DNS Abuse Activity Reporting

Tracking DNS abuse by ICANN SSR

Dr. Samaneh Tajalizadehkhoob

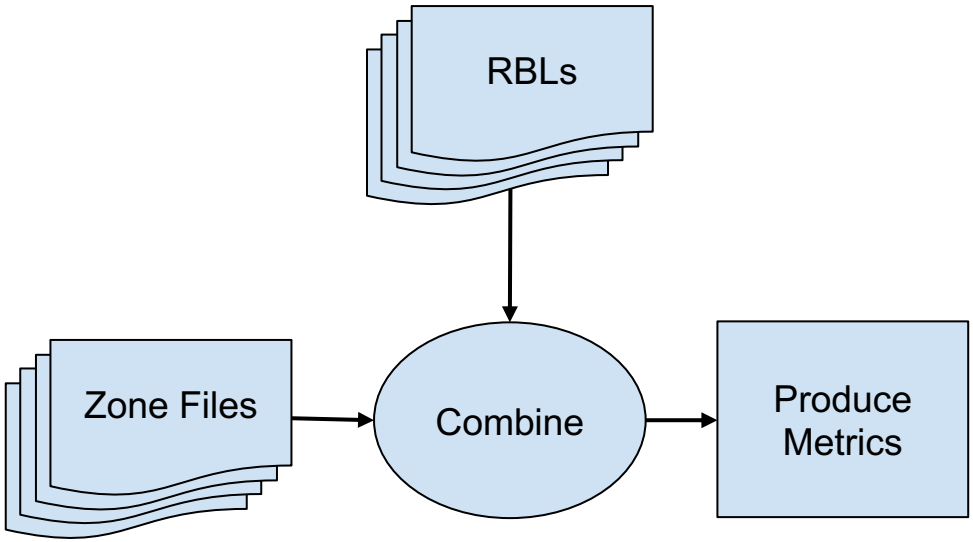
24 October 2023

GAC Discussion on DNS Abuse ICANN 78

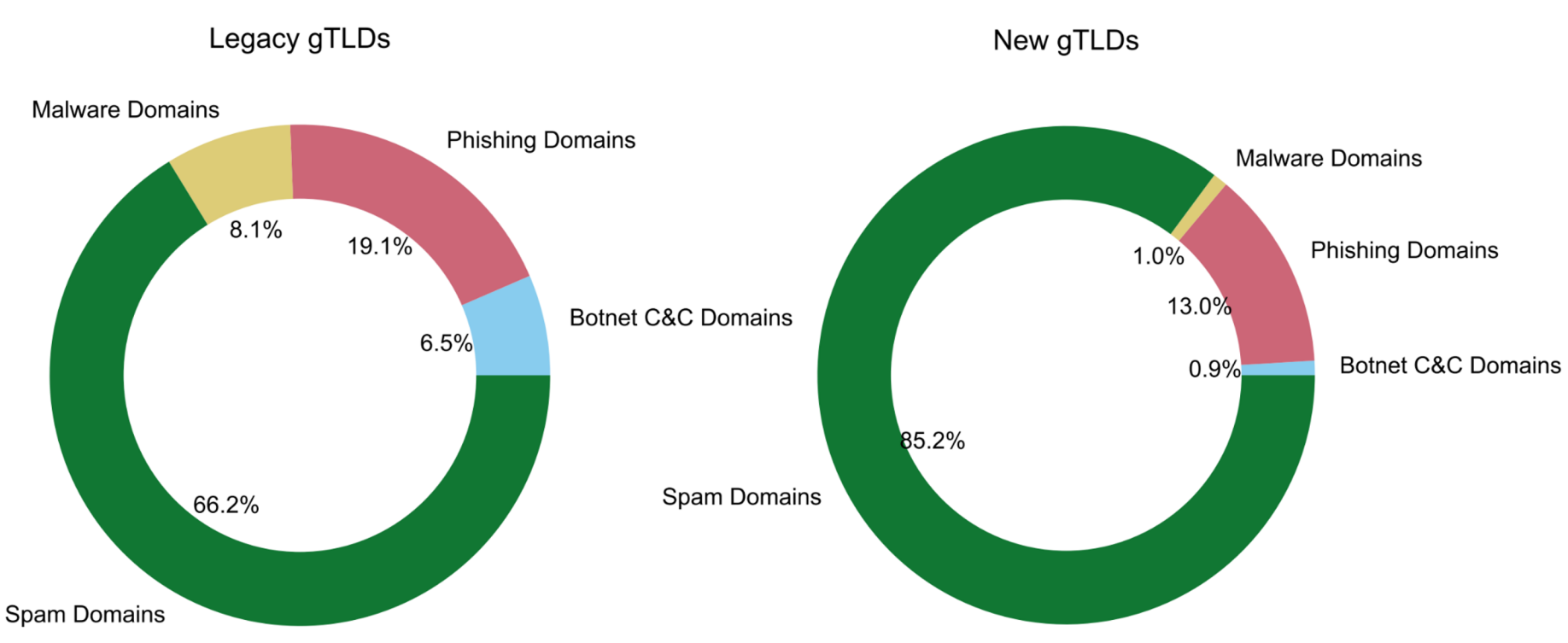
DAAR (Domain Abuse Activity Reporting)

- Aggregate data from **RBLs** at TLD level (**count per TLD**)
- Combine with **count of domains** from **zonefile**
- Maintain **consistent** methodology since October **2017**
- **Monthly** reports
- **Daily** access through the API
- Longer term trends

DAAR (Domain Abuse Activity Reporting)

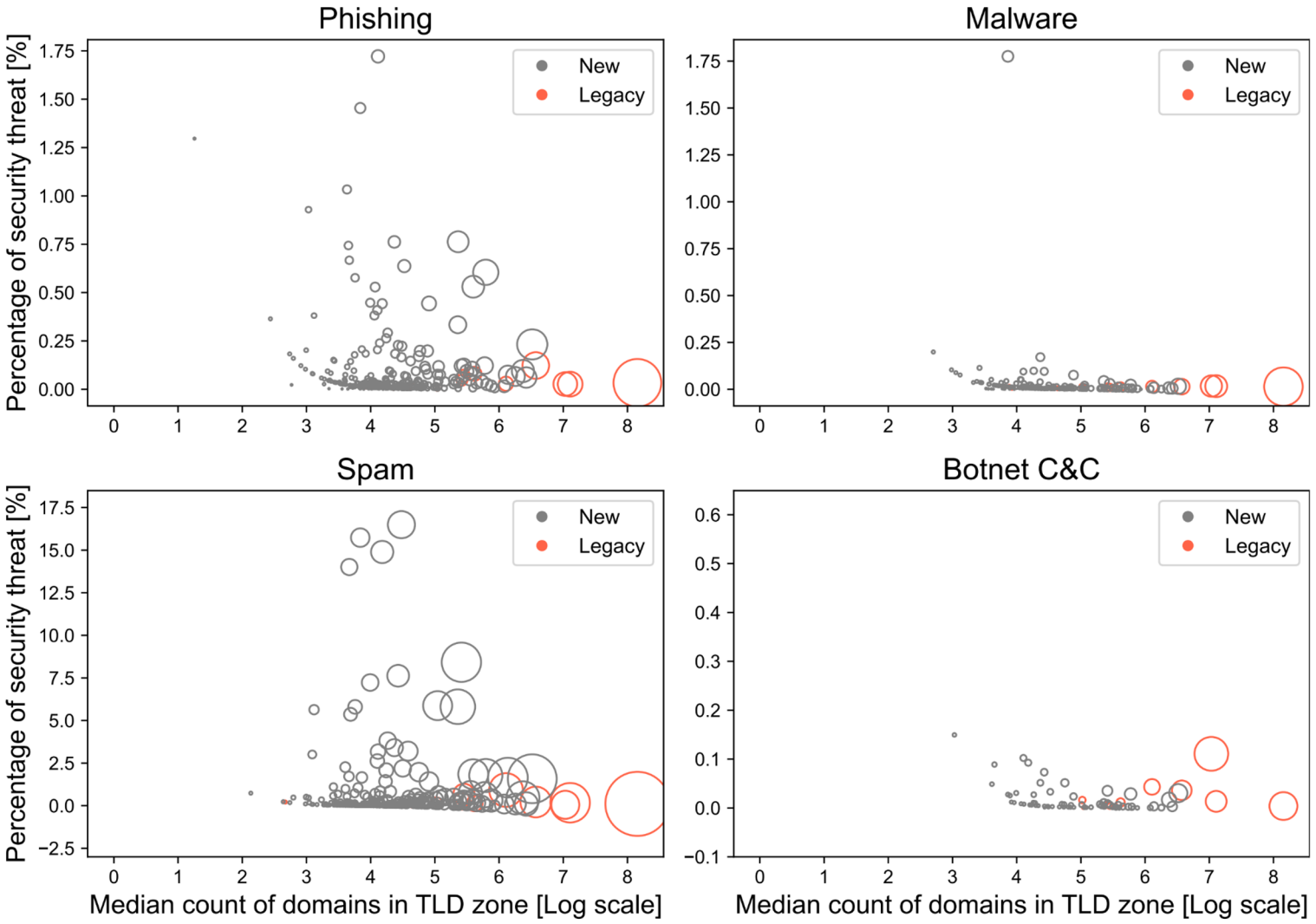


Overview



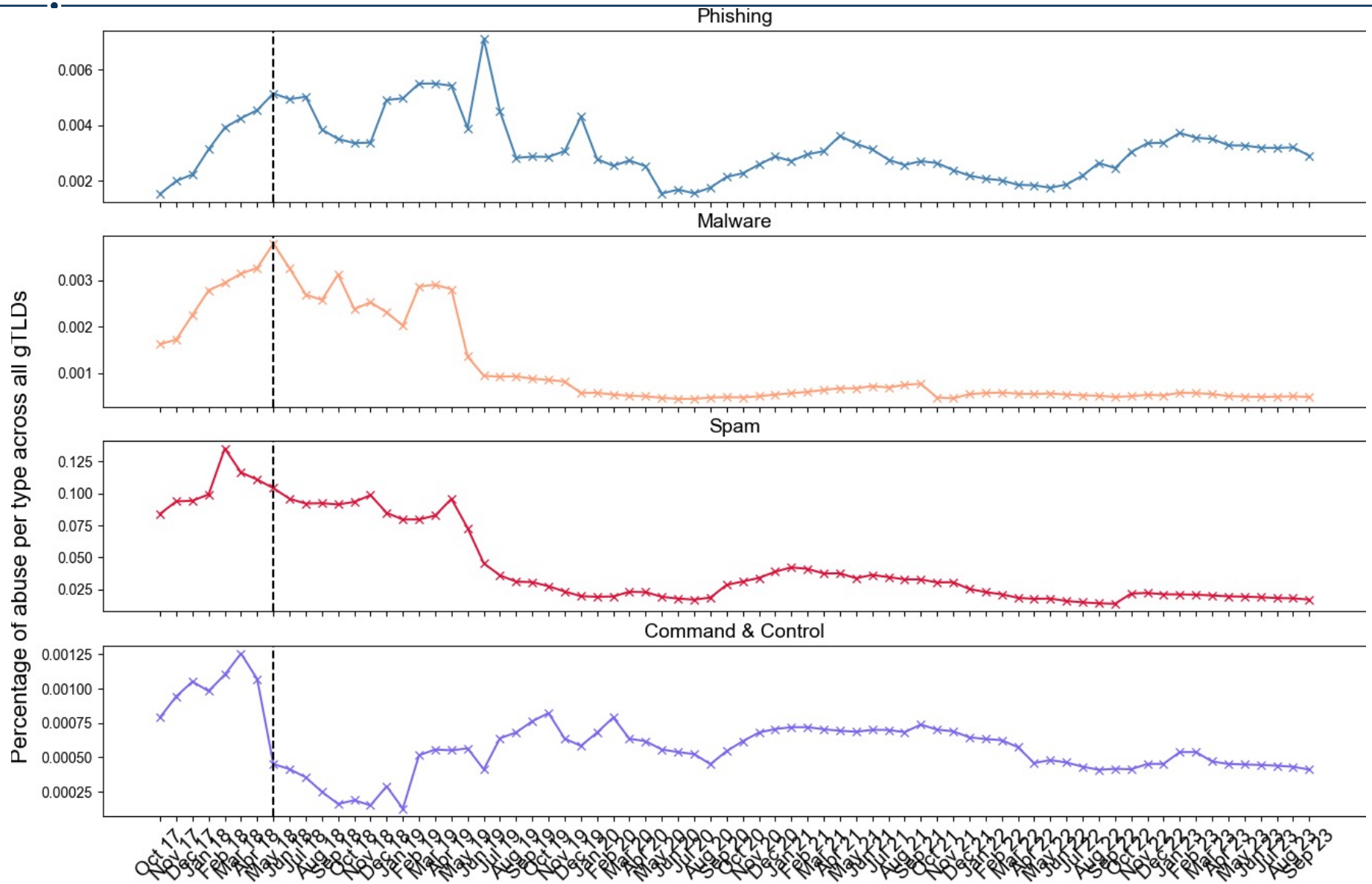
(Legacy gTLDs are those delegated pre-2010)

Differences between TLDs



Circle size indicates median threat counts [square root]

Trends of DNS Abuse Percentage



DAAR Project Uses, and Limitations

- DAAR data **CAN** be used to
  - Report on threat activity at TLD level
  - Historical analysis of security threats or domain registration activity
  - Help TLD operators understand their reputations in the DAAR RBLs or the impact of their anti-abuse programs or terms of service
- DAAR data **CANNOT** be used to
  - Aggregate domains to the registrar level
  - Provide info about mitigation
  - Distinguish maliciously registered vs. compromised domains
  - Provide information on individual security threats within domains
  - Rank TLD providers in terms of their security concentrations

What is Next?

ICANN's Next Platform

It's a Measurement Platform

- Modular
- M1: **registry** and **registrar** metrics, visuals and stats accessible via a
  Dynamic dashboard
  API
- Search functionality that allows for domain level RBL access [with a limit]
- ccTLDs that are participating can also see their RBL domains [with a limit]

Future Plans

- Adding more ccTLDs
- DAAR Evolution
  - Provide domain level sharable RBL data
  - Registrar level metrics
  - Measure uptime (Security Threat Persistence Metrics)
  - Malicious registrations vs. Compromised domains
  - Parked page detection
  - Security threat prediction
  - Improved threat classification
  - Dynamic dashboard
  - API
  - Others …