Long-Term Persistence of Attacker Infrastructure Across DNS Intelligence and Honeypot Observations

IETF Lightning Talk

Yuanyuan Zhou
University College London (UCL)
Yuanyuan.zhou.23@ucl.ac.uk

Motivation

Security Observation Layers

Large Honeypot Collection

Attacker Behaviours

DNS Threat Intelligence(TI)

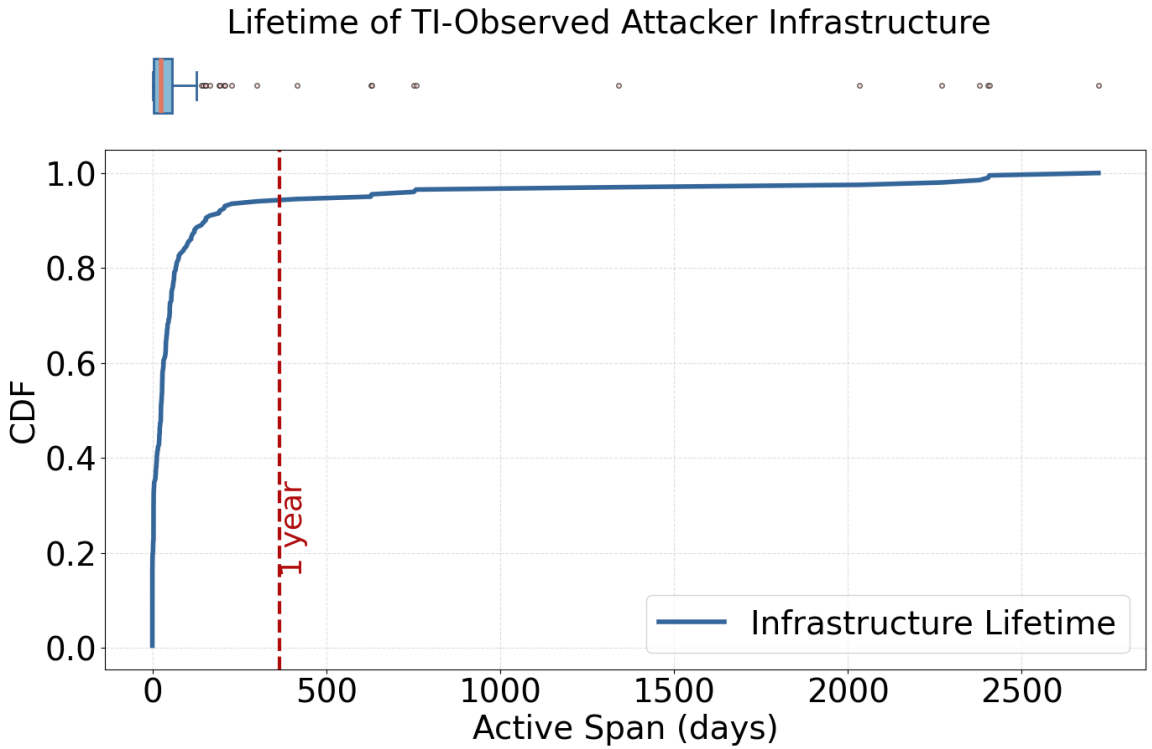
Infrastructure Reputation

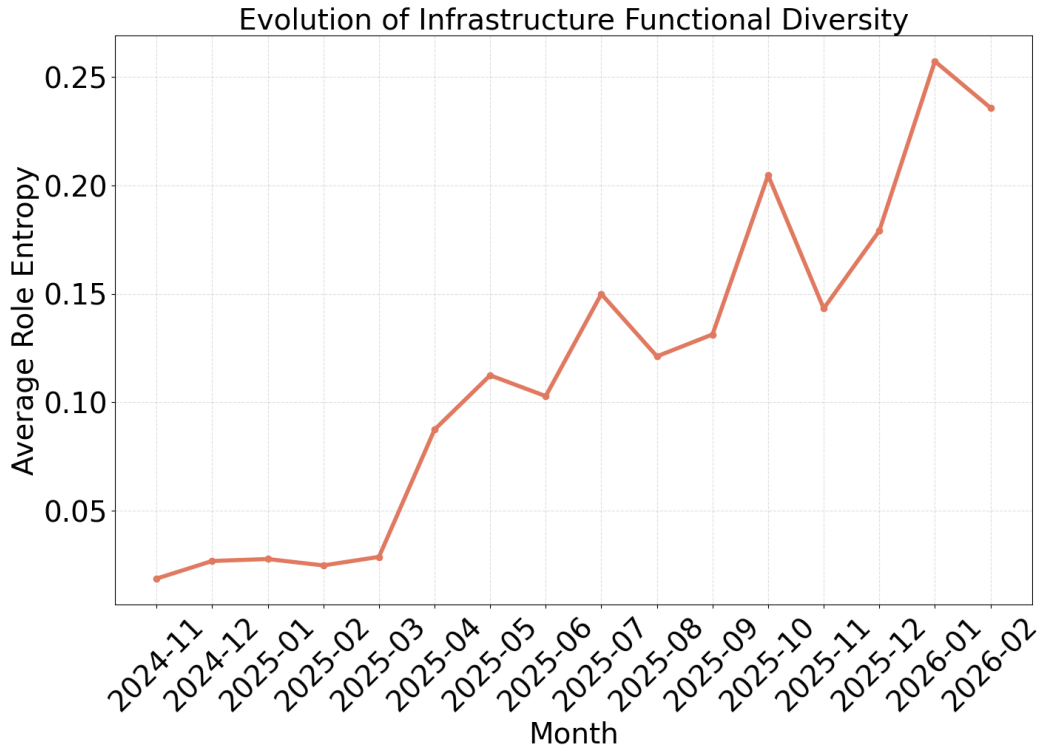
- Security systems observe attacker infrastructure from **different perspectives**
- Honeypots capture **interaction behaviour**
- DNS threat intelligence captures **infrastructure roles**

Understanding Persistent Attacker Infrastructure

Attacker Infrastructure Persistence

Observation window **Nov 2024 – Feb 2026**

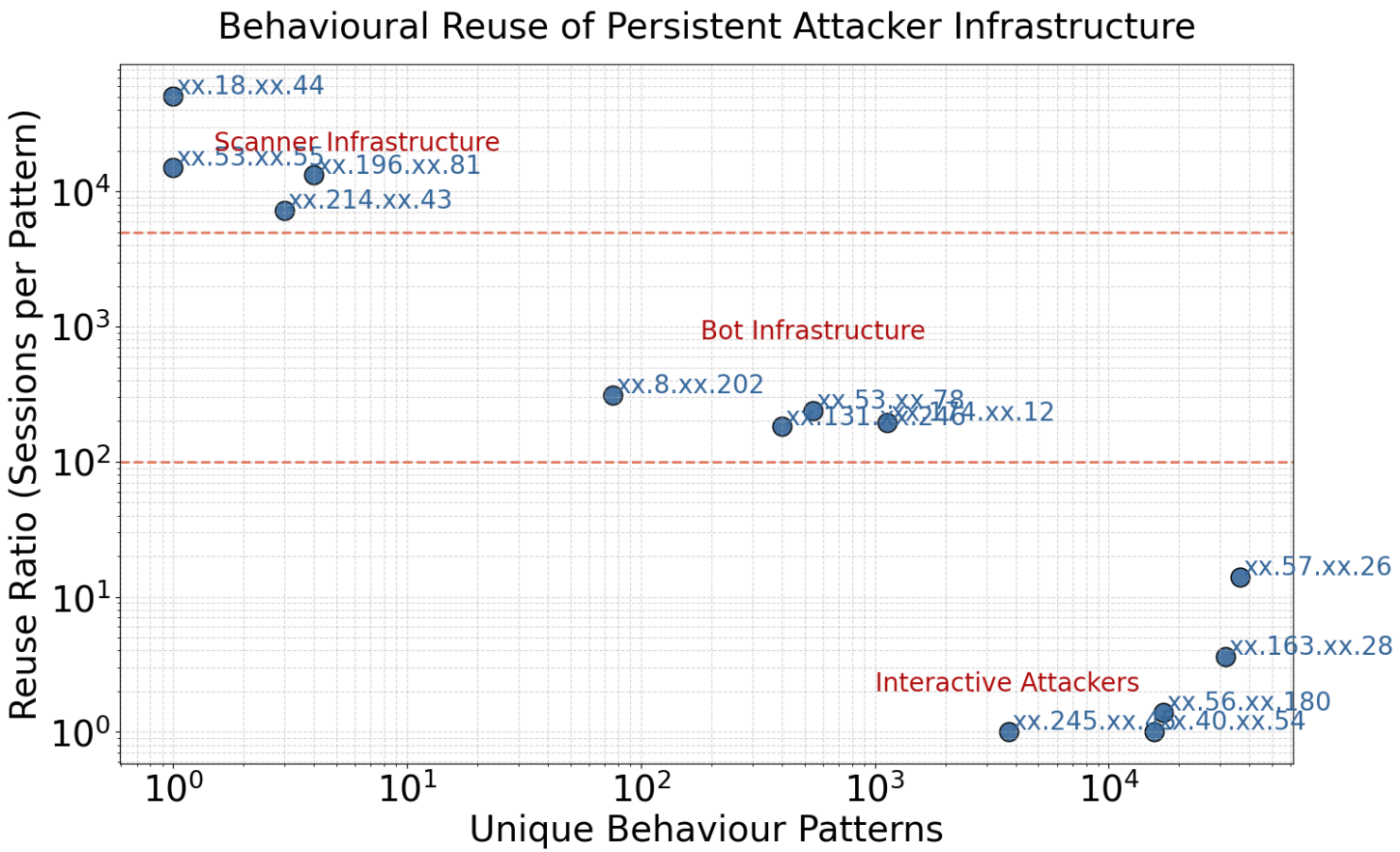




- Most attacker infrastructure is short-lived.
- However, a **small fraction persists for very long periods**

- The infrastructure ecosystem becomes **more functionally diverse**.
- More infrastructure roles emerge over time.

Behaviour of Persistent Infrastructure



Persistent infrastructure exhibits different behaviours

- **Automated scanners**

  repeated simple behaviour
- **Semi automated attackers**

  botnet scripts / exploitation frameworks
- **Interactive attackers**

  manual sessions and command execution

Takeaway

- A small number of infrastructure nodes drive many attacks
- Long lived infrastructure may evade detection if TI visibility is short
- Combining **behavioural observation (honeypots)** and **infrastructure intelligence (DNS TI)** provides a richer view

Looking for feedback and discussion with researchers and operators working on DNS abuse, Internet measurement, and attacker infrastructure.

Yuanyuan Zhou
University College London
yuanyuan.zhou.23@ucl.ac.uk

SafeNetIoT
SECURING THE IOT