Domain Abuse Activity Reporting (DAAR)

Edward Lewis (in person) for Dr. Samaneh Tajalizadeh Khoob

APTLD 76
5 September 2019
The Problem Statement

- Growing need for proactive detection and mitigation strategies by TLD operators & registrars

- Lack of visibility into
  - Abuse concentrations in TLD registrations
    - Quantify the challenges
  - Abuse mitigation performance in comparison to peers
    - Quantify effectiveness
What is DAAR?

- A system for reporting on domain name registration and abuse data across TLD registries and registrars
  - A methodology that is reproduceable
  - Relies on external data feeds

- Anyone can replicate the work but they will have to "purchase" the needed data feeds
DAAR Process Flow

Centralized Zone Data Service
*TLD Zone Files*

List of Delegated Names

Registration Information *(Whois/RDAP)*

Industry Reputation (Block/Black) Lists

DAAR Reputation Metrics per Registry
Current Reputation Lists Included

- SURBL Lists (surbl.org): Spam, Phishing, Malware
- Spamhaus Domain Block Lists: Spam, Phishing, Malware, Botnet C&C
- Anti-Phishing Working Group (APWG): Phishing
- Malware Patrol: Malware, Ransomware, Botnet C&C
- Phishtank: Phishing
- ABUSE.CH: Ransomware tracker, Feodo tracker

*Using Domains information only*
Abuse Type Distribution

- Spam Domains: 87.8%
- Malware Domains: 3.4%
- Phishing Domains: 6.8%
- Botnet C&C Domains: 2.0%
Abuse Counts - Absolute and Relative to Size – among gTLDs

- Shown only to demonstrate that DAAR is currently operating
- Much more detail is covered and ongoing work to analyze
Access to DAAR Data

- General Public
  - Aggregate results are published on the ICANN web site
    - https://www.icann.org/octo-ssr/daar
  - Monthly reports for 2018 and 2019
  - Public comments on the DAAR
  - Methodology paper

- ICANN's Contracted Registries
  - Access their own, per-TLD, data via an API dedicated for contracted parties
  - Per-TLD data is not publicly distributed
Project Next Steps

- **Methodology**
  - Improving the system based on comments and reviews
  - Developing and documenting a process for systematically reviewing feeds

- **Results**
  - Developing similar metrics for registrars and ccTLDs
  - Developing new metrics and analytics based on DAAR (e.g., looking at other TLD related attributes in addition to legacy and new [2012])?

- Having ongoing discussions with contracted parties and others to keep improving DAAR
Engage with ICANN

Thank You and Questions
Visit us at icann.org or https://www.icann.org/octo-ssr/daar
Email: daar@icann.org, samaneh.tajali@icann.org, john.crain@icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann
instagram.com/icannorg