
From which coins frozen for tickets: 4923238
Therefore, coins remaining available to acquire: 4897977
Ticket pool size after purchase: 40960
From which malicious: 24689 (60.0% of total tickets)

RETURN ON INVESTMENT

Money invested in this attack are not lost, just exchanged from GBP to Decred.
Daily Decred expected from ticket block reward: 4726.18 (£107237.02)
Monthly Decred expected from ticket block reward: 143392.3 (£3253571.29)
Yearly Decred expected from ticket block reward: 1725055.7 (£39141513.83)
Estimated profits should also take into consideration any potential increase in the highly volatile original coin price with which tickets were acquired.

SUMMARY

Number of tickets required for malicious majority: 24689
This will take this number of days to be realised: 17 DAYS
Estimated total cost with inflation (£): 63801318.075
Ticket pool size: 40960
From which malicious: 24689 (60.0% of total tickets)

INSIGHTS: WHAT PROBLEMS CAN WE CAUSE RIGHT NOW?

(1) PREVENT HONEST PROPOSALS TO GO THROUGH

EXAMPLE

Downvote key consensus changes that would make the coin more scalable

DESIGN VULNERABILITY

Decred tries to be cencorship-free and fully guided from its community, therefore all decisions are respected and final, without asking anything.

SUCCESS LIKELIHOOD: HIGH

Since the dominant motivation of ticket owners is profit from PoS rewards and not the coin development, it was noticed that governance proposals do not attract more than half of pool size votes therefore there exists high voting abstention which makes this attack very possible to happen.

METHODOLOGY

By down-voting proposals so that 60% margin is not achieved

EXPLOITATION

Total votes from malicious tickets: 24689
Least honest votes required for net majority: 24689 (60% of ticket pool)
While ticket pool has a size of: 41147

(2) MALICIOUS PROPOSAL PASSES BY NEGLIGENCE

EXAMPLE

Malicious proposal up-voted from malicious tickets that had net majority prior to the start of voting window or even if they had not they can still dominate when voting abstention is high as it is in 99 out of 100 cases.

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 from malicious tickets: 24689
Least honest votes required for proposal rejection (40.1%): 16500
While ticket pool has a size of: 41147