RIPE 78

Reykjavík, Iceland
20 - 24 May, 2019

RIPE Meetings: connecting the Internet community

ripe78.ripe.net

Domain Abuse Activity Reporting (DAAR)

Samaneh Tajalizadehkhoob
ICANN’s Office of CTO

Outline

- **DAAR definition**
- DAAR data collection & methodology
- DAAR analytics
- Next steps & RIPEstat

Motivation

“Systems are particularly prone to failure when the person **guarding** them is not the person who **suffers** when they fail.”

Therefore,

Insecurity is as much an **incentive** problem as it is a **technical** problem

Ross Anderson, 2001

Problem

A **growing** need for proactive detection and mitigation strategies by TLD operators & registrars

But there is lack of knowledge about

- Abuse concentrations in TLD networks
- Operators' abuse performance in comparison to their peers

Domain Abuse Activity Reporting (DAAR)

What is DAAR?

A system for reporting on domain name registration and abuse data_across TLD registries and registrars

Outline

- DAAR definition
- **DAAR data collection & methodology**
- DAAR analytics
- Next steps & RIPEstat

Data Sources

1. DNS zone data
2. WHOIS
3. Open source or commercial abuse threat or reputation blacklist (RBL) data*

*Certain data feeds require a license or subscription

Data Collection in a Nutshell

CZDS

TLD 1

TLD 2

1

List of domains in zone

DNS Zone Data

2

WHOIS

3

Blacklist/Blocklist

DAAR Reputation Metrics per Registry

Reputation Block Lists: Identifying Threats

DAAR collects domain data for

- Phishing
- Malware
- Spam
- Botnet Command & Control

Current Reputation List

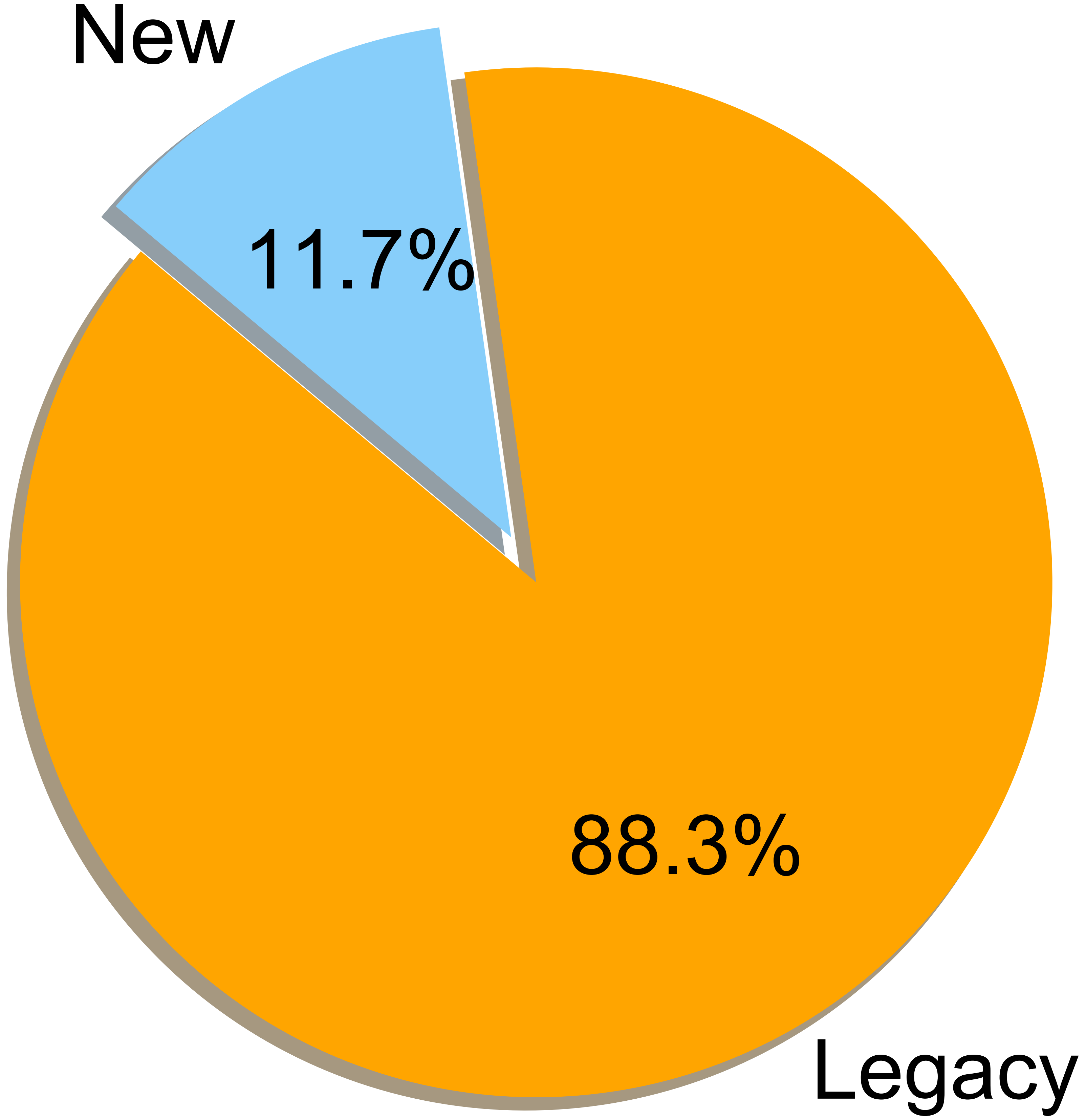
Domains only

- SURBL lists (Spam – Phishing - Malware)
- Spamhaus Domain Block List (Spam - Phishing - Malware - Botnet C&C)
- Anti-Phishing Working Group (Phishing)
- Malware Patrol (Malware, Ransomware, Botnet C&C)
- Phishtank (Phishing domains)
- ABUSE.CH (Ransomware tracker, Feodo tracker)

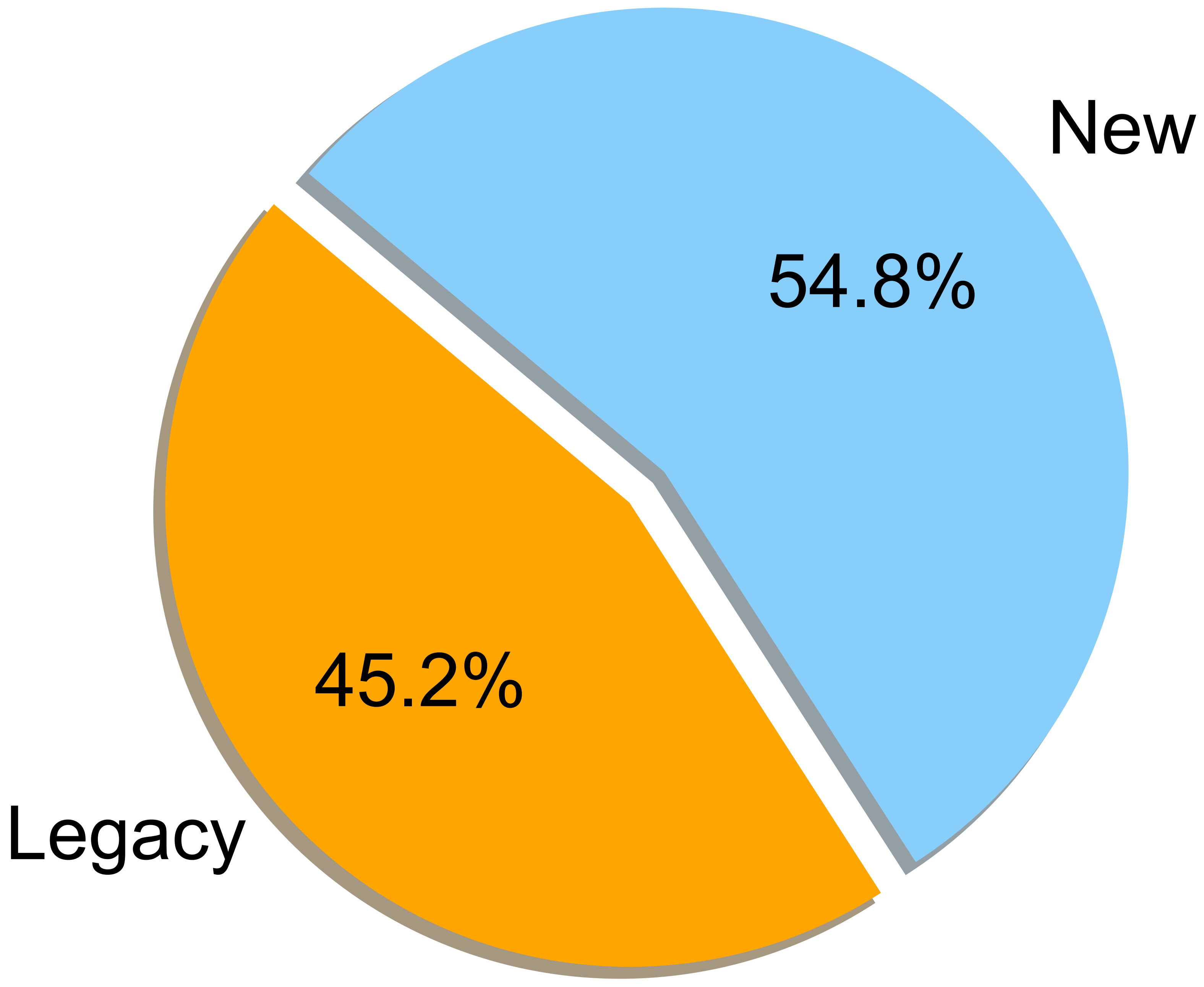
Outline

- DAAR definition
- DAAR data collection & methodology
- **DAAR analytics**
- Next steps & RIPEstat

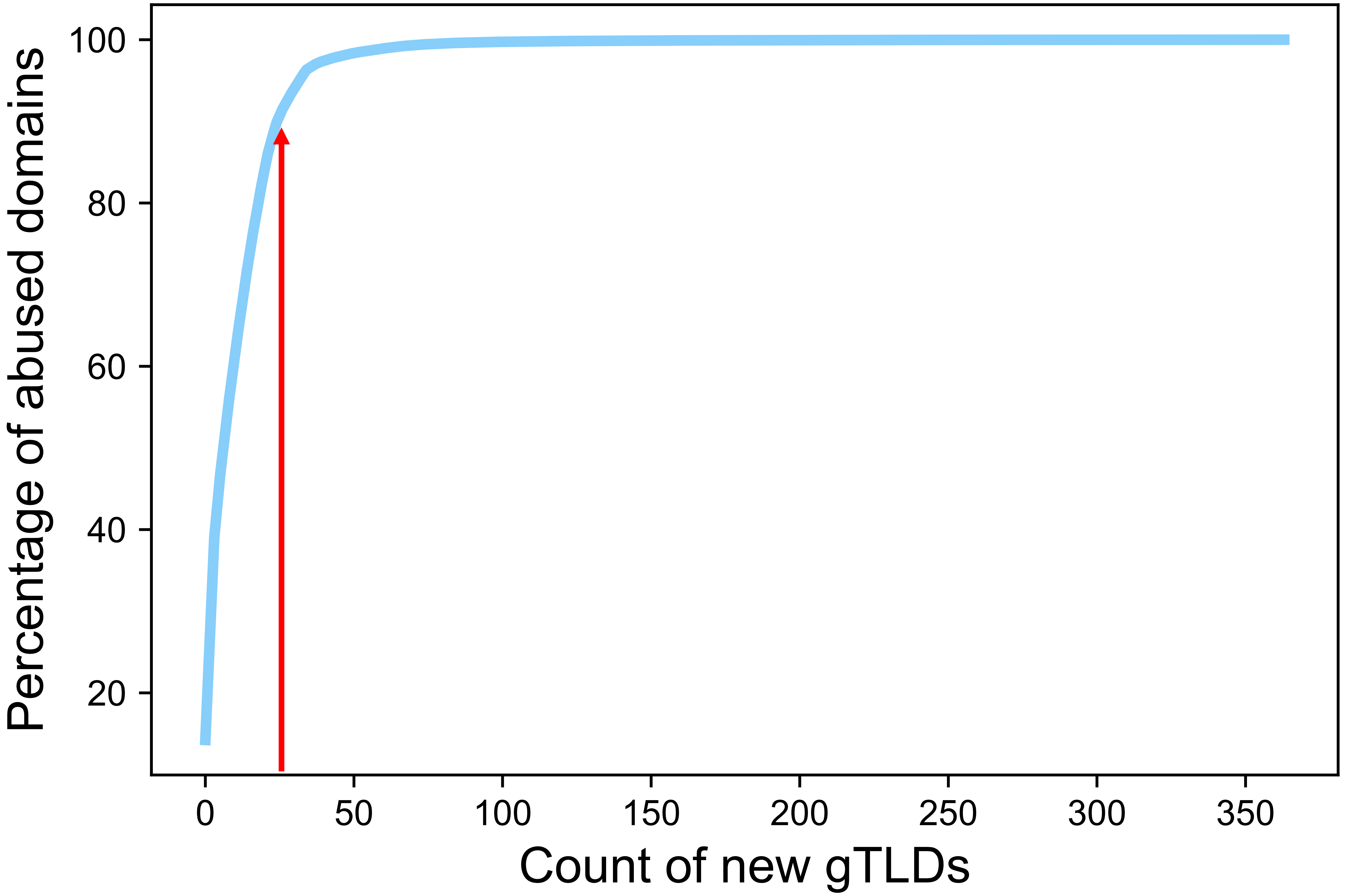
Distribution of Domains in gTLD Zones



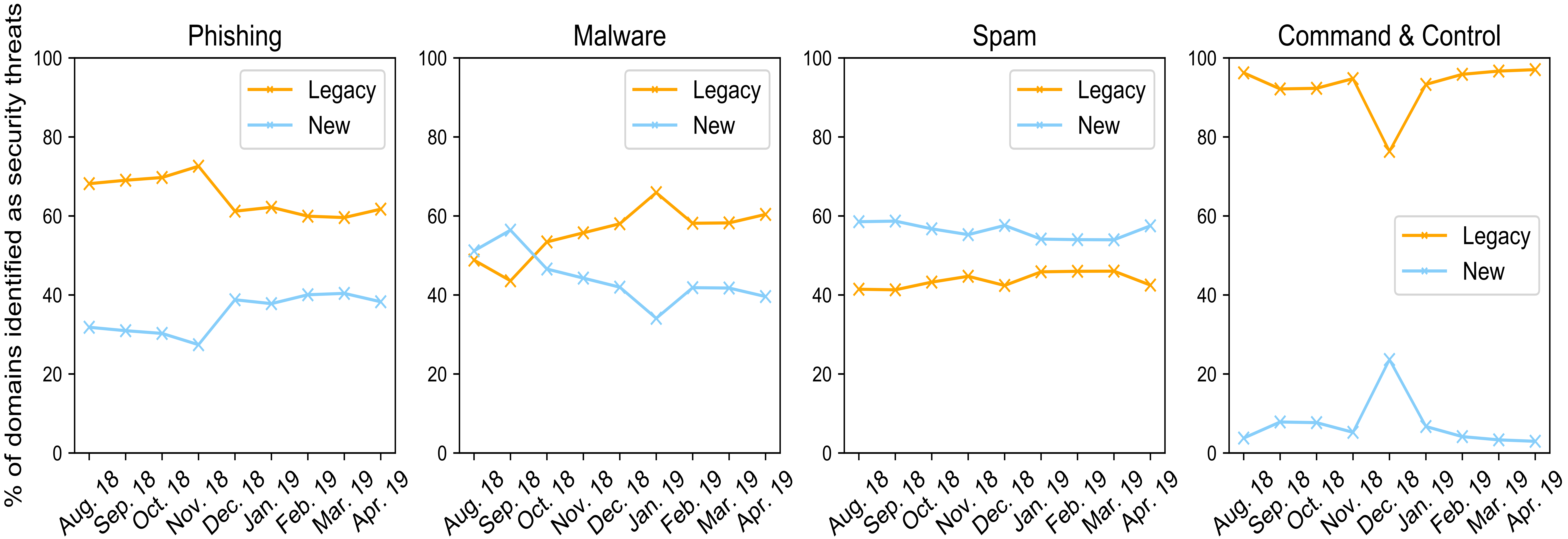
How Many gTLDs are Driving the Bulk?

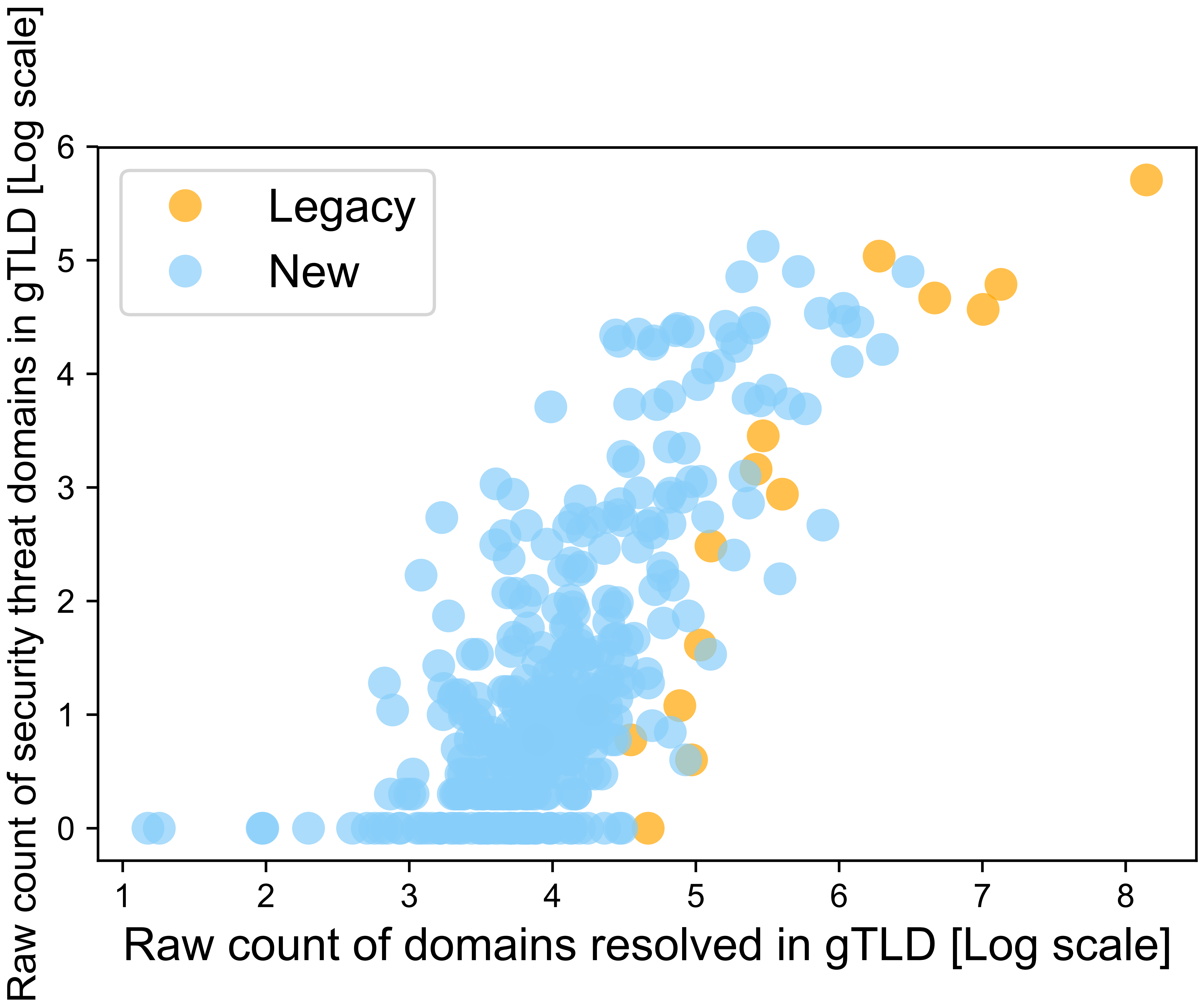


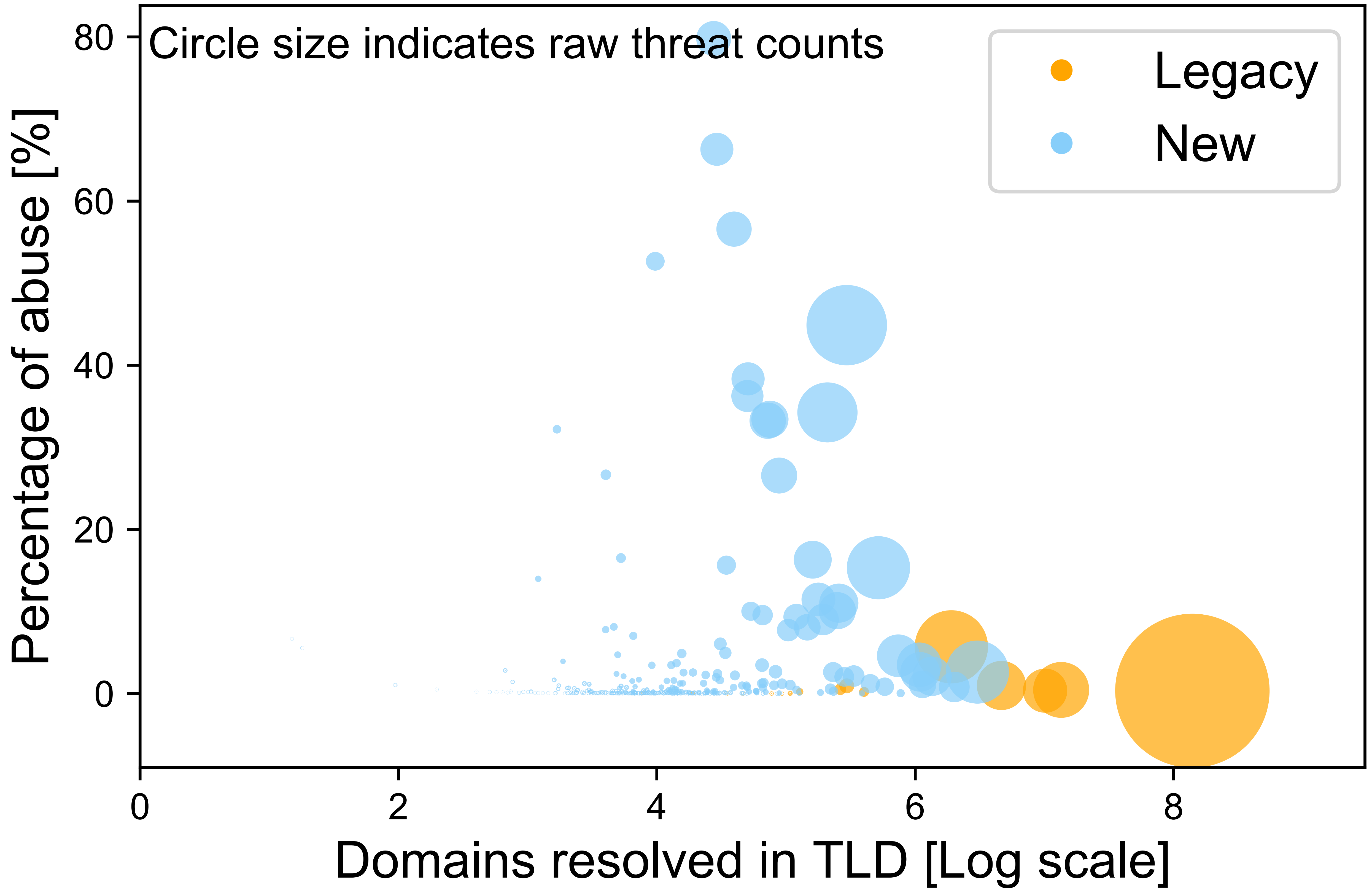
Abused



Abuse Type Breakdown







Abuse: raw counts vs normalized counts

Outline

- DAAR definition
- DAAR data collection & methodology
- DAAR analytics
- **Next steps & RIPEstat**

RIPEstat: Abuse Reporting

- Upcoming feature to be integrated into the RIPEstat
    - Domain/IP/Prefix/ASN Level Abuse Reporting
    - Diverse abuse threat types
    - Aggregated and longitudinal abuse metrics

- Initial steps
    - Develop a criteria for evaluating abuse reputation feeds
    - Maintain and aggregate abuse feeds
    - Create snapshot and longitudinal abuse analytics
    - Continuously update the approach based on the feedback from the community

Question or Comments?

Contact us:

Daar@icann.org

Samaneh.tajali@icann.org

John.crain@icann.org

Check our recent article about “Website Popularity Rankings” on the RIPELab

https://labs.ripe.net/Members/samaneh_tajalizadehkhoob_1/the-tale-of-website-popularity-rankings