peer-observer

bitcoin P2P attack and anomaly detection

Idea

- Run Bitcoin Core “honeynodes” on mainnet in different configurations
- Attach monitoring for
  - P2P in/outbound messages
  - P2P connections opened, closed, evicted, misbehaving, …
  - Mempool changes, addrman changes, connectblock timings, …
  - …
- then:

detect ⇒ analyse? ⇒ react?

- Goal
  - detect attacks & network anomalies
  - test PRs and RCs

Current status

- Infrastructure-as-Code using NixOS: declarative and reproducible
- 12 Bitcoin Core nodes running
  - 8x `x86_64` and 4x `aarch64`
  - 4 continents
  - 3 hosters
  - 1 full-node (with block filters), 11 pruned nodes
- Metrics exporter and Grafana Dashboards
- Attached fork-observer and addrman-observer
- Historical debug logs with categories: `net`, `validation`, mempool, …
- Tooling to detect spynodes, ping-spammers, …
- Currently running 27.0rc1 and 26.1rc2

Next steps

- Anomaly detection and more metrics
- Alerting on anomalies or known attacks
- Summer of Bitcoin project
- Onboard interested developers

Demo time

peer-observer