

# APLD 84

**Session 5A – Registry Abuse Mitigation for ccTLDs 19 September 2023**

**Raedene McGary**

**VP Registry Services Tucows**

**[tucows/registry](https://tucows/registry)**

**tucows/registry**

# **DNS Abuse**

**Making the Internet Better**

**Date: 19 Sept 23**

# DNS Abuse

## Definitions

malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse

**tucows/registry**

# What we do about abuse?



## **Tucows Registry Services for ccTLDs and gTLDs**

Offer our own technical Abuse  
monitoring and Reporting Service

using third party reporters to  
analysis and identify actionable  
reports

Offer full Abuse Management



## **Tucows Registrars: Tucows, OpenSRS, Enom, EPAG, Hover & Ascio**

Founding member of the  
Framework for Abuse

Compliance Team take  
action to manage abuse  
across all our domains

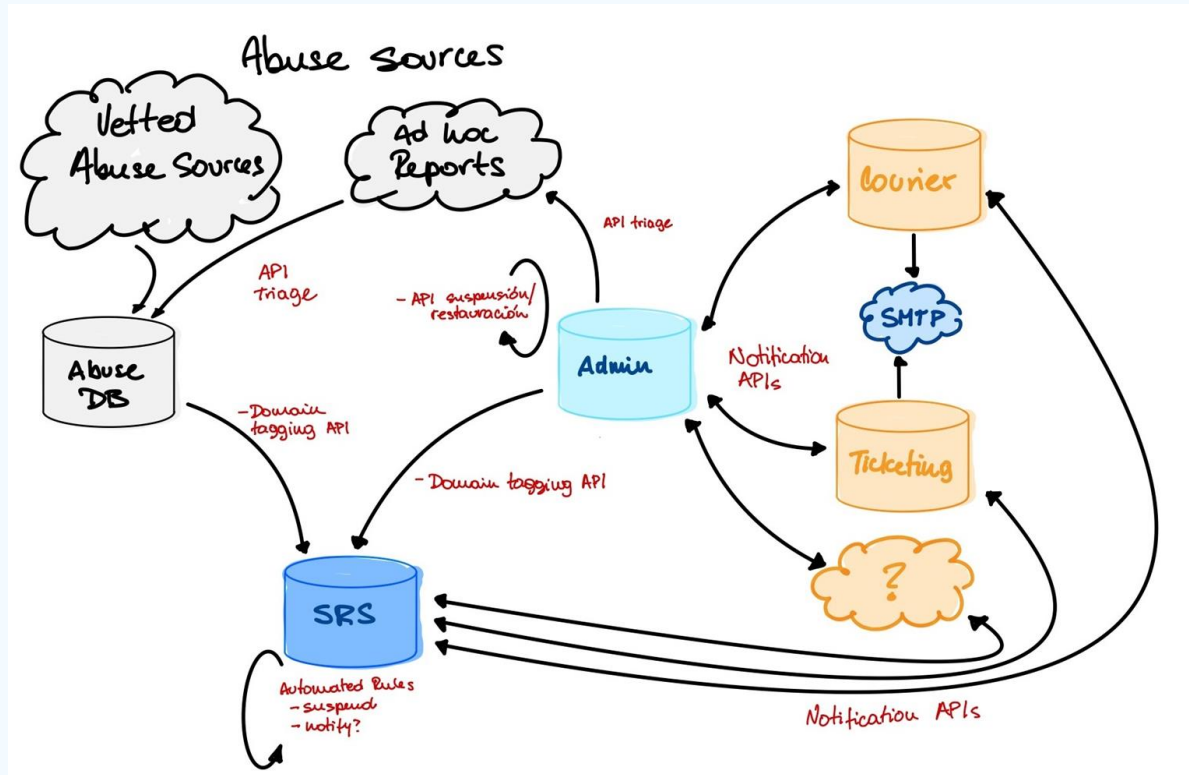
# Abuse Mitigation Goals and Lessons

- Detection and measurement
- Continuous, rich feedback to internal stakeholders
- Develop specialized communication channels with registrars

- Relationships with anti-abuse organizations and LEOs
- Better models, data to advise registry customers about commercial policies
- Improve tooling and monitoring
- Implement abuse thresholds to protect TLD goodwill

- Various integrations to customers' anti-abuse tools and processes
- Interactive tools for customers' abuse analyst teams
- *Augment model using evidence-based processes*

# Abuse Mitigation — Technology Overview



- Capture data from vetted and non-vetted sources
- Normalise data, correct for bias
- Export supported results to SRS for human review and follow up
- Export supported results for automated management reporting

# Abuse Mitigation — Human Review and Management

- Historically, email-based reporting has proved to be the easiest for registries to assimilate
- Integration into the registry admin UI provides for a consolidated view of the domain profile
- Registry can triage and schedule mitigation for domain names at will

The image shows two overlapping screenshots from the Tucows Registry. The background screenshot is an email titled "Daily [redacted] abuse report" addressed to "Dear Stakeholders". It mentions "domain abuse complaints received in the last 24 hours" and includes a table with columns "Domain", "Seen", and "Event". The foreground screenshot is the "Domain Manager" web interface. It features a navigation bar with "Domains", "Registrars", "Reports", "Documents", and "Admin". Below the navigation bar, there are filter options for "Domain name" (containing "Filter by domainName") and "Abuse Types" (listing botnet, deface, malware, phishing, spam, etc.). A table lists domains, with the first entry being "24supportteams.tld", which is marked as "Reported for Abuse". The table includes columns for "Registrar", "Created on", "Expires on", "Registrant", "RPG Status", and "URS Status".

**tucows registry**

Daily [redacted] abuse report

Dear Stakeholders:

Please see below [redacted] domain abuse complaints received in the last 24 hours. Reports from reputable sources have been made. The following results.

Domain	Seen	Event
health [redacted]	2023-07-11	spam

A CSV report with this information

Note:

"Exists" Indicates whether the domain was processed. Some data the DNS, as a way to warn malicious indicators.

"Source" Number of distinct, well-verified sources.

"Event Types" Type of malicious behavior event to be reported for a domain.

Sincerely,  
The Tucows team  
ops@tucows-registry.com

You're receiving this communication as part of our regular reporting process.

Copyright © 2023 Tucows

**tucows registry**

Domains Registrars Reports Documents Admin

### Domain Manager

Domain name [dropdown] contains [dropdown] Filter by domainName [input] + ADD FILTER x REMOVE FILTERS

x Abuse Types are botnet,deface,malware,phishing,spam,spam body,spam new,spam shortener

x Domain name contains 24support

ACTIONS [dropdown] Download CSV [checkbox] Select this page [checkbox] Table view [radio] Off [radio] Off More options [radio] Off [radio] Off Total: 3 rows [1]

<input type="checkbox"/> <a href="#">click</a> 24supportteams.tld	Reported for Abuse			
Registrar	Created on 2023-02-04	Expires on 2024-02-04	Registrant: [redacted] Redacted for Privacy	RPG Status: ok URS Status: Ok
Last billable event on 2023-02-04	Total Discount -\$8.50	Nameservers 2		
Registration \$0.50	Abuse Activity Suspend			

<input type="checkbox"/> <a href="#">click</a> 24supportteams.tld	Reported for Abuse			
Registrar	Created on 2023-02-04	Expires on 2024-02-04	Registrant: [redacted] Redacted for Privacy	RPG Status: ok URS Status: Ok

# Abuse Mitigation

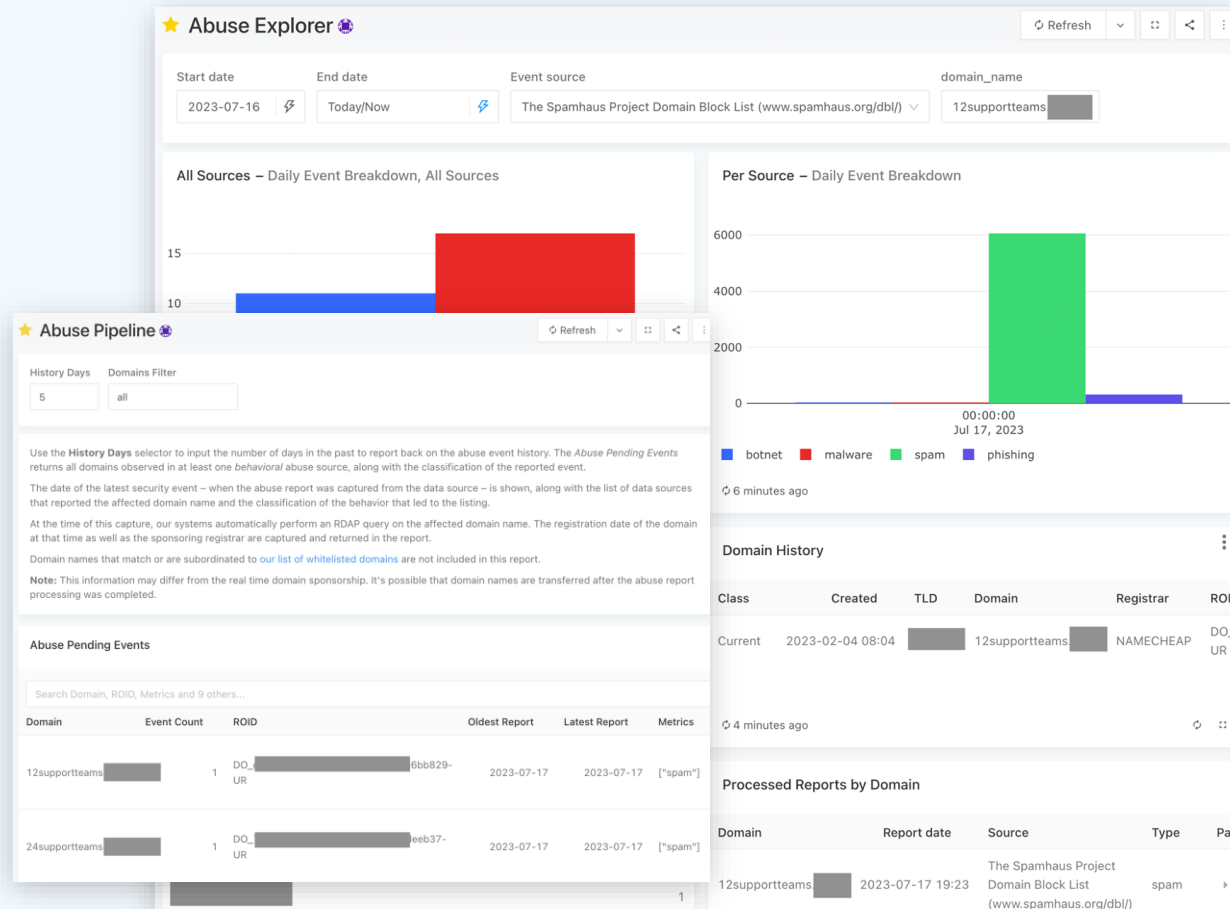
- Baseline technical model
- Email-based reporting
- Manually tuned batch process for notification and suspension
- Involvement of registrar relations areas

- Automated trend monitoring
- Work in pricing / registrar / abuse level correlation
- Abuse pipeline → SRS integration

- *One on one work* with registries to address unique anti-abuse requirements
- *Customized reporting* for 3rd party anti-abuse providers on a *per-client basis*

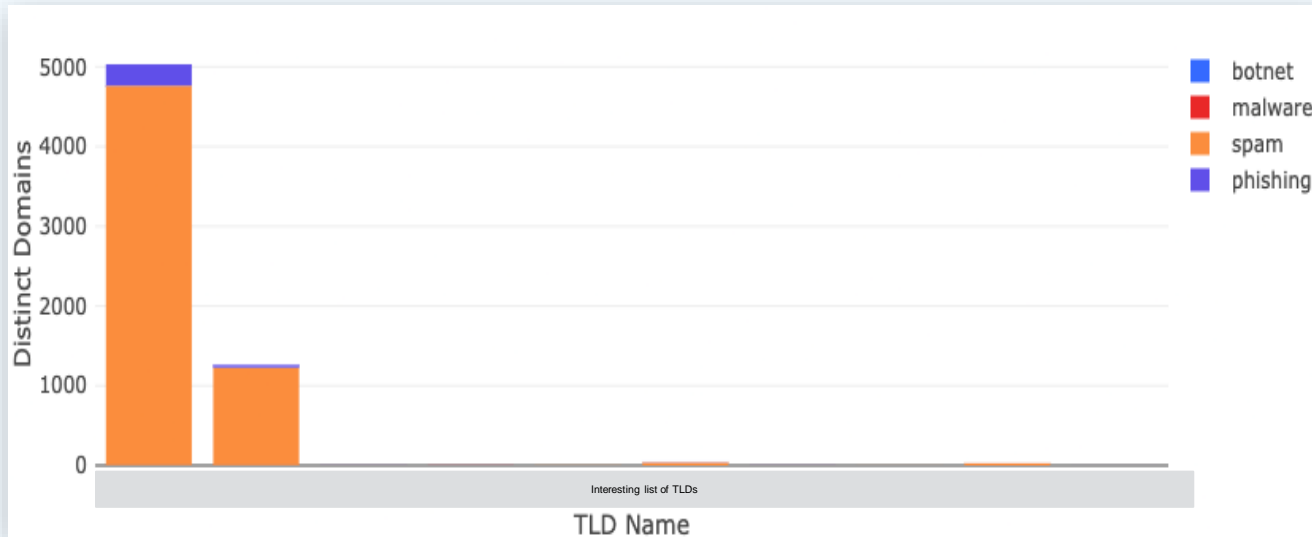
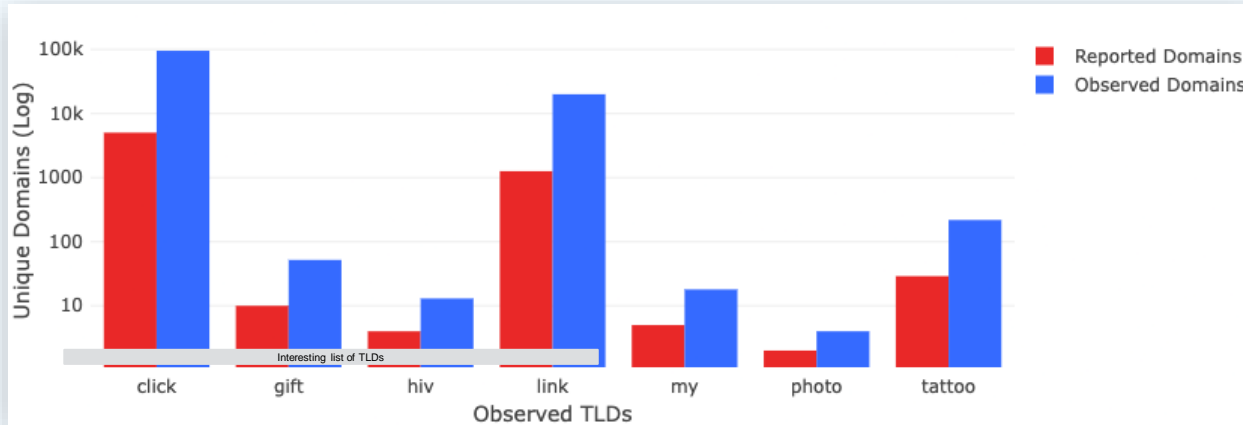


# Abuse Mitigation — Custom Processes



- Customizable reporting provides insight for custom abuse mitigation processes
- Data can be fed to—or from—bespoke tools that notify registrars, suspend promotions, suspend domain names or perform any other action required by the registry

# Abuse Mitigation — Measurements and Indicators



- Specialized trends designed to identify and respond to bad actors registering names for nefarious purposes
- Abuse data can be folded into promotion eligibility, ensuring registrars will participate in the upkeep of the namespace
- Each registry can implement its own set of policies independently

# Questions?

[tucows/registry](https://tucows/registry)

**Thank you!**

# Thank you!

Raedene McGary  
[Rmcgary@tucows.com](mailto:Rmcgary@tucows.com)

**tucows/registry**