Title: Worm-Assisted Filter Surveillance Attack on Monero

Summary
This research presents a novel Tier-1 level cyber threat model targeting the Monero (XMR) privacy cryptocurrency. The model outlines how a nation-state adversary can use entropy-based filters and behavioral worms to trace Monero transactions and identify real wallet locations -- bypassing traditional defenses like Dandelion++, ring signatures, and decoys.

Objective
To demonstrate how combining network-wide worm deployment and high-entropy packet filtering enables deanonymization of privacy coin users at scale.

Core Techniques Used

- Entropy Filtering: Detecting encrypted Monero packets due to high randomness in data.
- Worm Activation Logic: Worms remain dormant until Monero-like traffic is seen.
- Behavioral Analysis: Worms probe system to differentiate real vs. decoy wallets.
- Nationwide Surveillance: Assumes ISP-level access across all routers and nodes.

Threat Model Details

- Adversary Level: Tier-1 (nation-state)
- Capabilities:
    - Full access to ISP backbone
    - Filtering encrypted traffic
    - Worm deployment to endpoints
    - Behavioral monitoring of wallet activity
- Goal: Identify receiver's device, location, and break Monero’s endpoint privacy

Why It Matters
Even with strong cryptography, Monero can be compromised at the network and behavioral level, especially under nation-controlled cyberspace.

Possible Defenses

- Use of cold wallets with no network exposure
- Decoys that mimic real wallet behavior
- Transaction broadcasts via foreign relays or I2P mixnets
- OS hardening via Whonix or Tails

Author & Info

Author: Sidhant Negi
Date: June 2025
Status: Research Draft (Open for peer review or collaboration)