

# Measuring DNS Abuse

DNSAI: Compass™

Rowena Schoo,  
Director of Programs and Policy,  
DNS Abuse Institute

# About the Institute

- Created and funded by Public Interest Registry (PIR / .org) in service of its public interest mission
- Operating since 2021
- Outward, industry focused
- External multi stakeholder Advisory Council
- No revenue or cost recovery generating activities
- DNS Abuse: technical abuse: phishing, pharming, malware, botnets, and spam\*

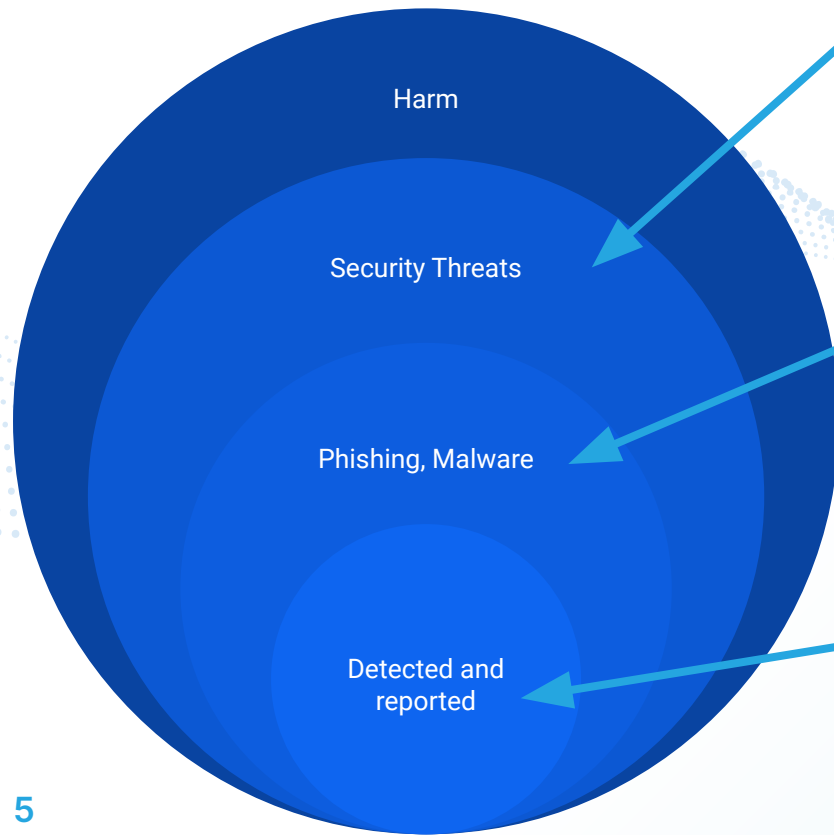
# DNSAI: Compass

Measuring phishing and malware

# Compass

- Why?
- What?
  - A comprehensive, consistent, independent, academically robust metric DNS Abuse
  - Prevalence and persistence of phishing and malware
  - Collaboration with [Kor Labs](#) (Prof. Korczynski, @Grenoble Alpes University)
- Public reporting:
  - <https://dnsabuseinstitute.org/dnsai-compass/>
  - 12+ months or aggregated reporting
- Private reporting:
  - Dashboards for every TLD and Registrar
  - Bespoke analysis – today

# What?



Starting with technical abuse/security threats – most widely accepted

Focus on harms we (KOR Labs) could reliably evidence

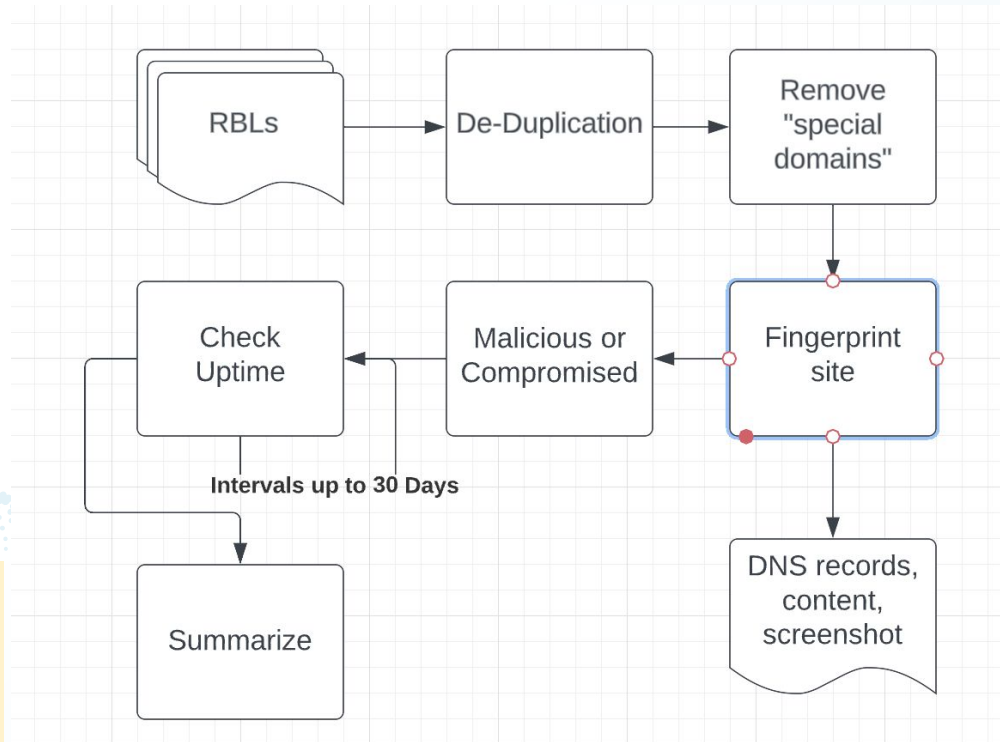
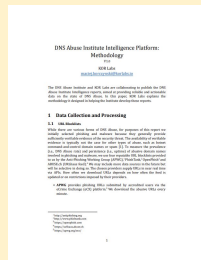
We can only measure what gets reported

# How?

Note:

- ccTLD loss of data, and general undercounting across the board
- Unique domains not URLs

- Methodology



# APTLD Members

# Caveats

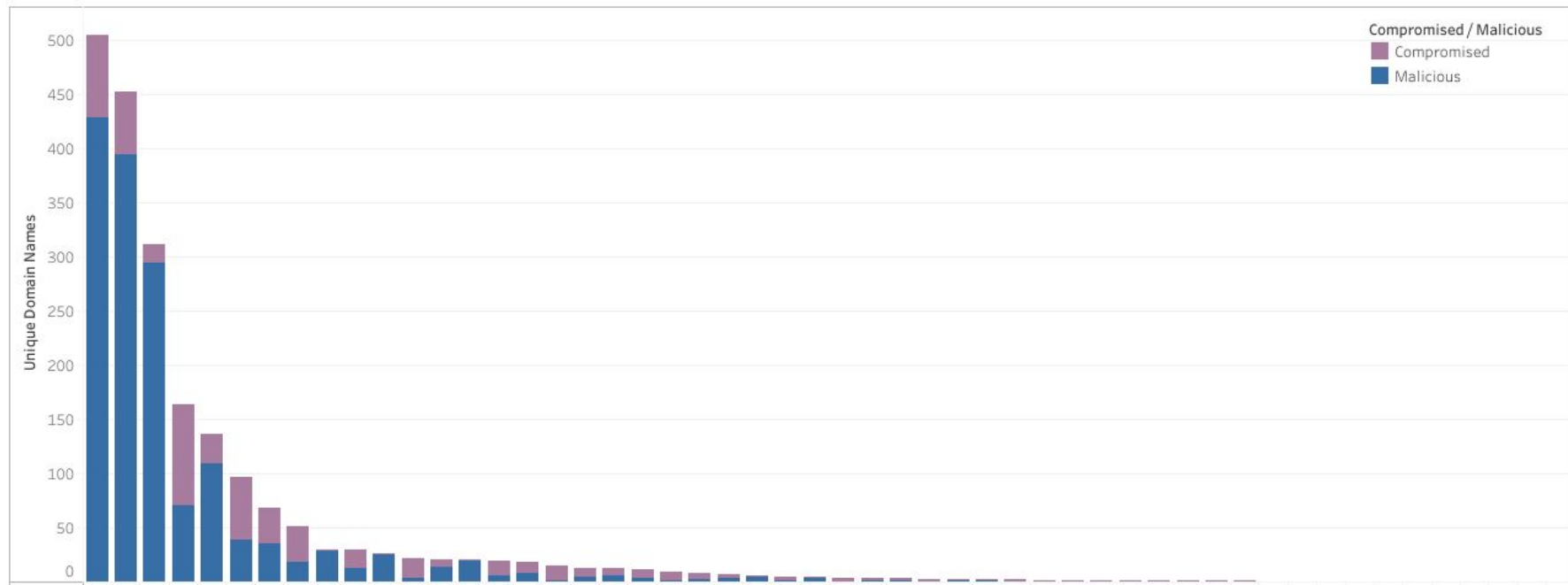
- We know this isn't perfect, best efforts
- Using public data: Size of zone for many is low
- Someone needs to be highest
- Many APTLD members have negligible numbers of abusive names (<10)
- This is not an entire picture of everything harmful in your zone
- Potential geographical/language bias in lists



## 9

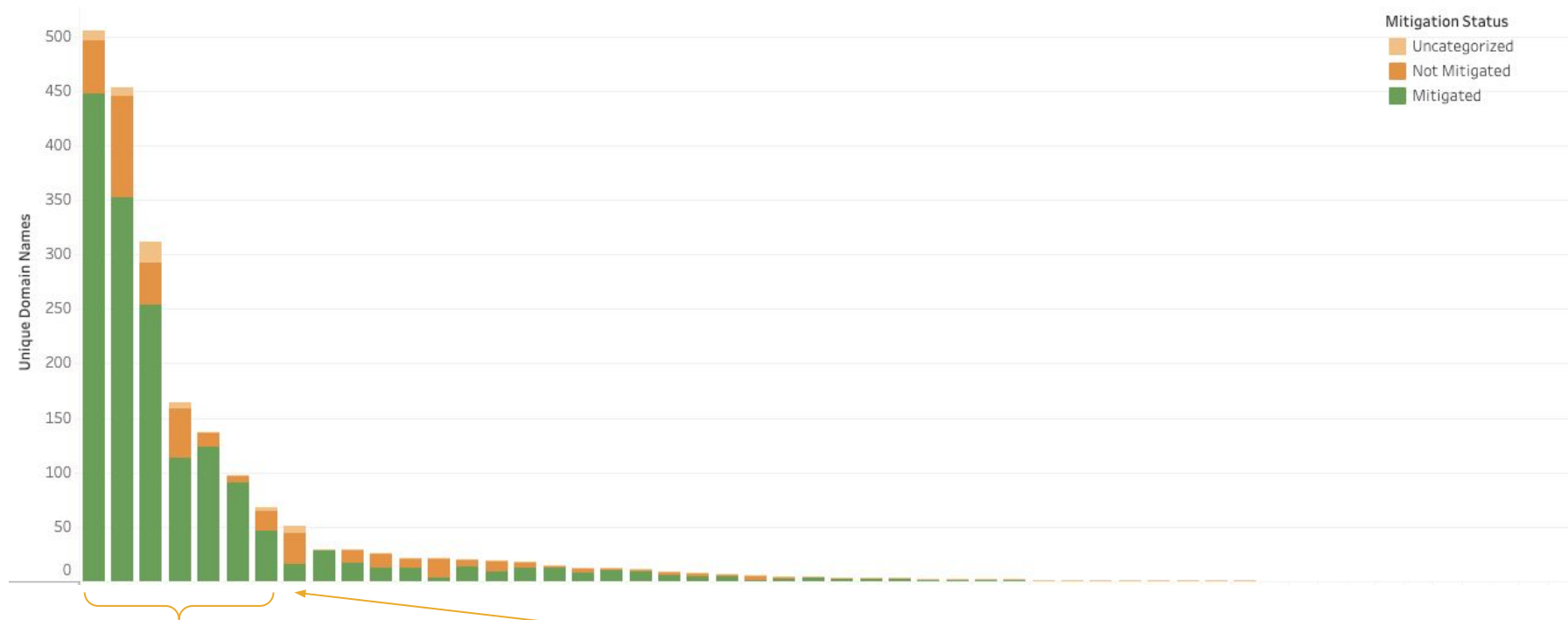


# Type of registration: APTLD Members



Typically more malicious (85%,87%,94%), but not all TLDs (13%).

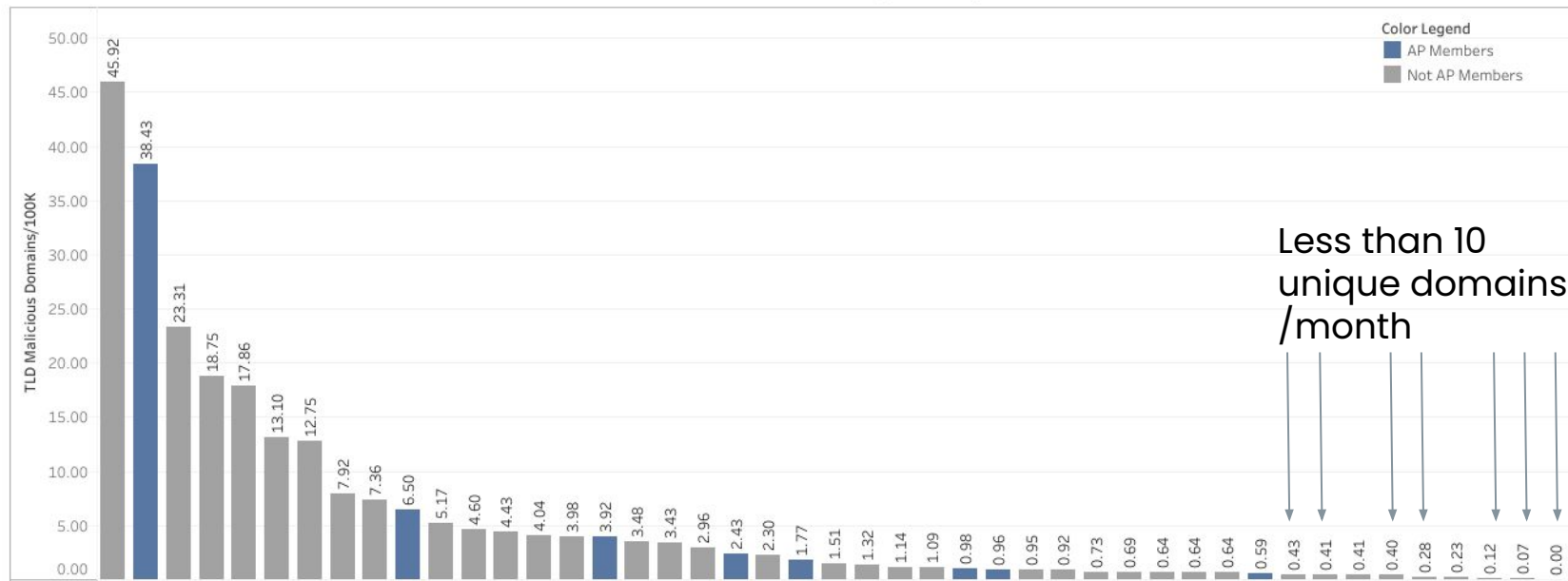
# Mitigation



Generally high % (89, 78, 81, 69, 89, 93), but not in all TLDs (14%).  
Note: include compromised.

# TLDs over 1 Million DUM

Observed Malicious Abuse per 100K DUM (+ 1M DUM): 2023-07

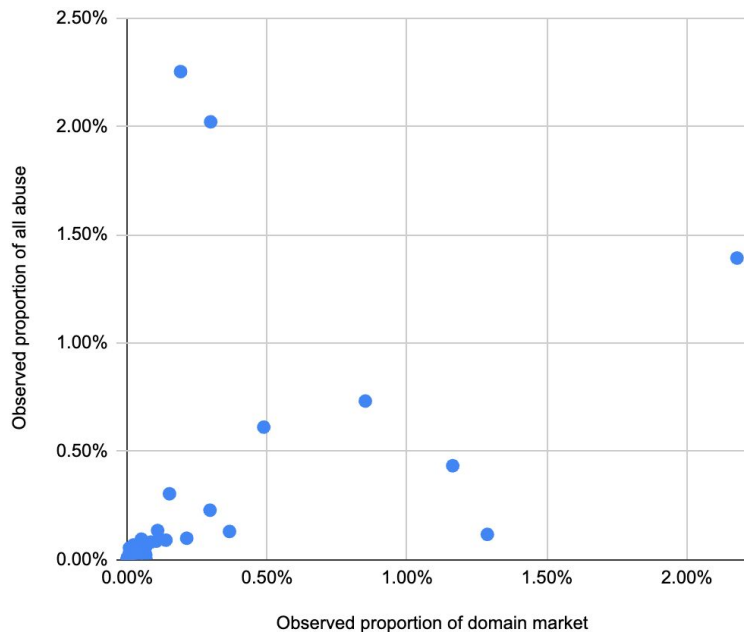


Generally low levels of abuse, but not always.

# What do we make of this?

- ccTLDs are not insignificant:
  - **~25%** of observed phishing and malware in July 2023
- APTLD members:
  - **9.32%** of **observed phishing and malware** in July 2023
- This is roughly in line with the **overall observed DUM** share in July 2023: **8.51%**
- However, this varies for different TLDs

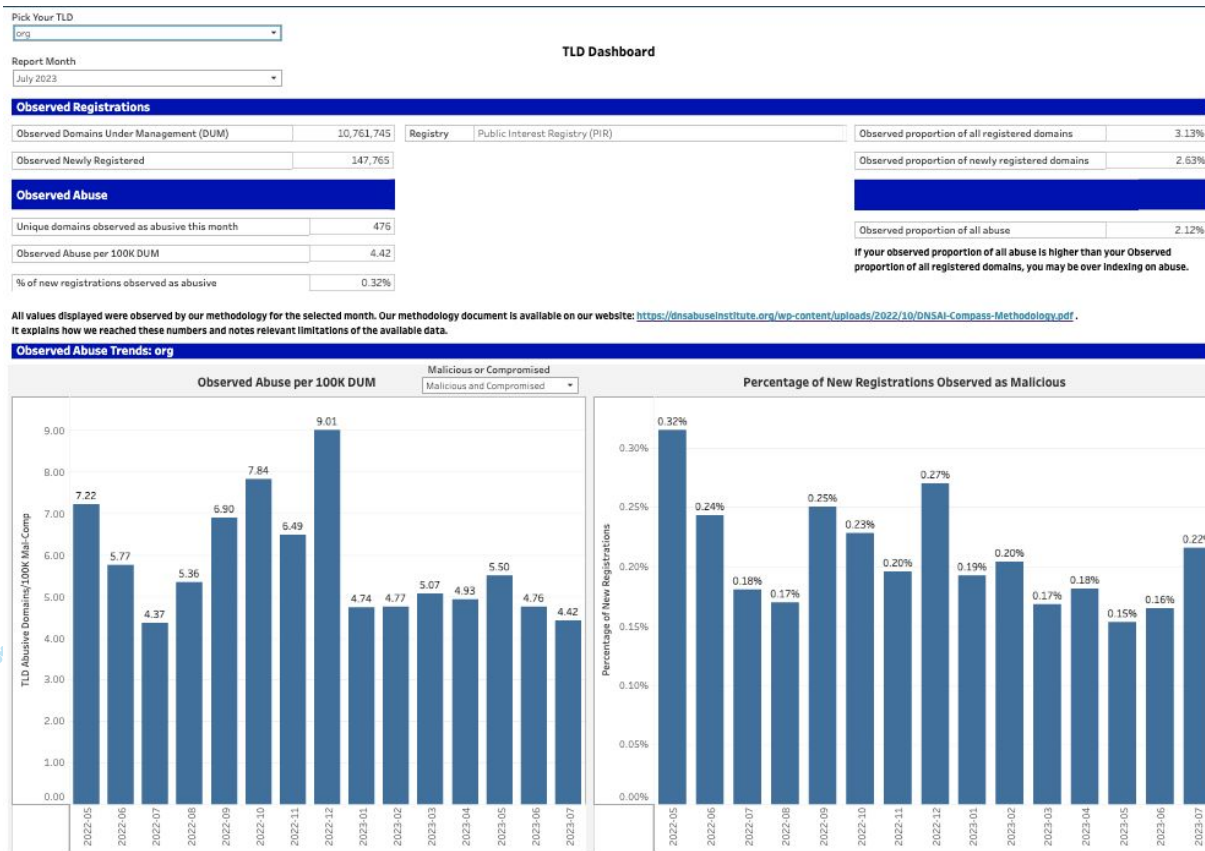
# However...



Variation exists between APTLD members

Some appear to over or under index on observed phishing and malware when compared to observed DUM

# TLD Dashboard Example



# Thank you!

Speak with us to view your individual private dashboard which contains considerable more data and insight.

This is **free**, we are not selling anything.

[rowena@dnsabuseinstitute.org](mailto:rowena@dnsabuseinstitute.org)

Publicly available data:

<https://dnsabuseinstitute.org/dnsai-compass/>