Identification and abuse characteristics of batch registered gTLD domains

Sam Cheadle - ML Engineer
Security, Stability & Resilience (SSR) Research
ICANN Office of the CTO

RIPE Presentation
May 2025

Structure of presentation

1. What are domain registration batches? How to identify them?
2. How common are batch registrations?
3. What are the **abuse profiles** of batch registered domains?
4. Conclusions and future work

What Are Domain Registration Batches?

Motivation

- Attackers often **register domains in bulk** to support large-scale malicious campaigns (Vissers et al., 2017, Spooren, 2019) including phishing, malware delivery & botnet C2.
- Prior work hypothesizes a **preference for APIs or bulk registration tools** to streamline and automate these registrations (Nosyk, 2025).
- Use of APIs introduces **detectable patterns**—e.g., bursty, time-bound batches of registrations.
- Batch patterns may reveal attacker infrastructure **early in the attack lifecycle**.
- Understanding these patterns enables more **effective detection, intervention, and mitigation**.

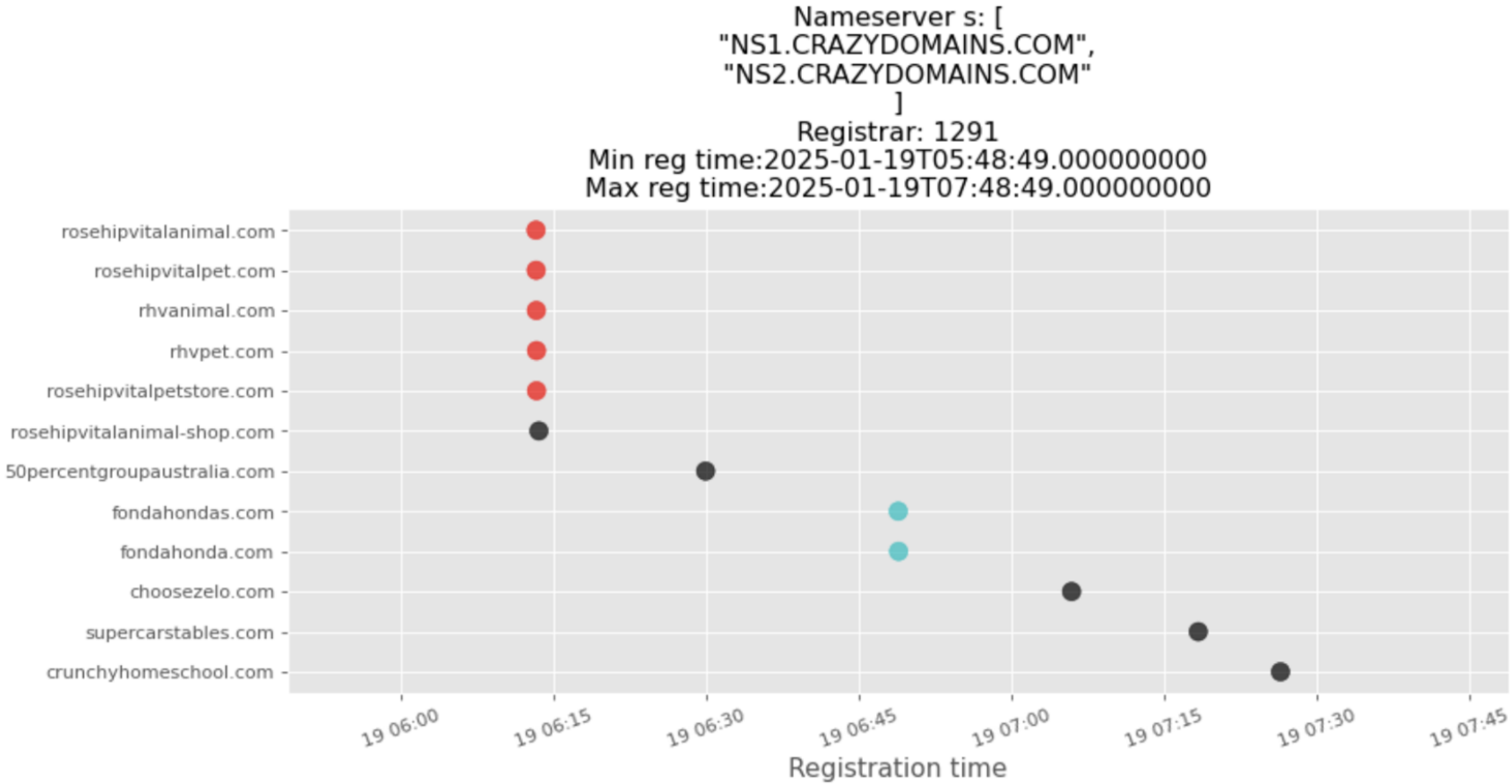
Method

- Perform batch registration clustering using **limited features**:
  - Registrar
  - Authoritative Nameservers
  - Creation date (full timestamp)
- Exclude **common shared nameservers** (e.g. default registrar nameservers)
- Density-based spatial clustering of applications with noise (**DBSCAN**) used as the clustering algorithm

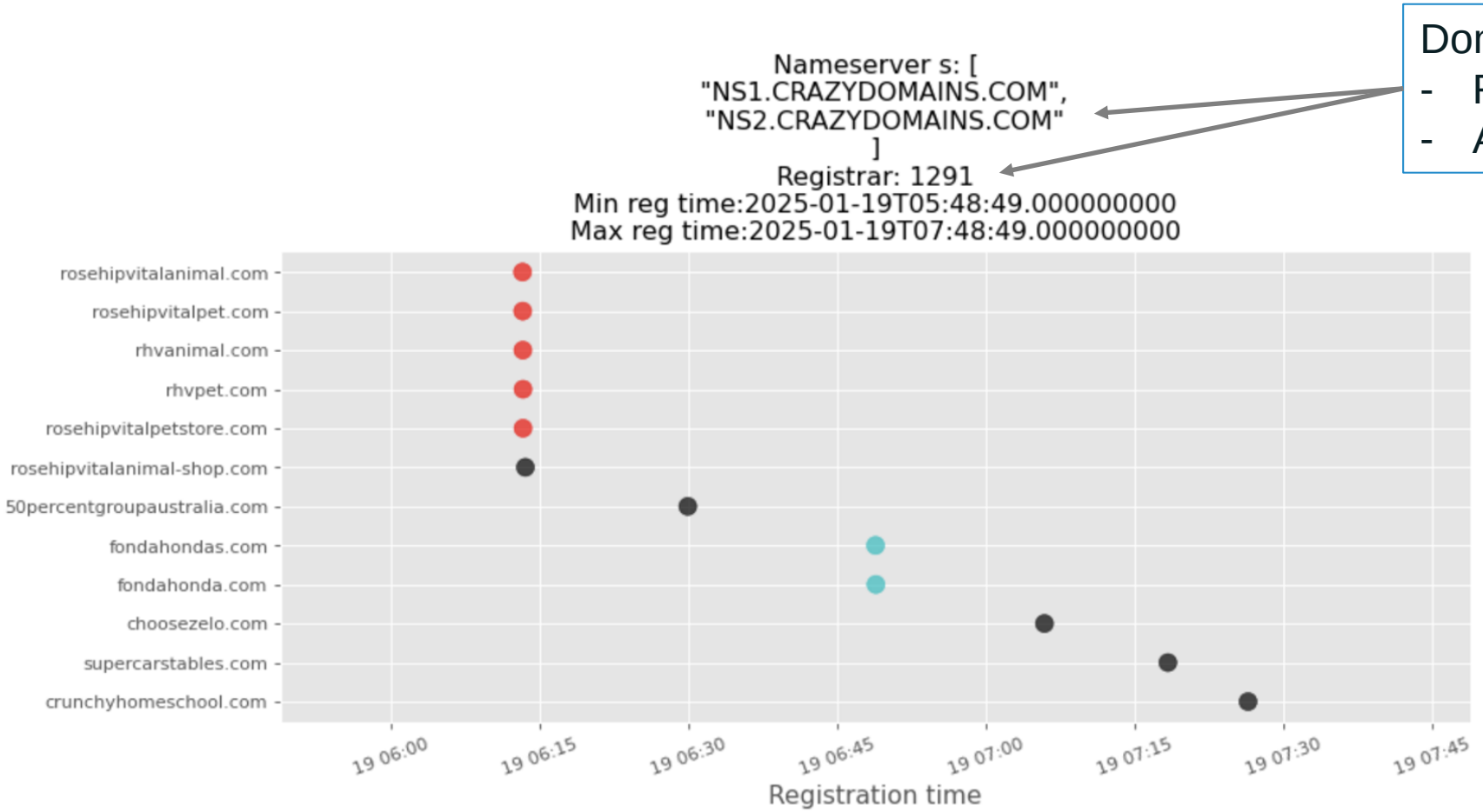
Data sources

- gTLDs Registration Data
  - Bulk registration data access (BRDA data)
- Reputation Block Lists (RBLs)
  - Spamhaus, SURBL, WMCGlobal, Phishtank, Urlscan, APWG, Urlhaus

Example batches – Plot A

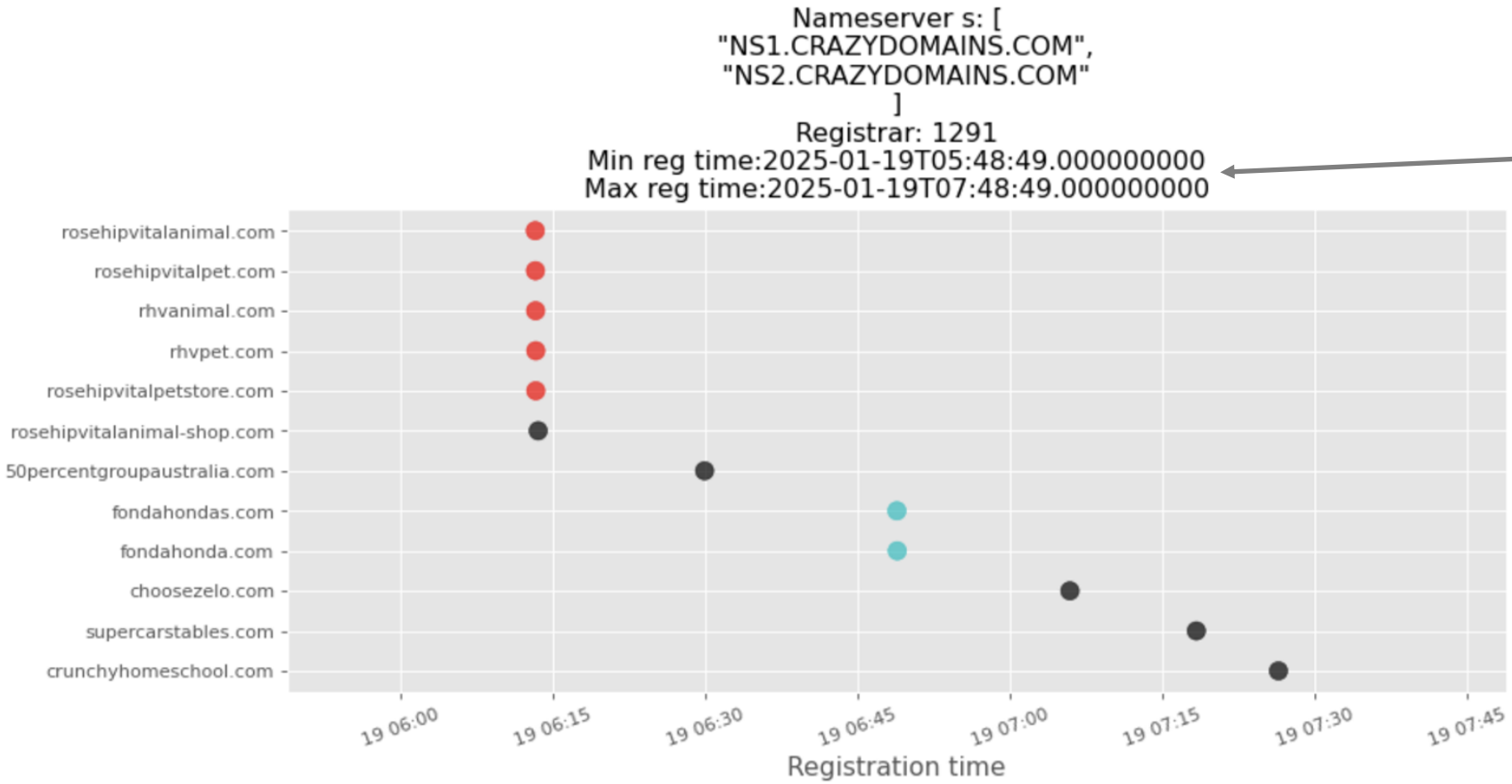


Example batches – Plot A



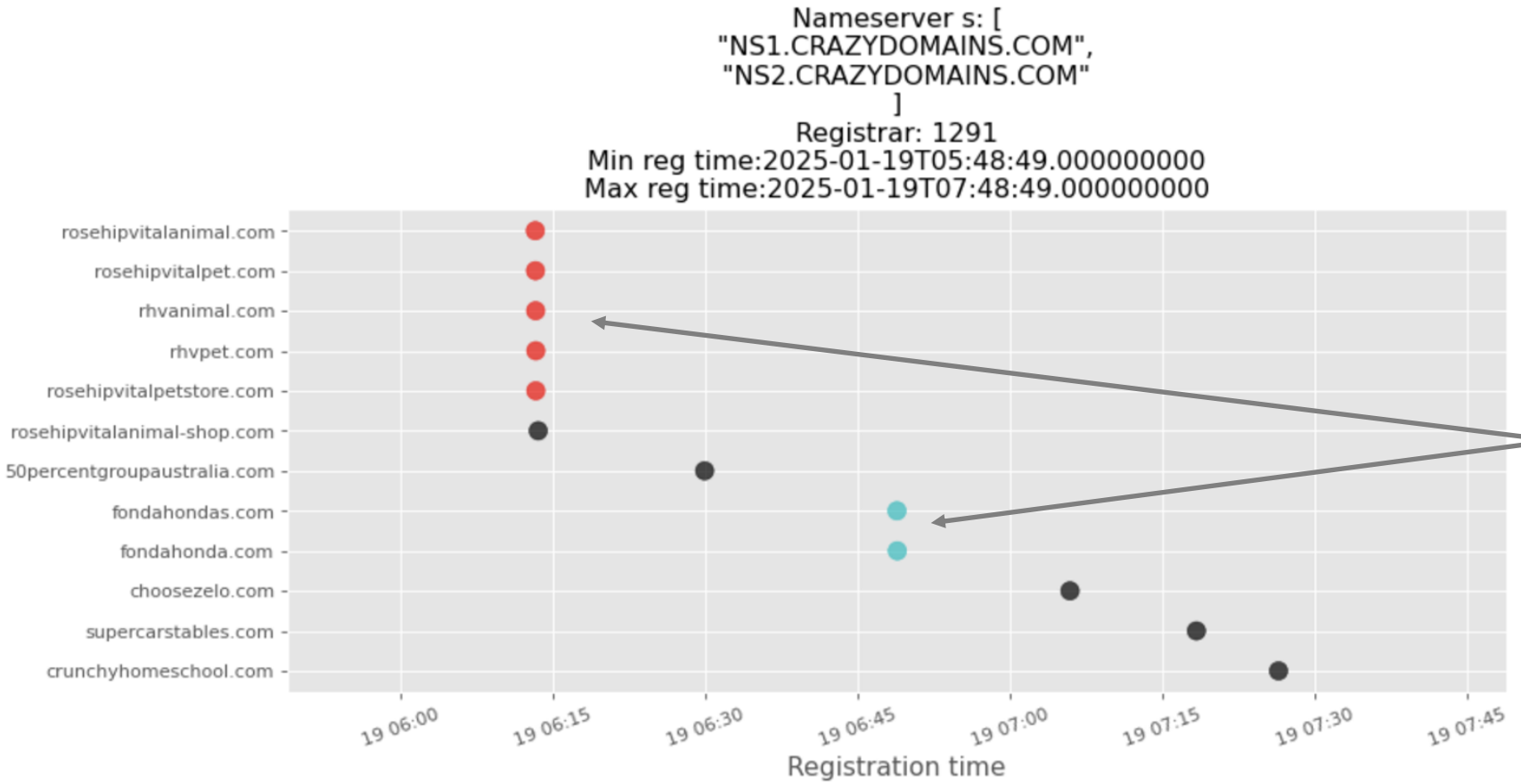
Domain registrations split by
- Registrar (IANA ID)
- Auth Nameservers

Example batches – Plot A



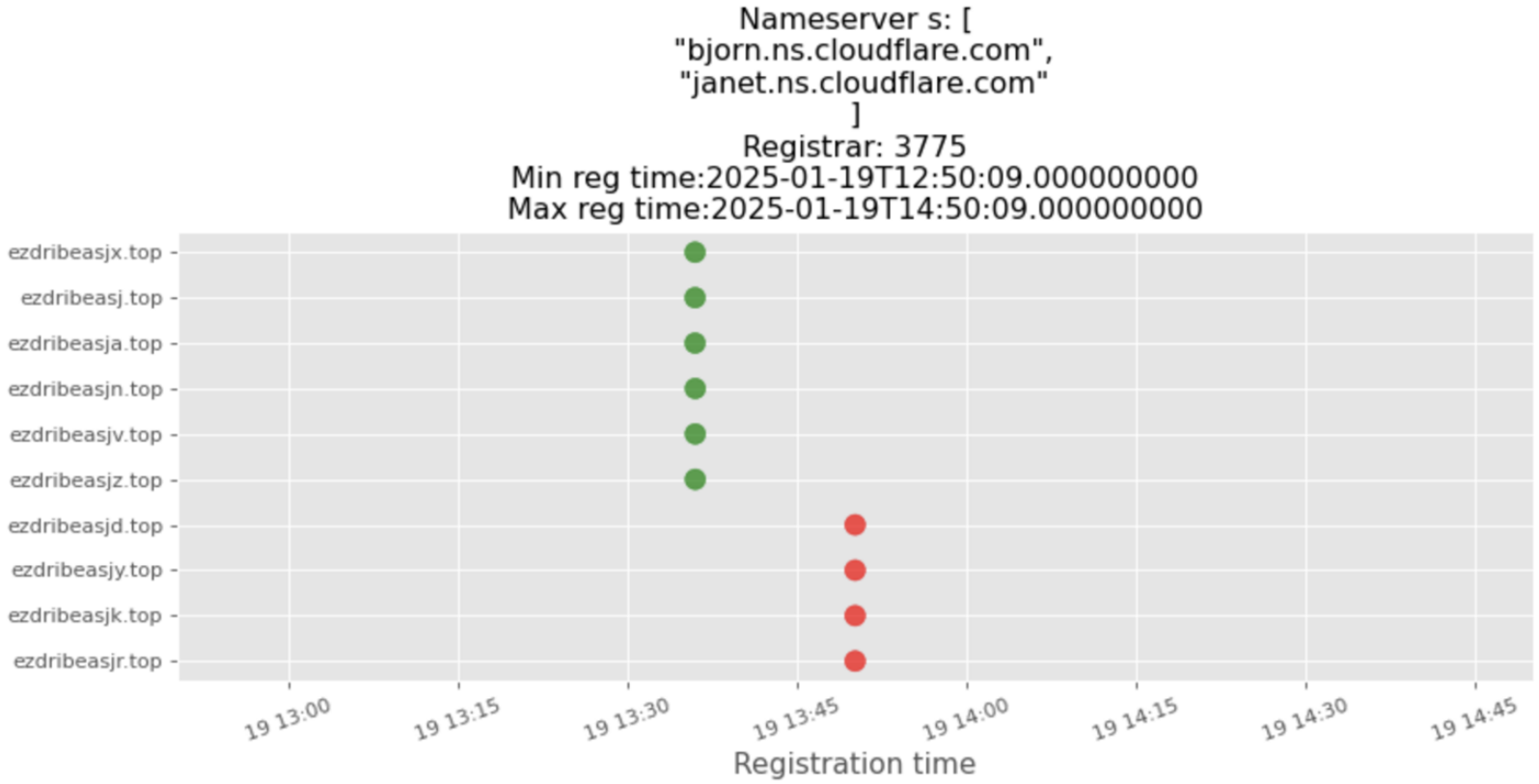
2 hour time window

Example batches – Plot A

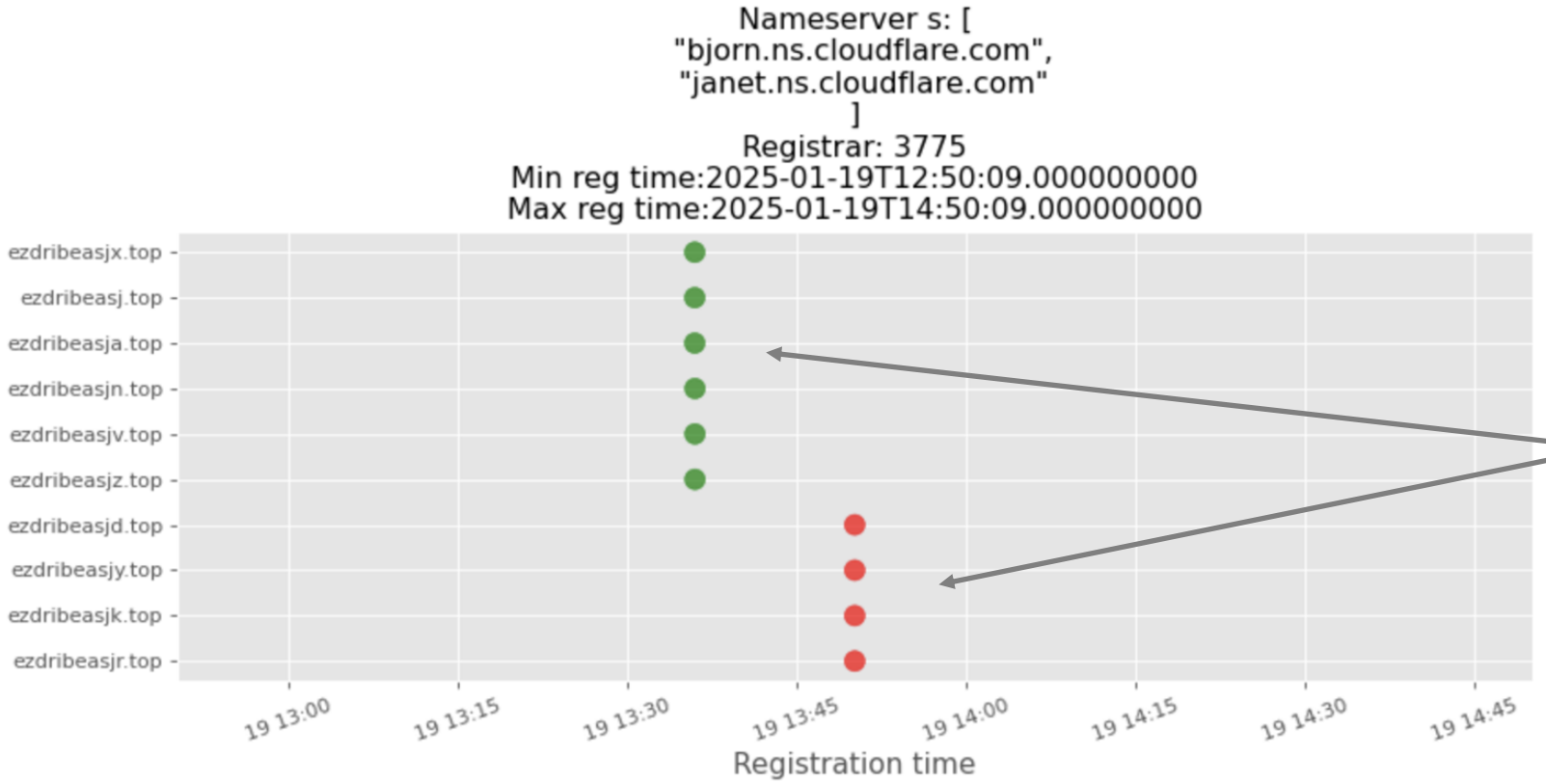


Clustered ‘batch registrations’

Example batches – Plot B



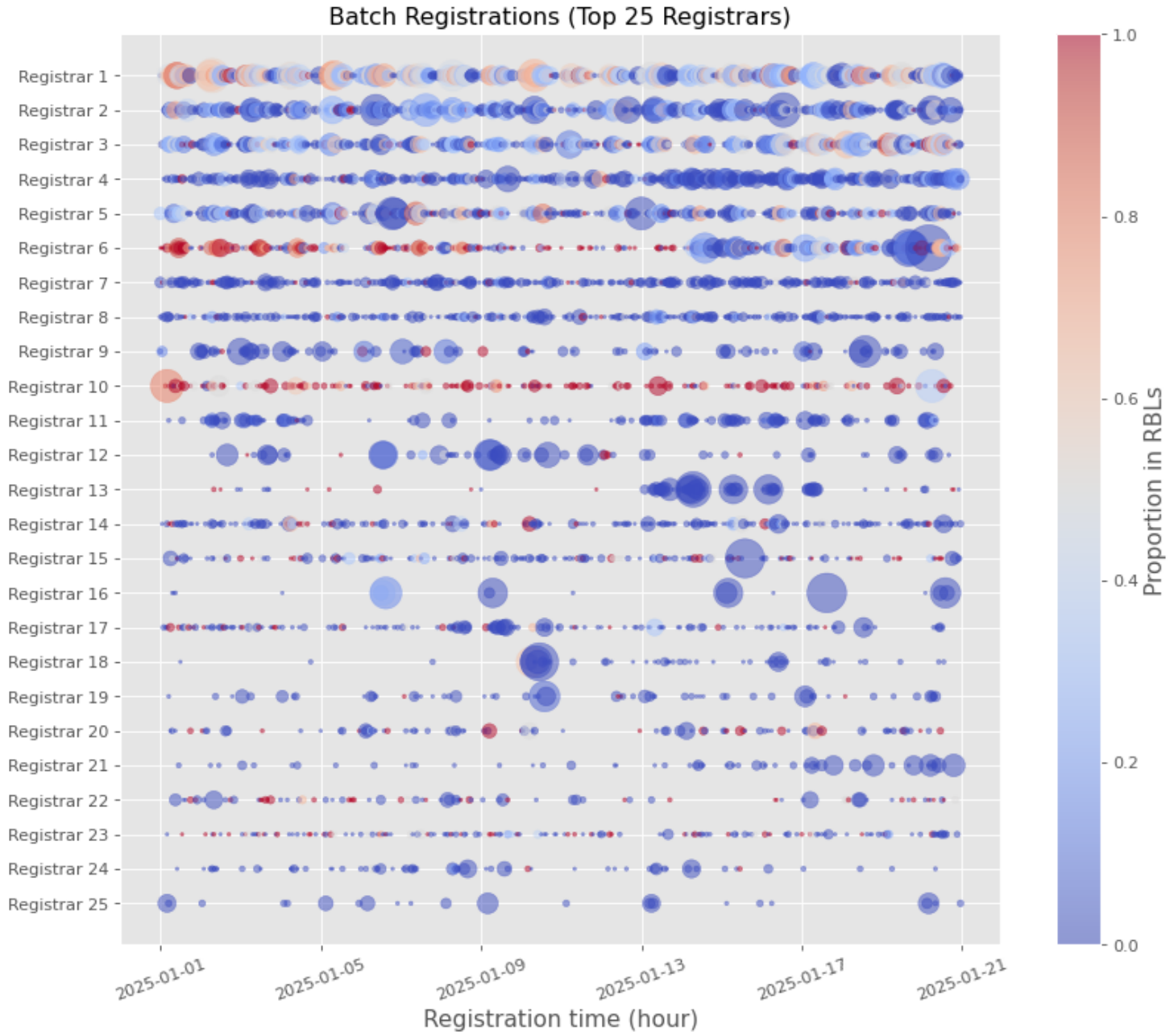
Example batches – Plot B



Distinct batches, but related ongoing campaign

Visualising batch volumes across registrars

- Hourly counts of batch registrations, for the top 25 registrars
- Highest reputation block list (RBL) overlap is shown in red
- 3-week time-period



How Common Are Batch Registrations?

How common are batch registrations?

- Analysis period: 2024-12-25 - 2025-02-18
- Total number of newly registered gTLD domains (ICANN centralized data): 10,351,522
- Total number of batch registered domains: 2,543,473 (**25% of all registrations**)

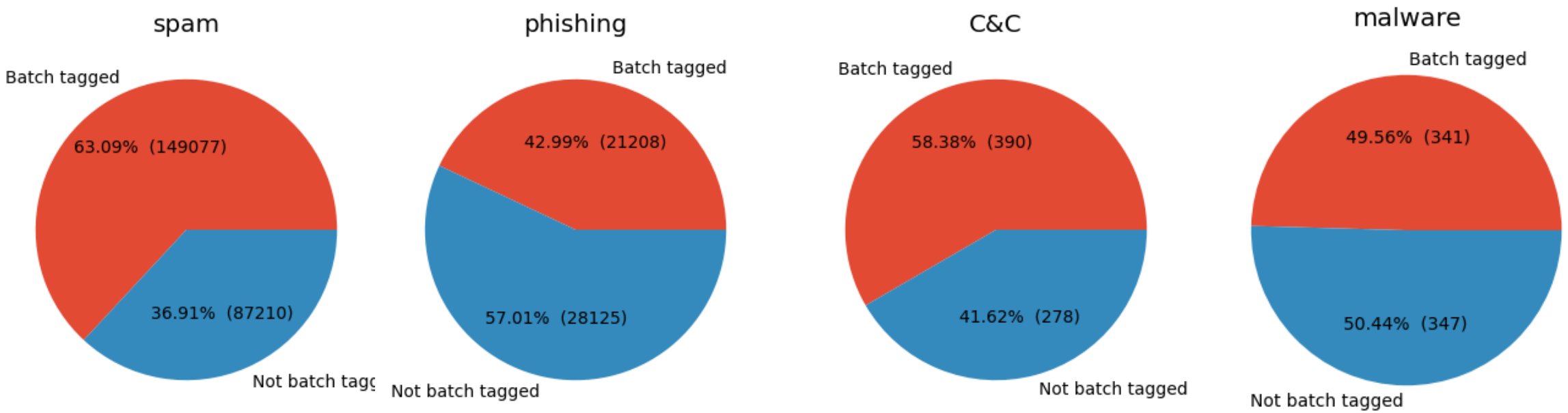
Abuse Profiles of Batch Registered Domains

Overlap with newly registered malicious domains

- Total number of RBL* domains: 288,218
- Total number of batch registered RBL domains: 171,662 (**60% of RBL domains**)

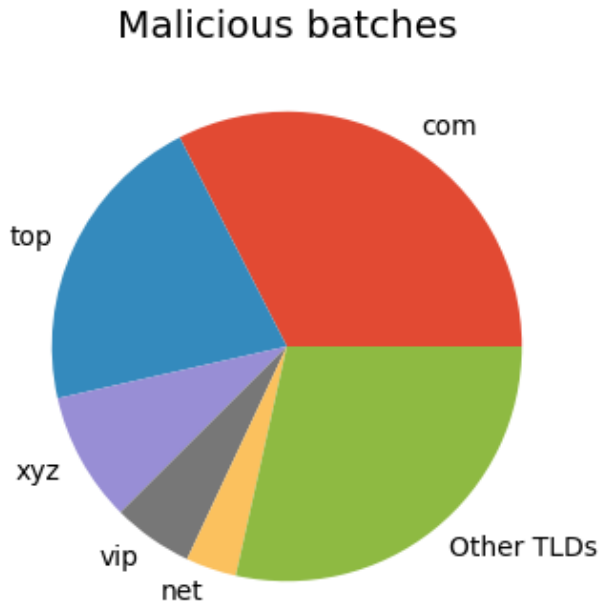
** newly registered within the analysis period*

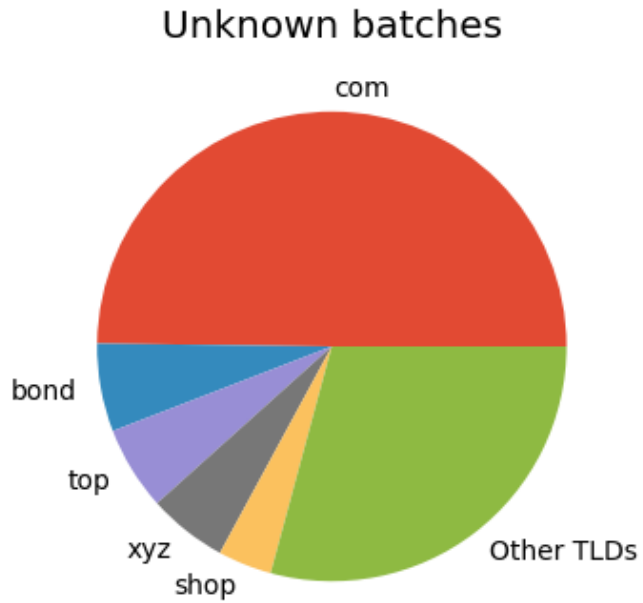
Overlap with newly registered malicious domains



- Spam domains - highest % tagged as batch registered (63.1%)
- Lowest % for phishing, but still > 40%
- Overall 60% of newly registered malicious domains tagged as batch registered

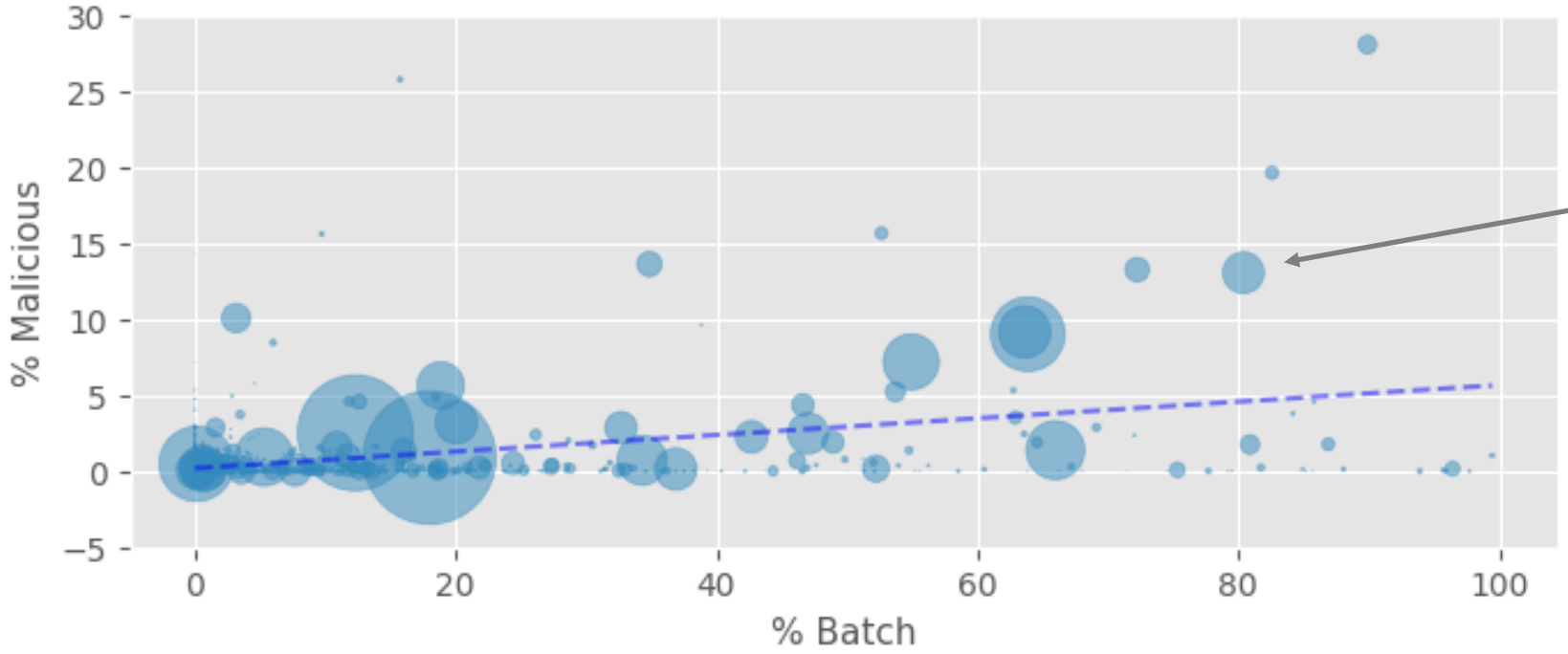
TLD composition breakdown – Top 5





- Majority of batch registered domains are under dot com
- Dot top is common within batches tagged as malicious
- gTLDs with known high abuse rates are common in both groups

Registrar level analysis



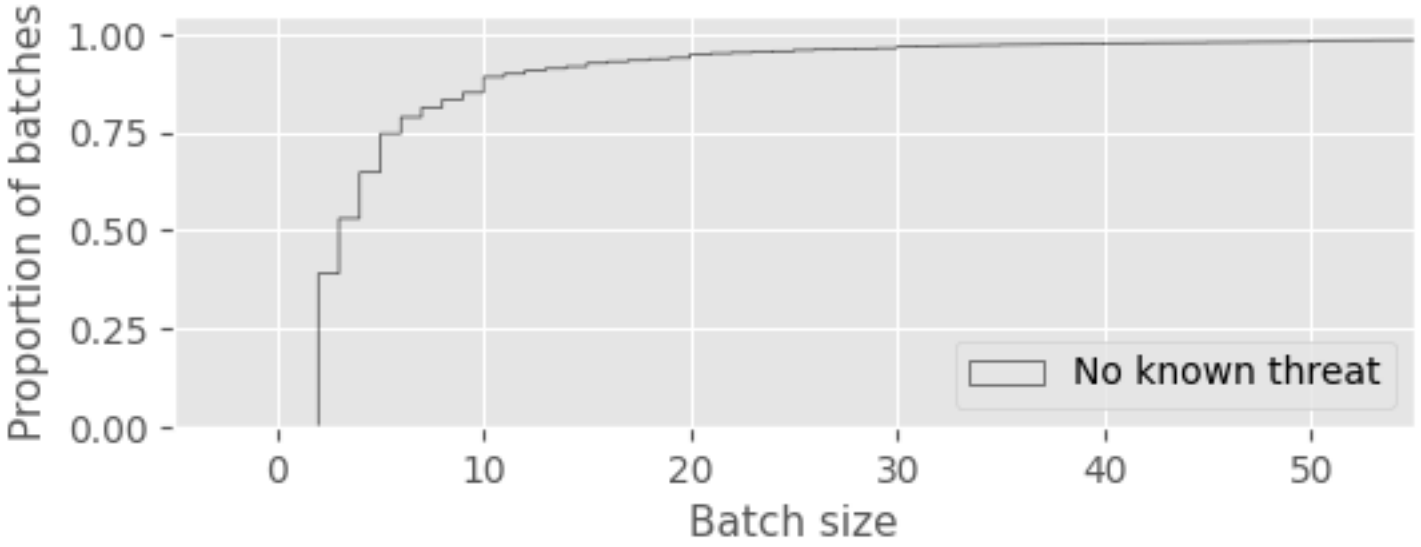
Each dot is a registrar

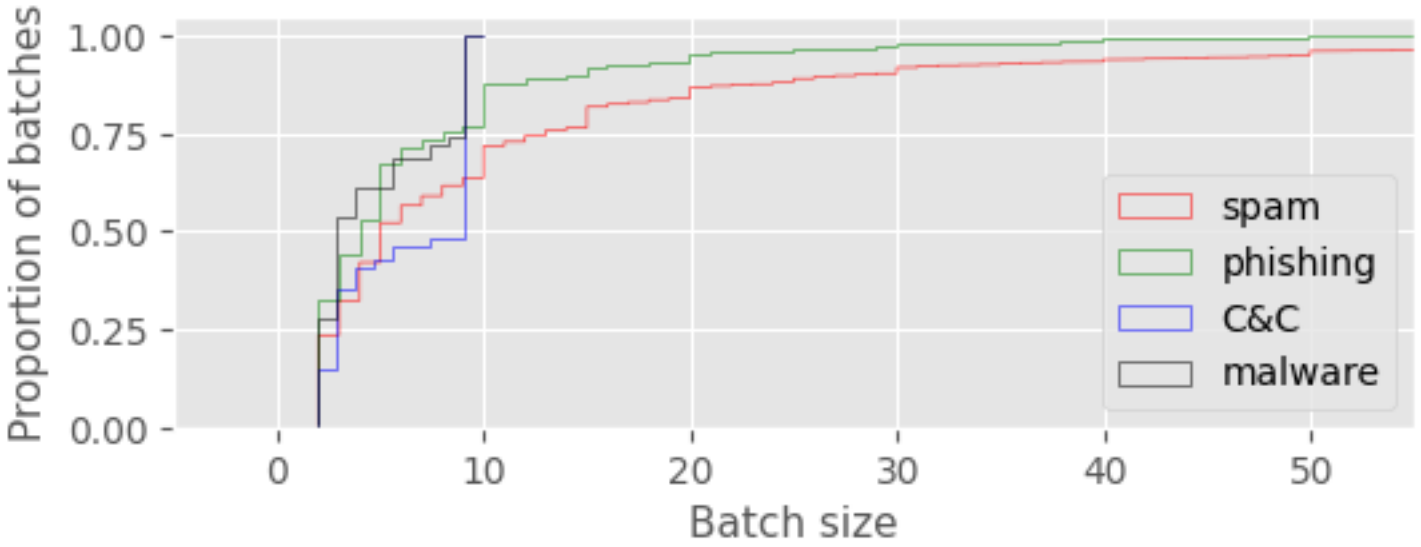
Size = DUM in sample

- What is the relationship between **batch** and **overall** abuse rates, per registrar?
- Statistically significant positive correlation (Spearman's r=0.422 p< 0.0001)

Distribution of batch sizes (CDF plots)

- Most batches are small (38% contain only 2 domains). Long tail distribution.
- Spam batches larger than phishing batches
- Malware, C&C batches – max size of 10, limited coverage
- Noticeable spikes at 10, 20, 30 etc





Abuse composition breakdown - individual batches

- Plot shows a sample of 300 malicious batches (min size: 10, max size: 500)
- Clusters sorted by size
- Known malicious / RBL domain count is shown in red

Abuse composition breakdown - individual batches

- **Expansion analysis**
- Total number of inferred (additional) malicious domains: 179,344
  - 104% increase on known batch RBL domains

Conclusions

- Clustering methods **effectively group batch registrations** based on limited but meaningful features.
- Most batches are small, but **certain sizes appear more frequently**, consistent with human selection preferences.
- **Larger batches** are more common for certain threat types (spam, phishing).
- There is a measurable link between batch registration activity and **abuse rates**.
- Expanding batch registration labels significantly increases the identification of **potentially malicious domains**.

Future work

- Validation / Ground Truth
  - Work with registrars to **validate reliability of the method**
  - E.g. Investigate impact of **reseller practices** (artificial batches?)
  - Interested registrars, please get in touch

- Broaden coverage to other types of **bulk registration patterns**
  - Identifying **non time-bound** registration patterns - e.g. time series analysis to pick out ongoing malicious campaign registrations

- **Monitor ongoing patterns** of abuse related to batch/bulk registrations

- Explore methods of **exposing the results** to the community

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann

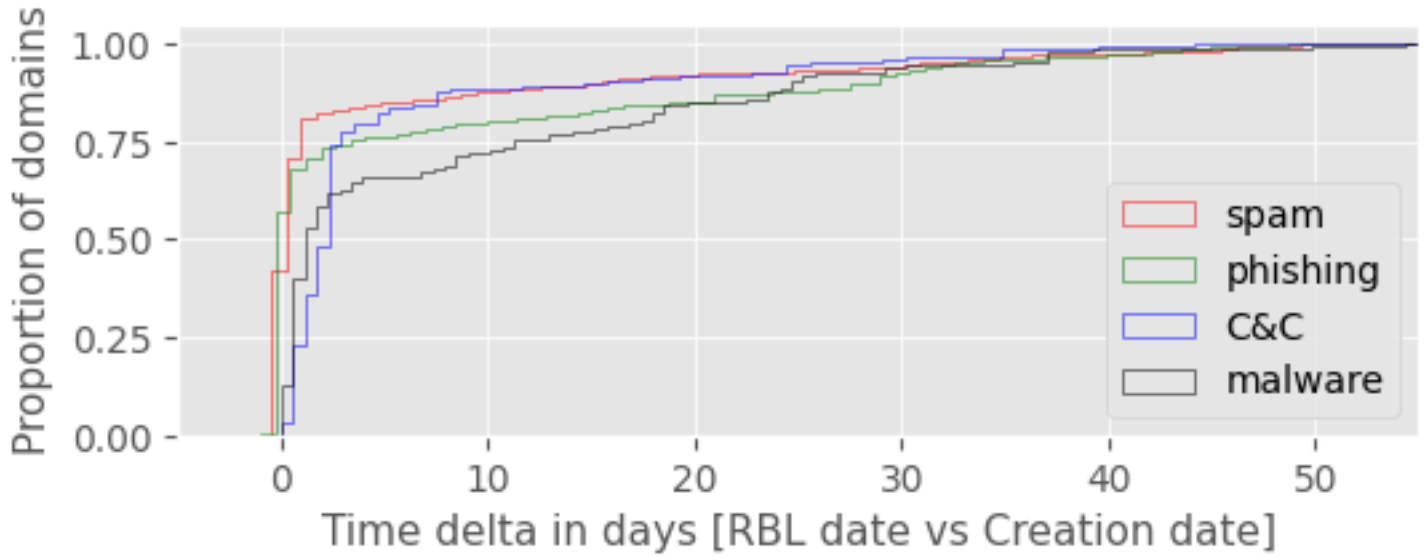
Contact:

sam.cheadle@icann.org

ssr-research@icann.org

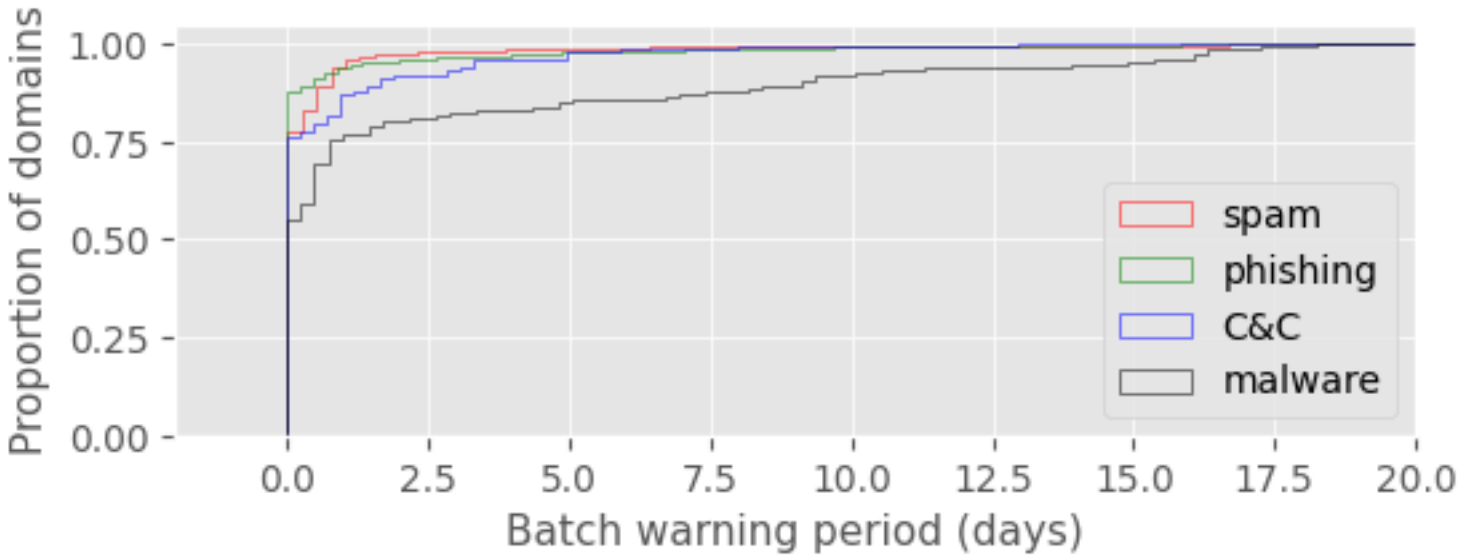
Additional slides

Domain Aging



- What is the time delta between domain creation and RBL flagging (weaponization)?
- The majority of domains are weaponized within 1-2 days of creation
- However, a substantial number of domains (20-30%) remain dormant for days or weeks

Warning period analysis



- How many batch registered RBL domains could have been **predicted earlier** by batch expansion? (Grace period of 12 hours)
- Total number of RBL domains with batch warning of 12 hours or more: 27,138
  - **16.0%** of all RBL batch domains