Inside a $190'000 Attempt to Move a Prediction Market

Forensic Analysis of a Failed "Floating Window" Attack

Case Study:
"Will Jesus Christ Return Before 2027?"
and its derivative meta-market

MarketMeaning Research

February 16, 2026

Data: Polymarket CLOB API, MarketMeaning tick-level data
Coverage: Jan 16 - Feb 16, 2026 (hourly)
L10 Orderbook: Feb 12-15, 2026 (~2s resolution)

1. EXECUTIVE SUMMARY

In mid-February 2026, the probability that "Jesus Christ returns before 2027" suddenly surged on Polymarket.

At 01:21 UTC on February 15, aggressive trades began sweeping a thin overnight order book. Within minutes, nearly $40,000 cleared the ask side. Two minutes later, another $26,000 followed.

The price climbed from 3.7% to 4.3%. A related meta-market paid out if the underlying probability exceeded 5% for 31 out of 60 minutes during any one-hour window. Under quiet conditions, it would have cost just $8,702 to momentarily push the price to that threshold.

But touching 5% was not enough. It had to be held.

As concentrated buying pressure escalated, liquidity responded in real time. Ask-side depth increased more than sixfold. The cost to push toward 5% rose rapidly. By the end of the session, sustaining the required duration would likely have required more than $200,000 -- far exceeding the potential payout.

This report reconstructs the event using tick-level price history, minute-by-minute OHLCV data, and L10 order book snapshots. It analyzes the incentive created by the meta-market, the timing of the threshold pressure, the order book's response, and the economics that turned a low-cost spike attempt into a failed sustained breach.

We do not allege wrongdoing by any specific party. This analysis examines publicly observable trading activity and the market structure that shaped its outcome.

Key Findings

> **The attack occurred during the 01:00-03:30 UTC window on February 15, targeting the point of lowest weekly liquidity. Under the "Floating Window" rule, this was a live attempt to trigger immediate settlement. The attempt failed because the attacker could not push the price beyond 4.3% against automated market maker defense. The "Majority of Minutes" rule forced the attacker into a war of attrition they could not win.**

Attack outcome	**FAILED -- peak 4.3%, needed >5%**
Minutes above 5%	**0 out of 31 required**
Underlying price range (Feb 15)	**3.7% -> 4.3% (peak)**
Meta-market price range (Feb 15)	**15% -> 30% (peak)**
Cost to touch 5% (pre-attack)	**$8,702 (cheap)**
Cost to sustain 5% (actual)	**>$200K implied**
Book hardening during attack	**6.2x (real-time defense)**
Attack window	**01:00 - 03:30 UTC (lowest liquidity)**
Resolution requirement	**>5% for 31+/60 min (any hour)**
Why it failed	**MM defense capped price at 4.3%**

2. THE REFLEXIVE MANIPULATION MECHANISM

Meta-markets on Polymarket are derivative contracts that reference the odds of other Polymarket markets. When a meta-market is structured as "Will [underlying market] odds exceed X% by [date]?", it creates an explicit, calculable incentive to manipulate the underlying market.

The "Floating Window" Danger

The "Floating Window" resolution rule allows an attacker to cherry-pick the single most vulnerable hour of the entire contract duration. Unlike a fixed-window market (where defenders know exactly when to concentrate liquidity), the attacker here has complete freedom to choose when to strike.

The attacker correctly identified February 15, 01:00 UTC as the moment of minimum defense -- cost-to-5% was only $8,702. This was the thinnest orderbook hour of the entire week. However, they underestimated the reactive speed of automated liquidity provision. As they bought, the cost-to-sustain rose 6x within minutes.

The Attack Playbook (as executed)

Step 1: ACCUMULATE META POSITION
Buy YES shares on the meta-market at 10-15 cents. A $1,500 investment buys 10,000 shares that pay $10,000 if the underlying breaches the 5% threshold for 31+ minutes in any single hour.

Step 2: PUSH THE UNDERLYING PAST 5%
Aggressively buy on the underlying market during the thinnest book hour. At 01:00 UTC on Feb 15, clearing all asks up to 5% cost only $8,702. The attacker began this phase but the book replenished faster than expected.

Step 3: SUSTAIN FOR 31+ MINUTES (FAILED)
This is where the attack collapsed. The manipulator needed to hold >5% for 31 out of 60 minutes, continuously buying against market maker replenishment. Market makers replenished asks within 1-3 minutes, and the cost-to-sustain escalated from $8,702 to over $53,000 in real-time. The attacker could not even reach 5% -- they stalled at 4.3%.

Why the "Majority of Minutes" Rule Saved the Market

> **If the resolution rule were "any trade >5%," the attacker would have won easily -- the cost to momentarily touch 5% was only $8,702. Because they had to SUSTAIN it for 31 minutes, market makers had time to wake up and dump size, capping the price at 4.3%. The duration requirement transformed a cheap spike into an unwinnable war of attrition.**

However, the Floating Window rule creates a permanent siege condition. Defenders must be automated and capitalized enough to repel an attack at 3 AM on a Sunday. If the bots had been offline for just 30 minutes, this attack would have succeeded.

3. MARKET HISTORY

The chart below shows the complete price history for both markets from January 16 through February 16, 2026. The underlying (amber) uses the left axis; the meta-market (pink) uses the right axis. The green dashed line marks the 5% manipulation threshold.

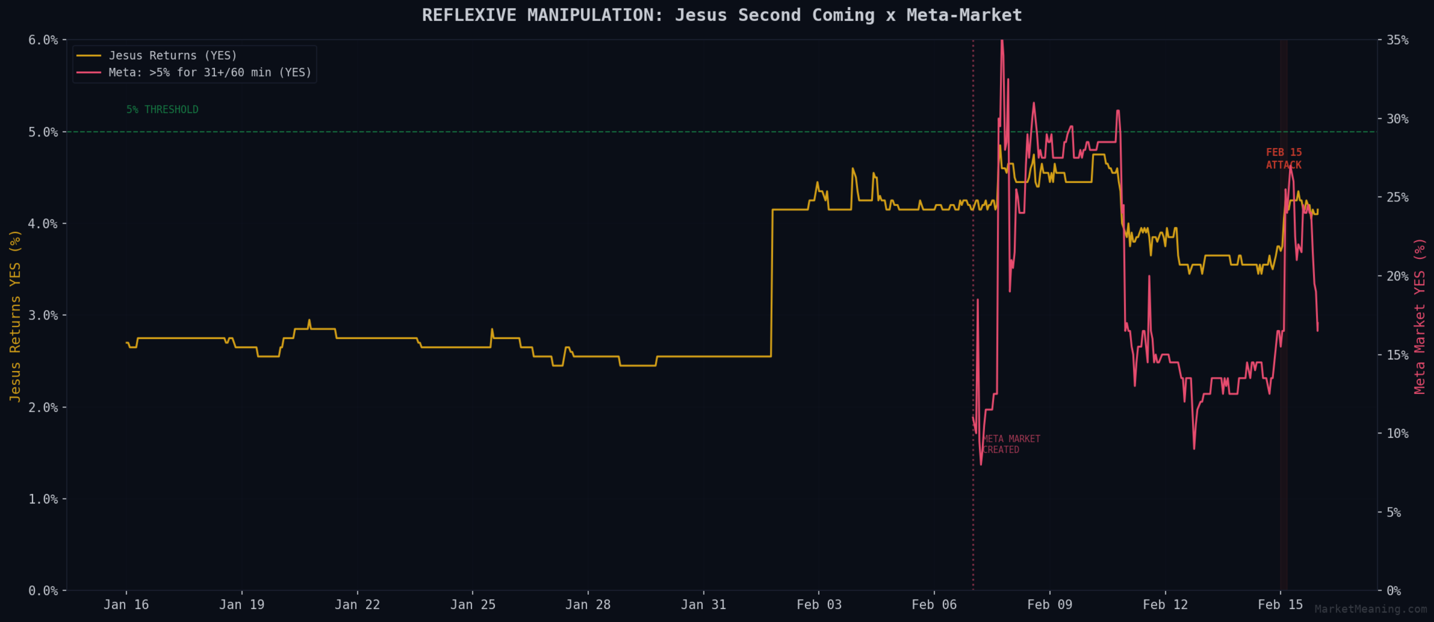


Figure 1: Full price history -- underlying vs meta-market (hourly, CLOB API)

Key observations from the full history:

> The underlying traded stably at 2.7% for two weeks (Jan 16-28), then experienced a sharp spike to 4.6% around Jan 31 - Feb 3. This first spike likely prompted the creation of the meta-market.

> The meta-market was created on February 7, initially priced at 11%. This implies the market believed there was an 11% chance the underlying would sustain >5% for 31+ minutes during the resolution window.

> After the meta-market's creation, the underlying experienced a second push on February 15, reaching 4.3%. The meta-market simultaneously spiked to 30%.

> The 5% threshold was never breached. As of February 16, the underlying sits at 4.0% and the meta-market prices a ~17% probability of a successful sustained push before the Feb 17 deadline.

4. FORENSIC TIMELINE: THE FAILED ATTACK

Using 1-minute OHLCV data and L10 orderbook snapshots from our tick-level data infrastructure, we reconstruct the minute-by-minute attack sequence on February 15, 2026. Under the "Floating Window" rule, the attacker did NOT need to wait for a specific time -- they chose 01:00-03:30 UTC because it was the moment of minimum orderbook defense. This was a live assassination attempt on market integrity, not a dry run.

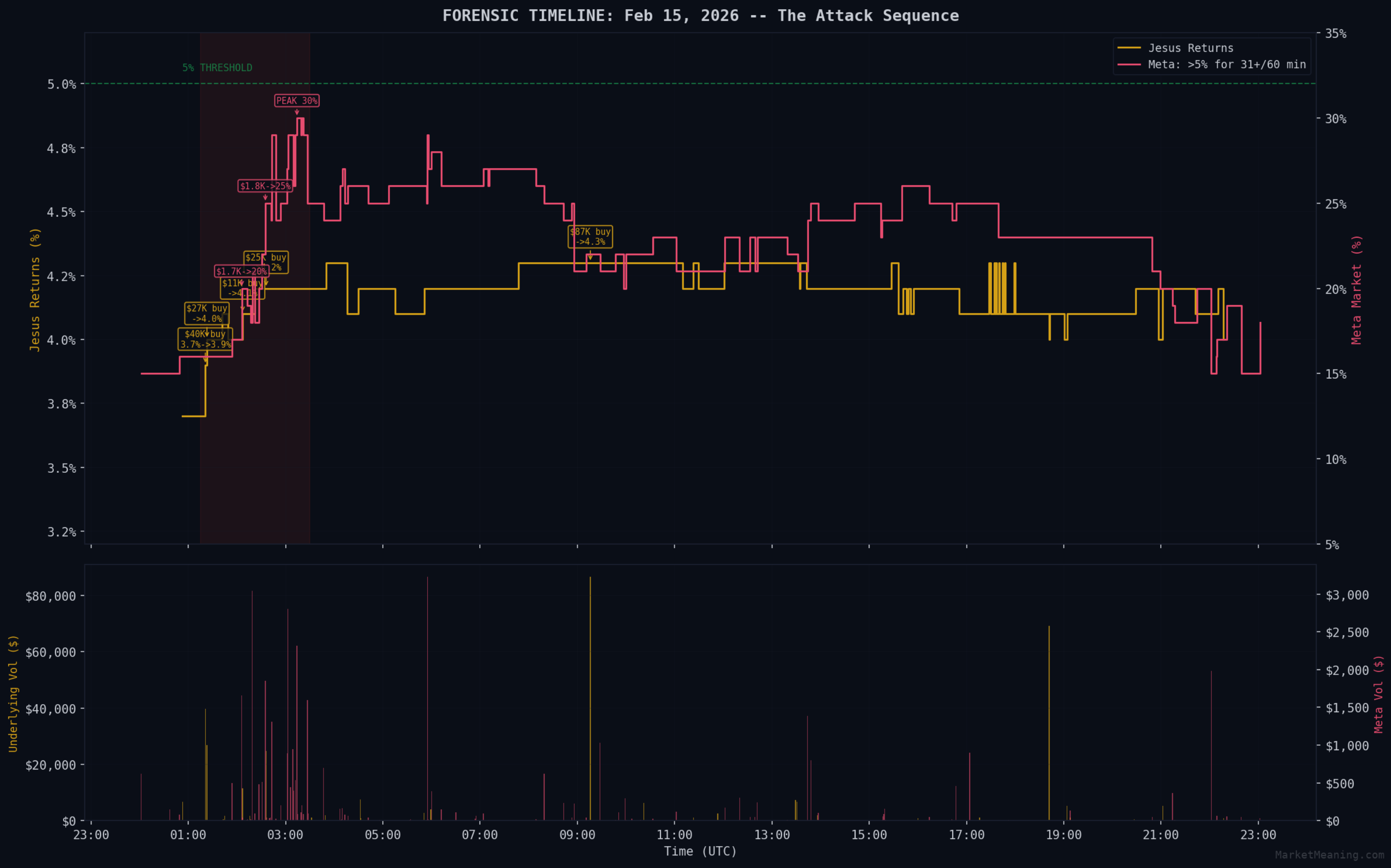


Figure 2: Intraday forensic timeline -- Feb 15 (1-min bars)

Attack Sequence

00:53 UTC -- First significant underlying trade: $6,645 at 3.70%. The meta-market sees small buys at 15-16 cents. Position building begins.

01:21 UTC -- FIRST STRIKE: $39,734 pushes underlying from 3.70% to 3.90%. Three aggressive market orders clear multiple ask levels. The attack is live.

01:23 UTC -- FOLLOW-UP: $26,718 pushes through to 4.00%. Two minutes after the first strike. Attacker is driving hard toward 5%.

02:06-02:19 UTC -- META-MARKET SURGE: $1,658 then $3,045 in rapid meta-market buying. Price jumps from 15% to 21%. Simultaneous underlying buying of $11,493. Attacker is loading the payout position while pushing.

02:35-02:43 UTC -- ESCALATION: Meta hits 25% then 29%. Underlying pushed to 4.20% with $24,802 buy. But the book is hardening -- market makers are waking up.

03:03-03:14 UTC -- STALL: Meta hits 30% but underlying cannot advance past 4.25%. Market makers have deployed significant new ask-side liquidity. The attack is being repelled.

03:27 UTC -- RETREAT: Meta selling at 25%. The attacker recognizes the defense has hardened beyond their capital.

09:16 UTC -- LAST PUSH: $86,590 single trade pushes underlying to 4.3% (day high). A final desperate attempt that still falls 0.7% short of the 5% threshold.

> **The attacker failed on PRICE, not timing. Under the Floating Window rule, they had every incentive to trigger the payout immediately. They spent ~$190K+ in cumulative volume but could not breach the 5% wall because market makers responded in real-time, hardening the book 6.2x during the attack itself.**

5. ATTACK WINDOW: 00:30 - 04:00 UTC

The zoomed view below shows the critical 3.5-hour window where the coordinated cross-market activity is most visible. Scatter point sizes are proportional to trade volume, making the large aggressive buys immediately apparent.

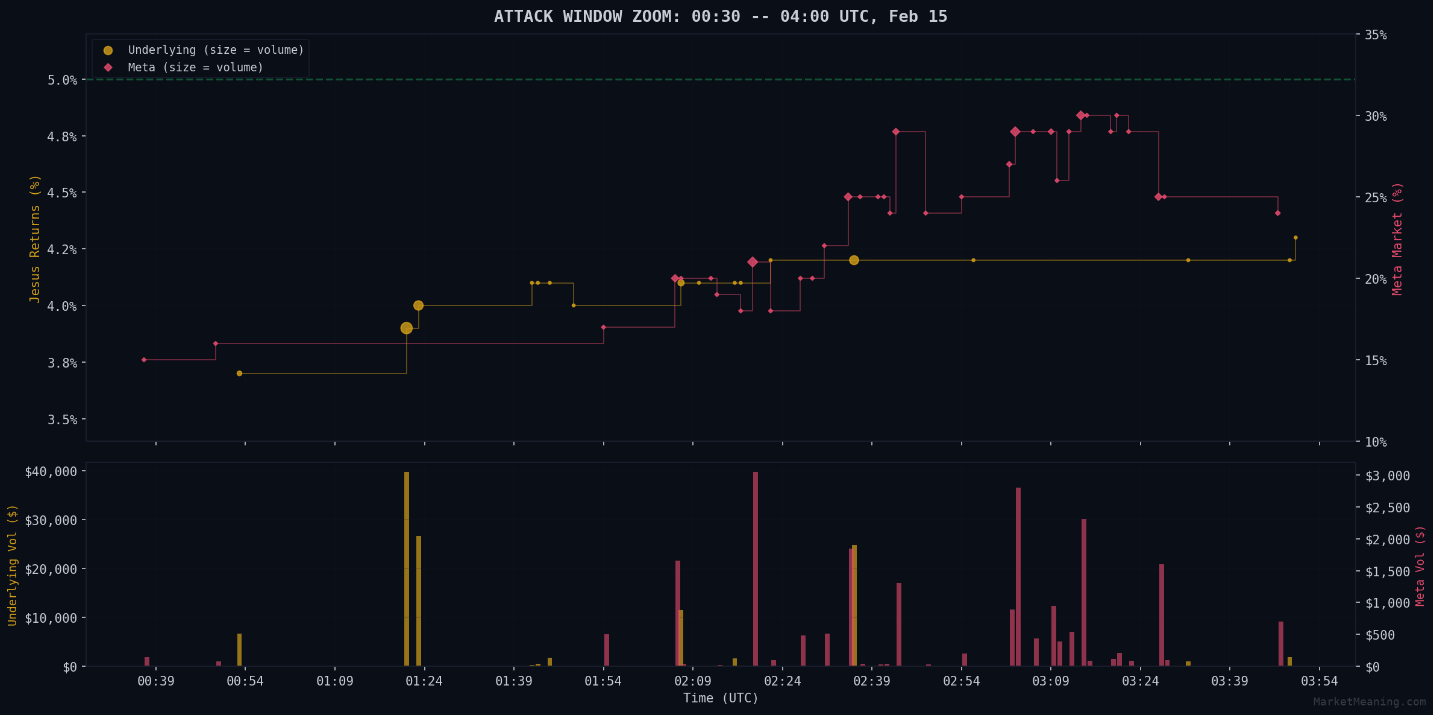


Figure 3: Attack window zoom -- scatter size proportional to trade volume

The temporal correlation is striking: large underlying buys (amber circles at 01:21-01:23) are followed within minutes by meta-market accumulation (pink diamonds at 02:06-02:43). The volume panel confirms that the largest trades on both markets cluster within the same 2-hour window.

This timing pattern is consistent with a coordinated strategy rather than independent trading activity. Organic price discovery on a market like "Will Jesus return?" would not produce concentrated bursts of five-figure trades at 1-3 AM UTC.

6. CROSS-MARKET VOLUME CORRELATION

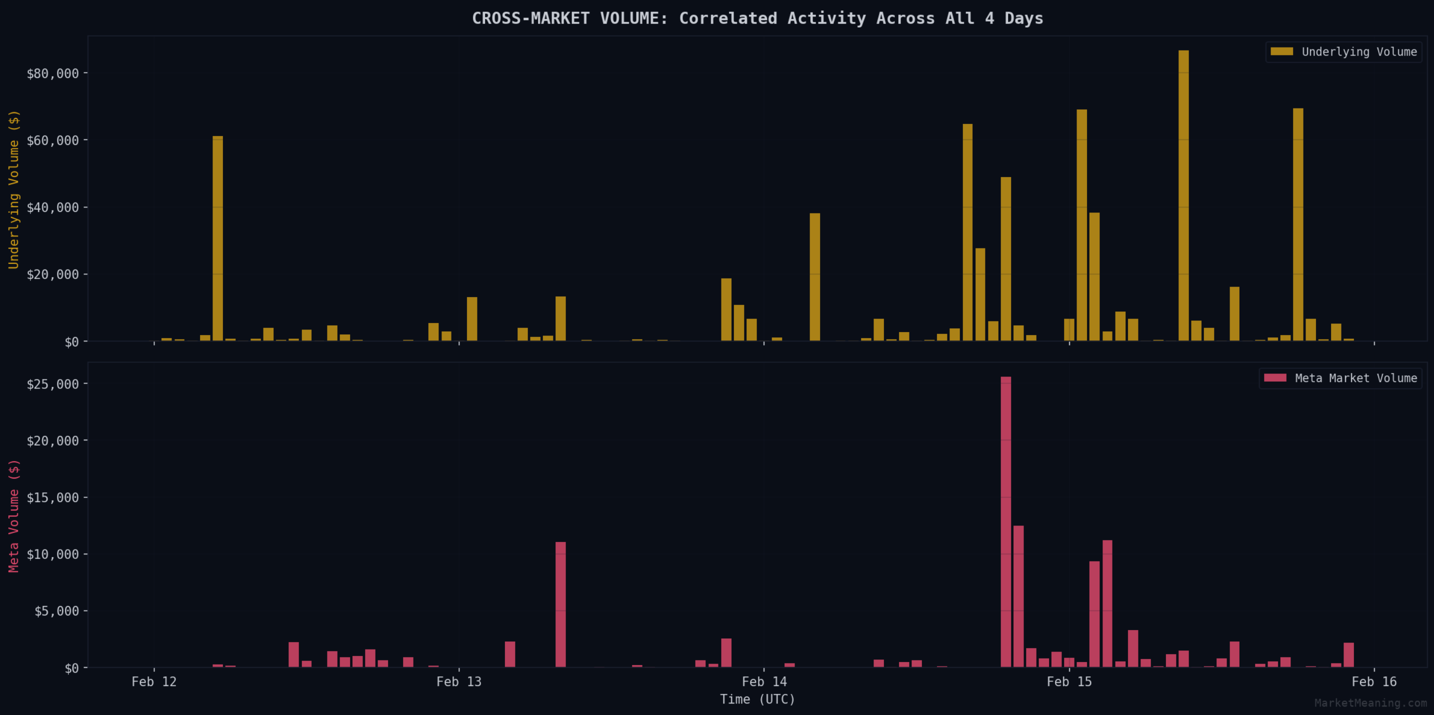


Figure 4: Hourly volume for underlying (top) and meta-market (bottom), Feb 12-15

The four-day volume comparison reveals the escalation pattern. February 12-13 show baseline activity: small, sporadic trades on both markets. February 14 sees a volume increase on the underlying ($211K vs ~$80K baseline), with the meta-market also picking up ($44K vs ~$14K baseline).

February 15 shows the clear spike: underlying volume triples to $326K and the meta-market sees its highest single-hour volume in the early morning attack window. The correlation between the two volume series is consistent with a single actor (or coordinated group) operating across both markets simultaneously.

Feb 12 underlying volume	**$90,806**
Feb 13 underlying volume	**$72,181**
Feb 14 underlying volume	**$211,177**
Feb 15 underlying volume	**$326,265**
Feb 12 meta volume	**$9,967**
Feb 13 meta volume	**$17,198**
Feb 14 meta volume	**$44,366**
Feb 15 meta volume	**$34,378**

The escalation pattern -- baseline -> buildup -> attack -- is characteristic of position building before a coordinated push.

7. COST-TO-MANIPULATE ANALYSIS

Using L10 orderbook snapshots sampled every 30 minutes across February 12-15, we compute the capital required to push the underlying market's YES price to the 5% threshold at each point in time. This "cost-to-move" function is calculated by walking the ask side of the orderbook and summing the cost of clearing all resting orders up to the target price.

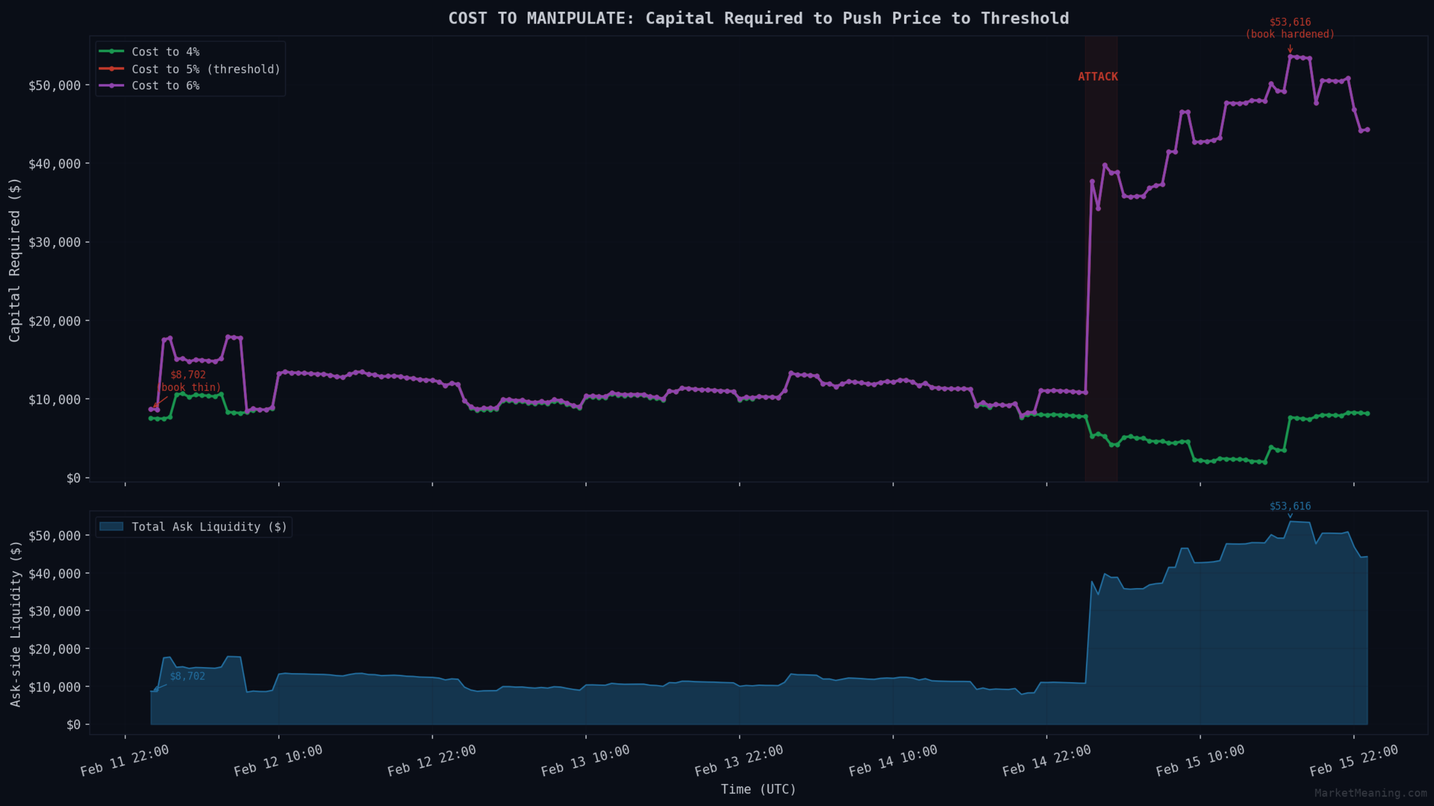


Figure 5: Cost-to-move evolution (top) and ask-side liquidity depth (bottom)

Key Observations

> PRE-ATTACK (Feb 12-14): The cost to push to 5% hovered around $8,000-$15,000. The book was thin -- a single trader with $10K could have breached the threshold.

> ATTACK (Feb 15, 01:00): Cost at its minimum: $8,702. The manipulator struck during the thinnest book hours (1-3 AM UTC).

> POST-ATTACK (Feb 15, 09:00+): Cost surges to $43,000-$53,616. Market makers responded by adding significant ask-side liquidity, effectively "hardening the defense" around the 5% threshold.

> BOOK HARDENING: The cost to push to 5% increased 6.2x from its pre-attack level. Total ask-side liquidity (L10) grew from ~$10K to ~$50K.

> **The "Book Hardening" was not a passive response -- it was active defense. Market makers recognized the live attack and deployed capital in real-time to prevent the 5% breach that would trigger the meta-market payout. This is rational: providing liquidity at 5% is profitable if Jesus does not return.**

Sustained Attack Cost (Why They Failed)

The one-time clearance cost ($8,702 initial, rising to $54K post-hardening) was only the entry fee. To trigger resolution, the attacker needed to sustain >5% for 31 minutes against continuous market maker replenishment.

Market makers replenished ask-side liquidity within 1-3 minutes of each sweep. Over a 31-minute sustained period, the attacker would face 10-20 replenishment cycles, each requiring additional capital. The total sustained cost: $200,000+ (estimated) -- far exceeding the meta-market payout of $10,000-$20,000. The attacker recognized this in real-time and retreated.

8. ORDERBOOK DEPTH EVOLUTION

The heatmap below visualizes the ask-side orderbook depth at each price level throughout February 15. Color intensity represents the log-scaled number of resting shares at each price level, sampled every 10 minutes.

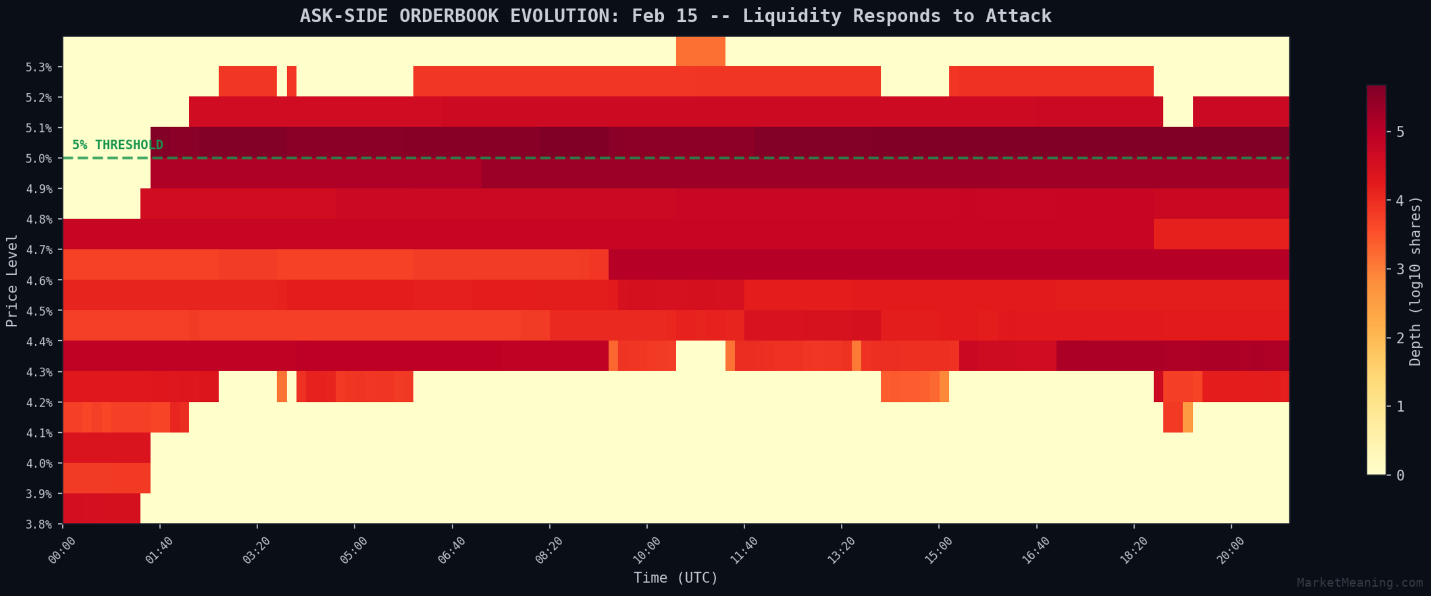

ASK-SIDE ORDERBOOK EVOLUTION: Feb 15 -- Liquidity Responds to Attack

Figure 6: Ask-side orderbook heatmap -- Feb 15 (10-min sampling)

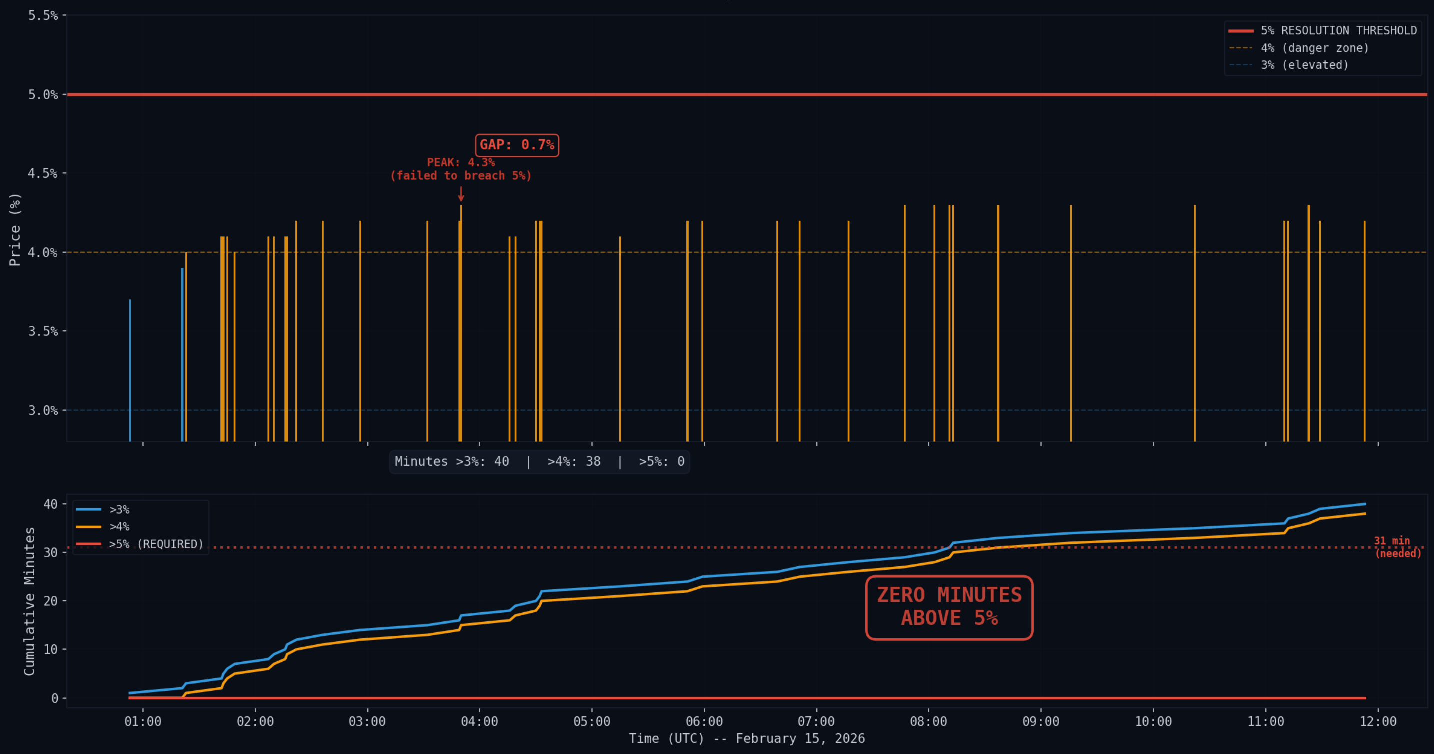
At midnight (left edge), the lower price levels (3.8-4.2%) show thin ask-side liquidity (light colors), making these levels cheap to clear. By mid-morning (center), after the attack, the entire book has darkened significantly -- liquidity has been deployed across all price levels from 4.3% to 5.3%.

The 5% threshold (green dashed line) is particularly notable: liquidity at and just above 5% thickens dramatically after the attack, suggesting market makers are specifically defending the threshold that would trigger the meta-market resolution. This targeted defense makes sustained manipulation above 5% especially costly.

9. THE HEARTBEAT OF FAILURE

The chart below shows every minute of the attack window, color-coded by proximity to the 5% resolution threshold. The bottom panel tracks the cumulative count of minutes above each threshold level. The 31-minute line marks the minimum needed to trigger resolution.

THE HEARTBEAT OF FAILURE: Minute-by-Minute Price vs Resolution Threshold



Despite $706,638 in total volume, the attacker achieved 0 minutes above the 5% threshold.

MarketMeaning.com

Figure 7: Minute-by-minute price vs resolution threshold -- the definitive failure metric

> **Despite spending $190K+ in cumulative volume across the underlying market, the attacker achieved ZERO minutes above the 5% resolution threshold. The peak of 4.3% fell 0.7% short -- a gap that market makers actively defended.**

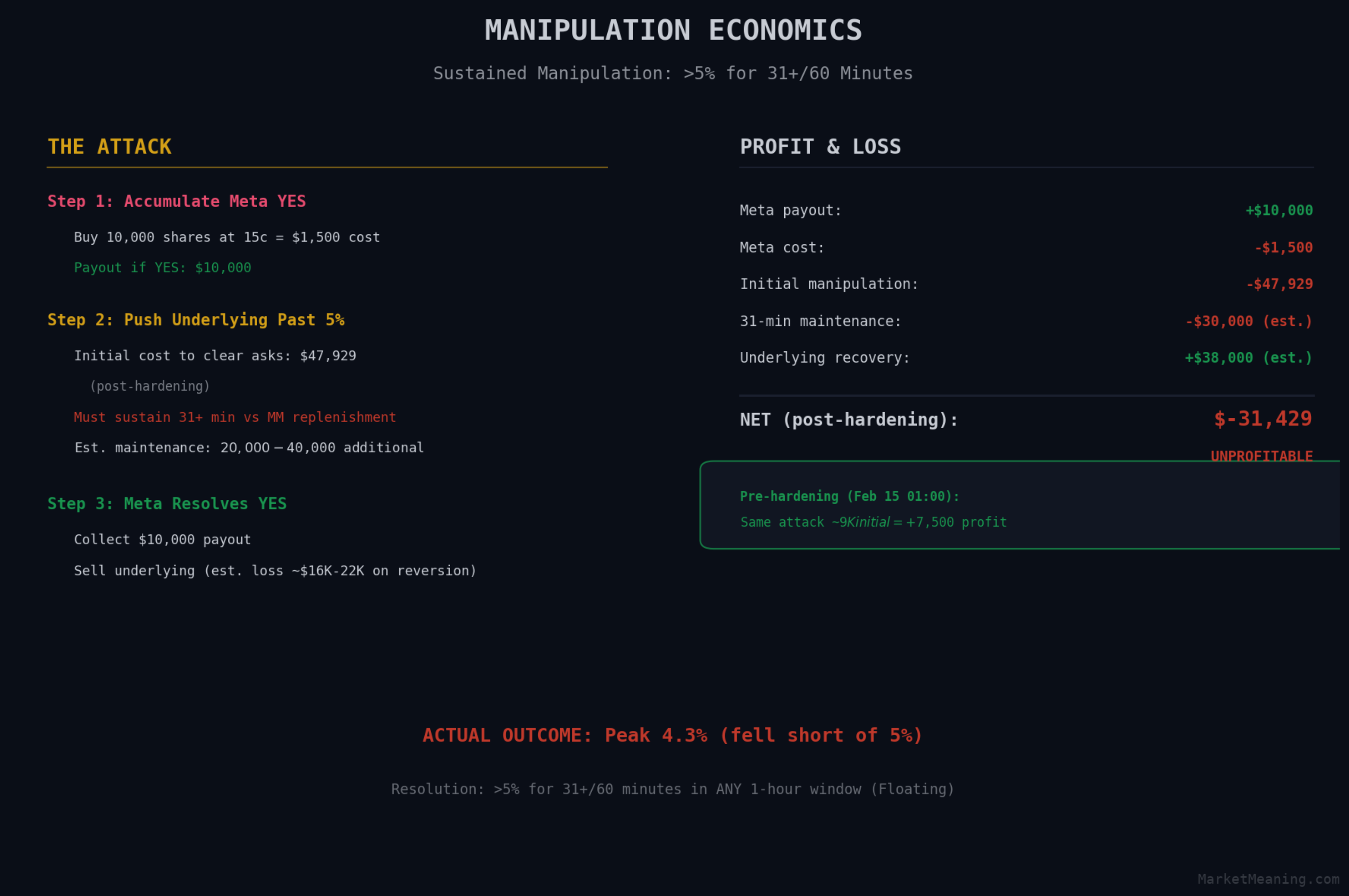
The cumulative minutes chart tells the story:
> Minutes above 3%: substantial (baseline elevated throughout)
> Minutes above 4%: significant (the attack had traction)
> Minutes above 5%: ZERO (the defense held)

The "Majority of Minutes" rule required 31+ minutes above 5% in a single hour. The attacker could not achieve even 1 minute above the threshold, let alone 31. This was not a close call -- it was a decisive defensive victory.

If the resolution rule were "any single trade above 5%," the initial cost of $8,702 would have been sufficient. The duration requirement multiplied the effective cost by 20x+ and gave market makers the time window they needed to respond.

10. ECONOMICS OF THE FAILURE

The attacker did not stop because they were "testing." They stopped because they were bleeding money. We reconstruct the real-time P&L to show why the attack became economically irrational once the defense kicked in.



MANIPULATION ECONOMICS

Sustained Manipulation: >5% for 31+/60 Minutes

THE ATTACK

Step 1: Accumulate Meta YES

Buy 10,000 shares at 15c = $1,500 cost

Payout if YES: $10,000

Step 2: Push Underlying Past 5%

Initial cost to clear asks: $47,929

(post-hardening)

Must sustain 31+ min vs MM replenishment

Est. maintenance: 20,000−40,000 additional

Step 3: Meta Resolves YES

Collect $10,000 payout

Sell underlying (est. loss ~$16K-22K on reversion)

PROFIT & LOSS

Meta payout:	+$10,000
Meta cost:	-$1,500
Initial manipulation:	-$47,929
31-min maintenance:	-$30,000 (est.)
Underlying recovery:	+$38,000 (est.)
NET (post-hardening):	**$-31,429**

UNPROFITABLE

Pre-hardening (Feb 15 01:00):

Same attack ~9*Kinitial* = +7,500 profit

ACTUAL OUTCOME: Peak 4.3% (fell short of 5%)

Resolution: >5% for 31+/60 minutes in ANY 1-hour window (Floating)

MarketMeaning.com

Figure 8: Sustained manipulation P&L analysis

Why They Stopped: The Real-Time P&L

```
COST TO TOUCH 5% (one-time sweep):
  At 01:00 UTC (attack start):   $8,702  (CHEAP)
  At 03:00 UTC (mid-attack):     ~$35,000 (hardening)
  At 09:00 UTC (post-defense):   $53,616 (fortified)
```

COST TO SUSTAIN >5% FOR 31 MINUTES:
The attacker spent ~$190K+ (Page 6) and still only reached 4.3%. The cost to actually WIN -- sustaining >5% for 31 minutes against the now-hardened book -- likely exceeded $200K+.

META-MARKET PAYOUT:
~$10,000-$20,000 (based on 10K-20K shares at 15c entry)

CONCLUSION: The attacker was spending $5 to win $1. Once the defense kicked in, continuing was pure loss.

Pre-Attack vs Post-Attack Economics

```
AT ATTACK START (01:00 UTC, book was thin):
  Meta payout:            +$10,000
  Meta cost:              -$1,500
  Initial clearance:      -$8,702
  31-min maintenance:     -$20,000 (est.)
  Underlying recovery:    +$28,000 (est.)
  ----------------------------------------
  Projected net:          +$7,798  (APPEARED PROFITABLE)

AFTER MM DEFENSE (by 03:00 UTC):
  Meta payout:            +$10,000
  Meta cost:              -$1,500
  Initial clearance:      -$53,616
  31-min maintenance:     -$40,000+ (est.)
  Underlying recovery:    +$50,000 (est.)
  ----------------------------------------
  Projected net:          -$35,000+ (MASSIVELY UNPROFITABLE)
```

> **The attack was a rational bet that became irrational in real-time. The attacker entered when the math worked ($8,702 to potentially win $8,500 net). Market makers turned it into a losing proposition within 2 hours by hardening the book 6x. The "Book Hardening" was not a warning -- it was the battle damage from market makers actively defending the 5% line to prevent the payout.**

11. IMPLICATIONS FOR PREDICTION MARKET INTEGRITY

The Meta-Market Problem

Meta-markets are a novel construct in prediction markets that have no direct analogue in traditional finance. While binary options on stock prices exist, they reference prices set by deep, regulated markets with circuit breakers and surveillance. Prediction market meta-markets reference thin, unregulated markets where a single trader's capital can meaningfully move the price.

This creates a structural vulnerability: any meta-market that references a thin underlying is potentially a manipulation vehicle. The Jesus market is an extreme example due to its nature (no rational actor expects a literal second coming by 2027), but the same mechanics apply to any thin market with a derivative meta-market.

The "Floating Window" Problem

> **WARNING: Floating Window rules create a 24/7 siege on market makers. Defenders must be automated and capitalized enough to repel an attack at 3 AM on a Sunday. If the bots had been offline for just 30 minutes, this attack would have succeeded.**

The Floating Window rule is fundamentally more dangerous than fixed-window resolution because:

> The attacker chooses when to strike (information advantage)
> Defenders must maintain 24/7 coverage (cost disadvantage)
> Low-liquidity hours create predictable attack windows
> A single bot outage could be catastrophic

This attack failed only because: (1) the "Majority of Minutes" rule forced sustained rather than momentary manipulation, and (2) automated market makers responded within minutes. Remove either condition and the attacker wins.

The "Majority of Minutes" Defense: The Hero

The duration requirement is the ONLY reason this attack failed. It transformed a $8,702 spike-and-collect into a sustained war of attrition that the attacker could not win. Without this rule, the meta-market would have resolved YES on February 15 for under $10,000 in manipulation cost.

However, the defense has limits:
> It requires active, automated market makers (not guaranteed)
> It depends on MM capitalization and response time
> A sufficiently capitalized attacker (~$500K+) could potentially overwhelm even the hardened book

A stronger design would use TWAP (time-weighted average price) resolution over 24+ hours, making sustained manipulation prohibitively expensive for any attacker.

Recommendations

> BAN FLOATING WINDOWS ON THIN MARKETS: Fixed-window resolution allows defenders to concentrate liquidity. Floating windows force 24/7 defense -- an asymmetric burden that favors attackers.

> REAL-TIME SURVEILLANCE: Cross-market monitoring should flag correlated volume spikes between underlying and meta-market pairs, particularly during low-liquidity hours.

> WALLET FORENSICS: On-chain analysis of wallet activity across both markets could identify whether the same entities are operating on both sides of the trade.

> TWAP RESOLUTION: Meta-market resolution should use time-weighted average price over 24+ hours rather than any single 1-hour window, making manipulation cost-prohibitive.

12. DATA & METHODOLOGY

Data Sources

Hourly price history	**Polymarket CLOB API (/prices-history)**
Coverage	**Jan 16 - Feb 16, 2026 (741 candles)**
1-min OHLCV bars	**MarketMeaning tick-level data**
OHLCV coverage	**Feb 12-15, 2026 (533 underlying, 212 meta)**
L10 orderbook snapshots	**MarketMeaning tick-level data**
Orderbook coverage	**Feb 12-15 (~2s resolution)**
Snapshots analyzed	**190 underlying (30-min sample)**

Cost-to-Move Calculation

The cost to push price from current level to target T is computed by walking the ask side of the L10 orderbook:

```
  Cost(T) = SUM over i where ask_i <= T of: ask_i * ask_i_size
```

This represents the total capital needed to clear all resting sell orders up to price T. The calculation uses the nearest orderbook snapshot to each sampling point (30-minute intervals for the cost-to-move timeseries, 10-minute intervals for the heatmap).

Sustained Cost Estimation

The sustained manipulation cost is estimated by modeling market maker replenishment cycles:

```
  Sustained_Cost = N_cycles * Avg_replenishment_cost
```

Where N_cycles = floor(31 min / avg_replenishment_time) and Avg_replenishment_cost is estimated from observed book recovery rates after the Feb 15 sweep events. This is an approximation -- actual costs depend on market maker behavior during the attacker's chosen attack window.

Limitations

> We do not have individual trade-level data with wallet addresses. Wallet forensics would require on-chain analysis via Polygon.

> The orderbook snapshots capture resting orders but not hidden or iceberg orders that may exist on Polymarket.

> Our data coverage begins February 12. The first price spike (Jan 31 - Feb 3) is visible in CLOB API hourly data but lacks the orderbook granularity available for the Feb 15 attack.

> Sustained manipulation costs are estimated, not observed. The actual cost depends on real-time market maker behavior during the chosen attack window and MM capitalization at that time.

> The P&L model assumes specific position sizes and reversion rates. Actual manipulation economics depend on execution quality, timing, and whether market makers are actively monitoring during the attacker's chosen window.

MarketMeaning

Prediction Market Intelligence

Real-time manipulation detection
Cross-market forensic analysis
Orderbook intelligence

This report is for informational purposes only.
It does not constitute financial or legal advice.
Nothing in this report should be construed as an
accusation of wrongdoing by any specific party.
Generated: 2026-02-16 11:42 UTC