Evaluation and use of third party Reputation Data

Siôn Lloyd

ICANN OCTO-SSR

IDS

September 2024

Introduction

What is Reputation Data?

How is it used?

What is Reputation Data?

- Datasets which describe entities behaviours
  - Entities can be domains, URLs, IP addresses, *etc.*
  - Can cover spam, phishing, malware, *etc.*
- Commonly used to block spam delivery, warn about phishing, protect networks, *etc.*
- Many different providers, with different collection methods, different focus
  - Commercial and open-source
- Reputation Block Lists - RBLs
- APIs

Different uses of reputation data

- Broader statistics vs focused view
- Historic vs current
- Consistency vs best available

Many use cases exist with…

Different requirements

Different issues

Different modes of “failure”

Different costs of “failure”

Different uses of reputation data

We don’t collect this data ourselves

We don’t control the collection methodology

Our use cases may not be those imagined by the data producers

Mitigation of mismatches is down to the consumer.

Understanding our RBL data

Understanding RBLs:

What we can quantify
Less tangible measures

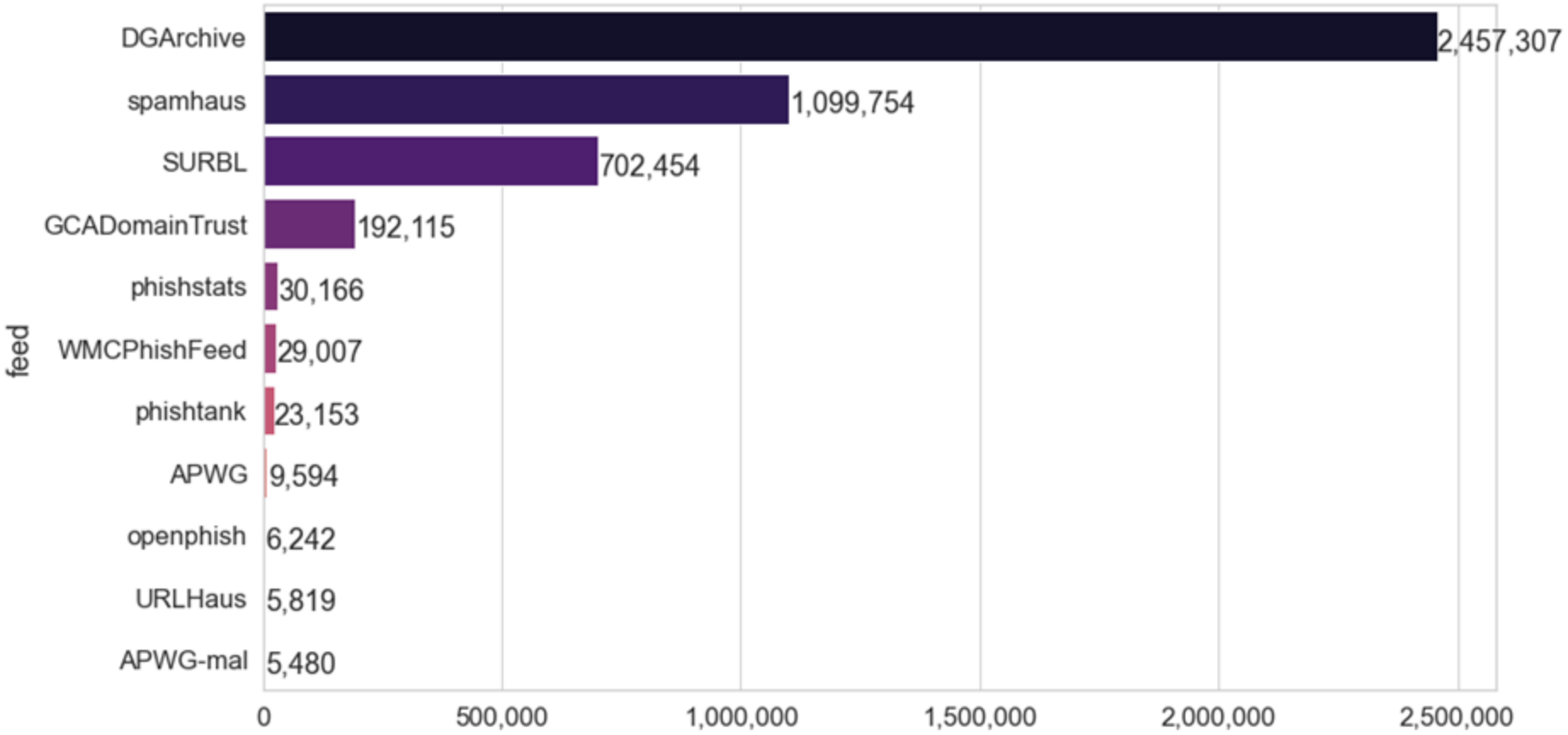
Understanding our RBL data – general description

- Entry Types
  - Spam, Phish, *etc.*
- Metadata
  - Malware family, phished brand, *etc.*
- Data transfer
  - rsync, https, *etc.*
- Data format
  - JSON, csv, *etc.*
- Entry provenance
  - Observations or predictive

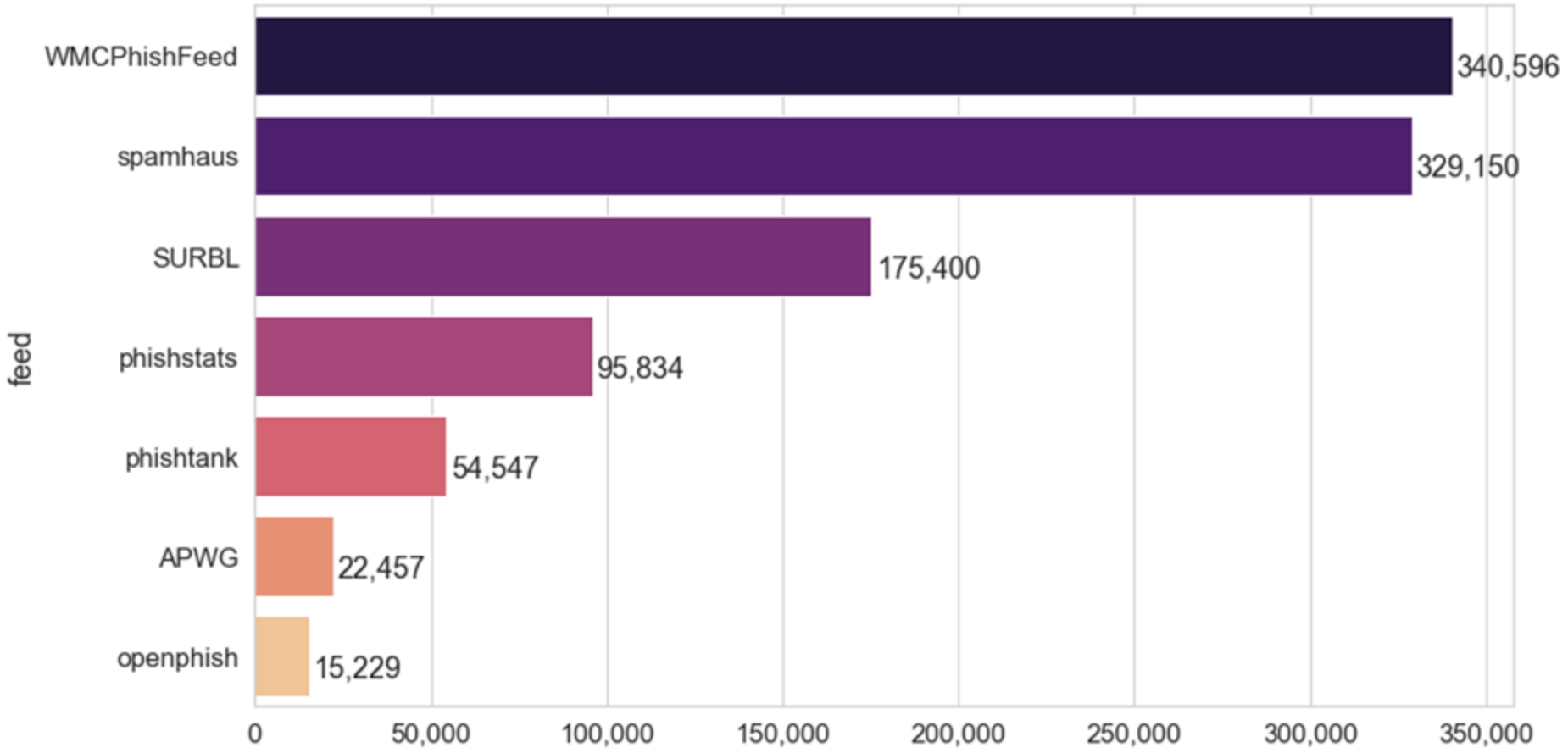
Understanding our RBL data – what we can quantify

- Volume
  - Like-for-like
- Overlap
  - In both directions
- Timeliness
  - Lead/lag
- Churn
  - How dynamic

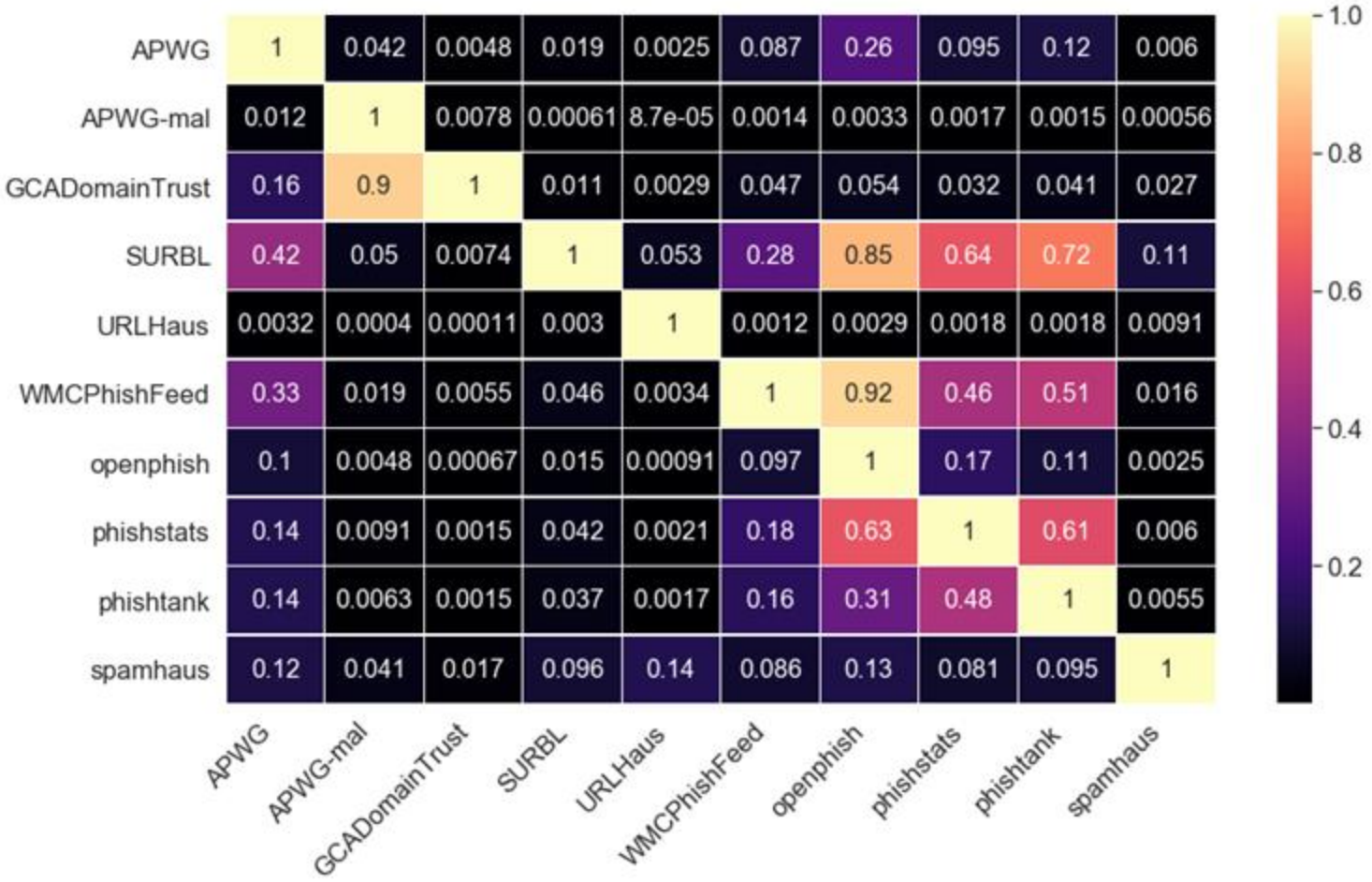
Understanding our RBL data – Volumes (unique domains)



Understanding our RBL data – Volumes (phishing reports)

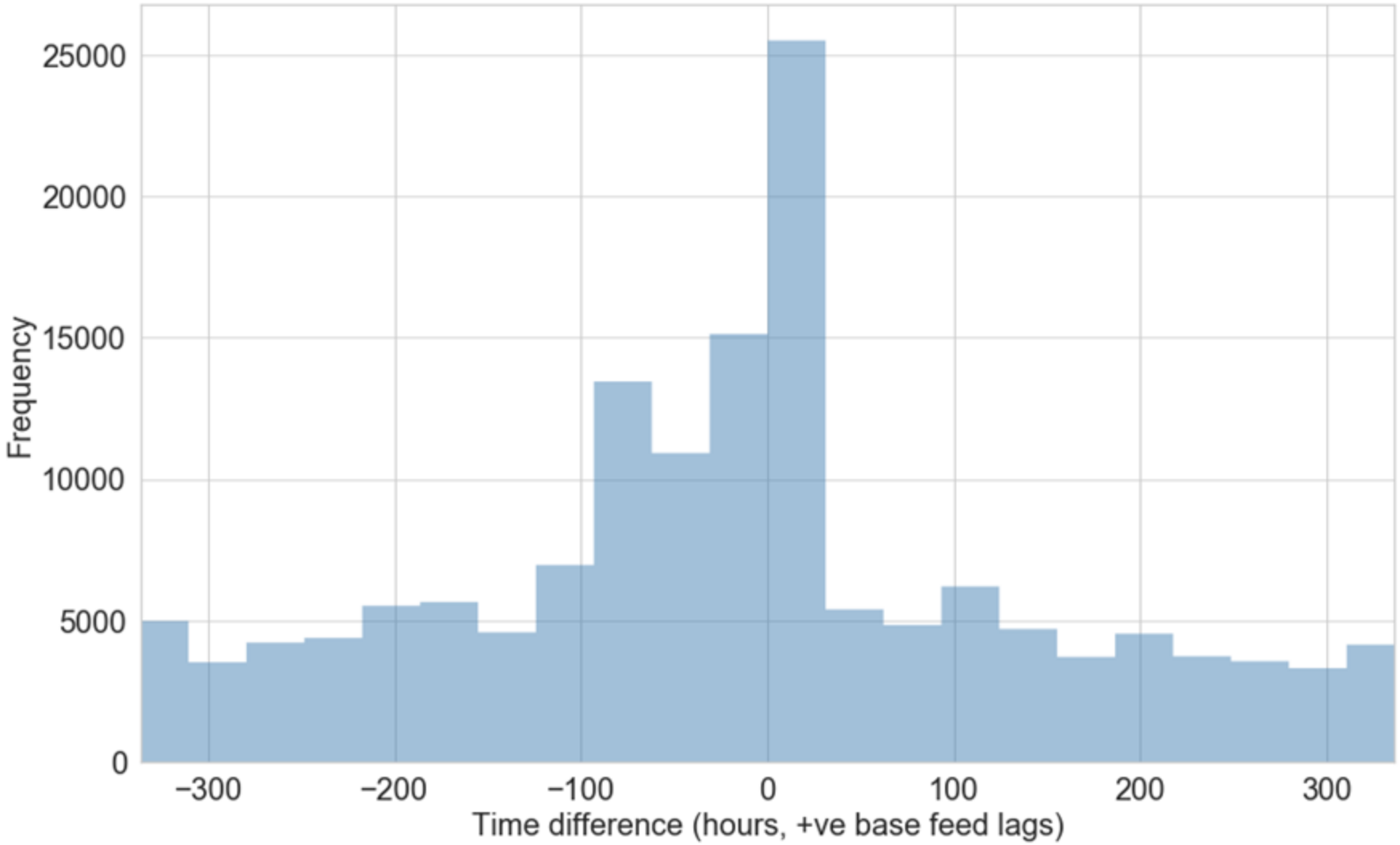


Understanding our RBL data – Overlap

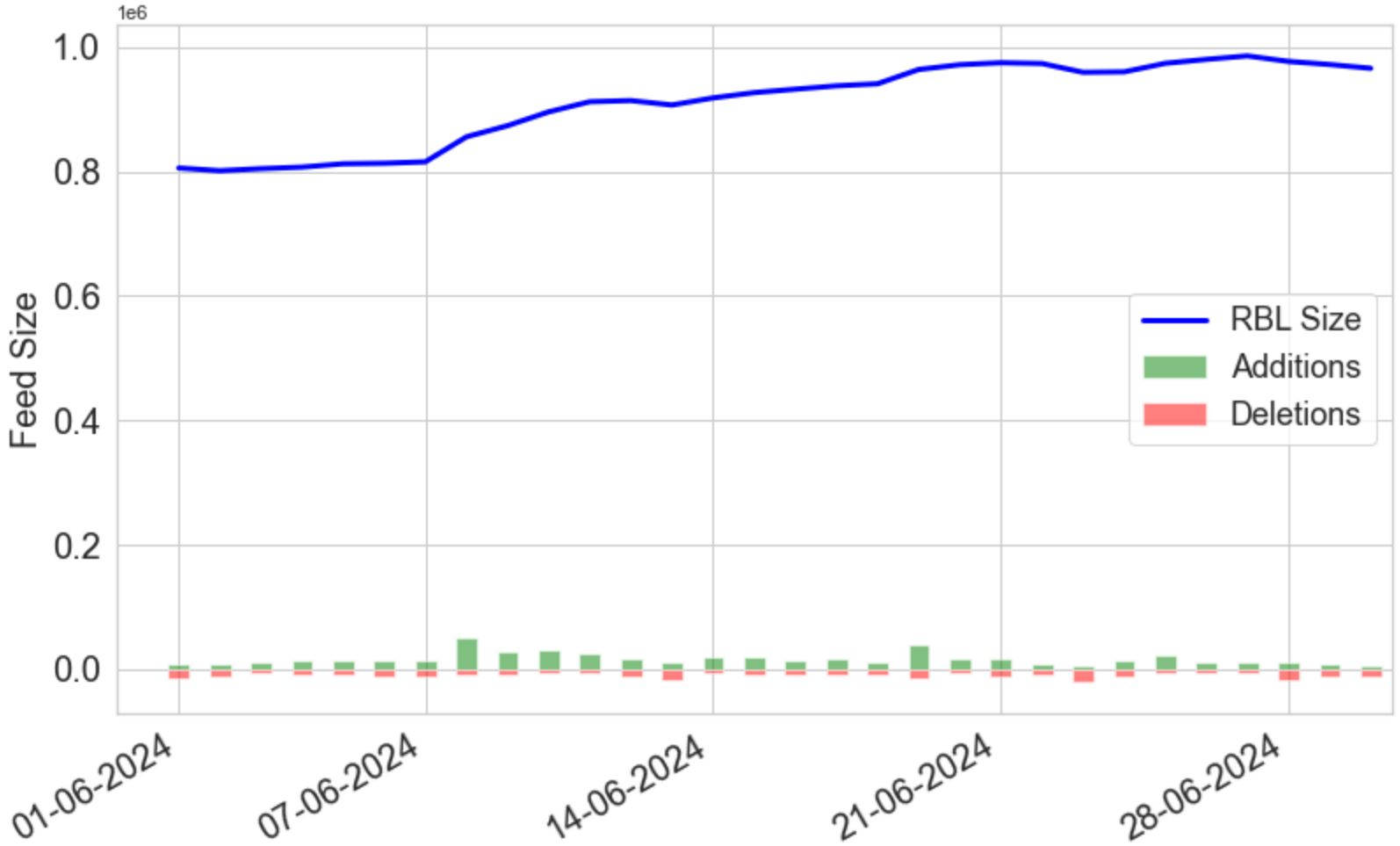


- Most overlaps are small
- Note the inclusion of open sources in other RBLs
  - Two reports on different RBLs might not be so independent

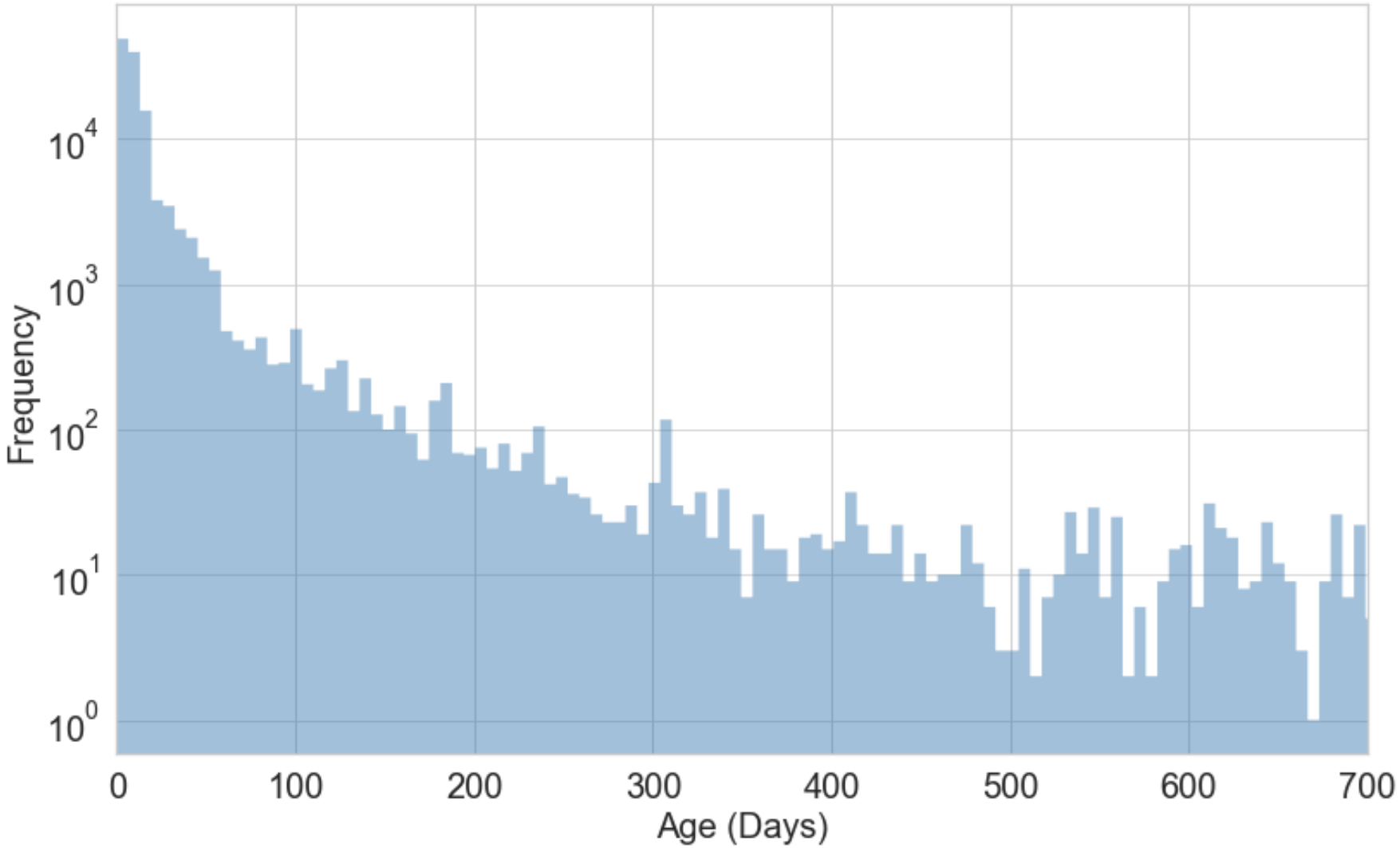
Understanding our RBL data – Timeliness



Understanding our RBL data – Churn



Understanding our RBL data – Entry ages



Understanding our RBL data – what we can get an idea of

- Liveliness
  - How many entries resolve
- Purity
  - How many (potential) false positives
- Accuracy
  - Does categorization match reality

Spot checks (sampling)

Cross-reference with high reputation sources (*e.g.* TRANCO)

Or other RBLs

Understanding our RBL data – what we can't measure

- Catchment
  - Is there a geographic blindspot
  - Do they capture mobile attacks
  - Do they capture email
  - Do they concentrate on one threat type (*e.g.* spam, phishing)
- Entry retesting
  - Are statuses reconfirmed periodically
  - Do entries "flip-flop"
- Reliability
  - Is the data always available

Rely on experience, RBL description, FAQs, *etc.*

Can we improve the data?

- Cross-reference with zone files
- URL Shorteners
- Remove “parked” pages
  - Parking as a service leaves a trace in DNS
- Malicious registrations vs. compromised domains

General Observations

- We often rely on data collected by third parties
  - Think about your specific needs
  - The costs of various “failures”, *e.g.*
    - false positives (false negatives?)
    - …
  - ~~Can the data be improved?~~ The data **can** be improved
- Understand how datasets complement each other
  - Be prepared to read multiple RBLs
- Don’t stop testing
  - Things change

https://www.icann.org/en/system/files/files/octo-037-11dec23-en.pdf

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin.com/company/icann

soundcloud.com/icann

instagram.com/icannorg