Address Poisoning Losses Surged 13× After Ethereum's Fusaka Upgrade

TL;DR

- Fusaka reduced gas fees 6×, making mass poisoning spam cheap enough to scale
- This helped attackers increase poisoning volume 5.6×
- In 73 days after Fusaka, victims lost $63.3M
- This is 13× more than in the same period before the upgrade ($4.9M)

In my previous article, I wanted to find out what caused the record-high activity on the Ethereum network, and it turned out that 80% of the growth was address poisoning spam, made economically attractive by the Fusaka upgrade reducing gas fees 6 times. At the time, I only had limited data that answered the question of what was behind the growth.

Address poisoning — an attack where scammers send tiny or zero-value transactions from addresses that match the first and last characters of the victim's real contacts, hoping the victim will copy the wrong address from their transaction history.

In this article, I researched how address poisoning grew overall and what the actual results of these attacks were. What's the total damage?

To answer this question, I built a detection pipeline that scans the Ethereum blockchain from September 1, 2025, through February 13, 2026, covering 93 days before Fusaka and 73 days after. It tracks dust transfers across 101 tokens, and identifies confirmed payoffs.

[Chart 1: Daily poisoning transactions]

Before Fusaka, attackers were sending an average of 30,000 dust transactions per day. After the upgrade, this jumped to 167,000 per day, a 5.6 times increase.

The January spike reached 510,000 transactions in a single day. Even excluding that spike, the sustained post-Fusaka level remains at 150,000–200,000 daily transactions.

Fusaka — a major Ethereum network upgrade (December 3, 2025) that expanded the network's capacity to process more transactions at once, making them cheaper. The upgrade is part of Ethereum's effort to attract mass adoption by reducing fees.

[Chart 3: Gas price vs. dust attack volume]

The chart shows a clear inverse correlation between gas price and dust attack volume. If the post-Fusaka spike in attacks were simply a coincidence, attack volume would have shifted

once and stayed flat regardless of daily gas fluctuations. Instead, the two variables move together continuously: when gas spikes, dust output drops; when gas dips, dust output rises. This dose-response relationship is a strong indicator that the link is causal rather than coincidental.

A dose-response relationship means the effect scales with the exposure: the bigger the dose, the bigger the response. It is one of the Bradford Hill criteria, a standard framework for distinguishing genuine causes from spurious correlations. Applied here, gas price is the dose and attack volume is the response.

Because attackers adjust their output day by day in proportion to gas cost, the data rules out the possibility that both trends shifted around the same time for unrelated reasons.

The day-level precision of this correlation likely means that the poisoning software has a built-in gas price threshold that regulates attack intensity automatically. Such settings are common across both legitimate and malicious Ethereum bots.

[Chart 2: Daily unique victim wallets targeted]

The number of unique wallets receiving poisoning dust rose from 12,000 per day to 38,000 per day, a 3.1 times increase.

Comparing equal 73-day windows before and after Fusaka:

- Pre-Fusaka (Sep 21 – Dec 2): $4.9M stolen
- Post-Fusaka (Dec 3 – Feb 13): $63.3M stolen

This is a 13-fold increase in stolen funds and a 2.6-fold increase in successful payoff events.

One transfer accounts for a large share of the post-Fusaka total: $50 million in USDT on December 19. Excluding it, the post-Fusaka total is still $13.3M, a 2.7-fold increase over the pre-Fusaka rate.

The $50M case is not an anomaly to be excluded. Address poisoning is a lottery-model attack with millions of cheap dust transactions for a few rare, large payoffs. This is how the attack is designed to work. Cheaper gas means more lottery tickets, which means higher odds of catching a whale.

The link between low fees and attack volume was already documented before Fusaka.

- A Carnegie Mellon University study published ten months before the upgrade found "a higher attack prevalence in chains with lower transaction fees."
- Seven months before the upgrade, Jameson Lopp of Casa concluded that address poisoning is only economically feasible in low-fee environments.

- A Penn State study published three months before Fusaka tested 53 Ethereum wallets and found that most failed to warn users about poisoning transfers.

Despite this, the Ethereum Foundation proceeded with the Fusaka upgrade.

Address poisoning is not the only attack type whose economics depend on gas cost. Sandwich attacks, fake token airdrops, sweeper bots on compromised wallets, and mass approval drains all become more profitable as fees drop.

There is nothing wrong with lowering fees, but the security problems that cheap transactions amplify should have been addressed before the upgrade. When the Ethereum Foundation claims it is building trillion-dollar security, user safety must be the strictest priority over growth metrics.

Methodology

The detector runs as a single SQL pipeline on Google BigQuery's public Ethereum dataset. It first identifies all legitimate ERC-20 and ETH transfers ≥$1 and extracts a fingerprint for each recipient address (first 3 + last 4 hex characters). It then detects poisoning by matching lookalike addresses against these fingerprints: zero-value ERC-20 transfers initiated by third parties, and ERC-20 or ETH dust transfers <$1 sent to victims within a 300-block window. A confirmed payoff is any subsequent ERC-20 or ETH transfer ≥$10 from the victim to a lookalike address.

The charts in this article display dust transfer activity only, as dust transfers are the primary measurable attack vector. Zero-value transfers are not shown on the charts but are used internally by the detector to build a complete map of victim-to-lookalike address pairs.

All 101 tokens are priced using weekly snapshots (23 dates). Contract addresses are excluded from the victim pool. The pipeline also filters out burn addresses, self-transfers, transfers not initiated by the victim, and cases where the lookalike was a known legitimate recipient before the poisoning event. One bot address that generated thousands of automated micro-transfers to poisoned addresses was excluded from payoff statistics.

The detector undercounts both attacks and payoffs. It only catches poisoning against addresses that made at least one transfer ≥$1 during the study period, and only tracks 101 tokens. The $68M figure is a confirmed lower bound. However, testing with various samples of tokens outside the whitelist showed that attacks involving unlisted tokens account for less than 1% of the total.

This study tracked two types of poisoning transfers: dust transfers and zero-value transfers. There are also other types, including counterfeit token transfers, fake ETH transfers, and approval-based variants. I did not include them because building such queries is significantly more complex and running them on BigQuery is expensive. Dust and zero-value transfers are

sufficient to see the full picture, because attackers typically combine several different methods against the same target, and cases where a victim receives only a counterfeit token transfer without accompanying dust or zero-value poisoning are rare.