Domain Abuse Activity Reporting (DAAR)

Looking back and forward

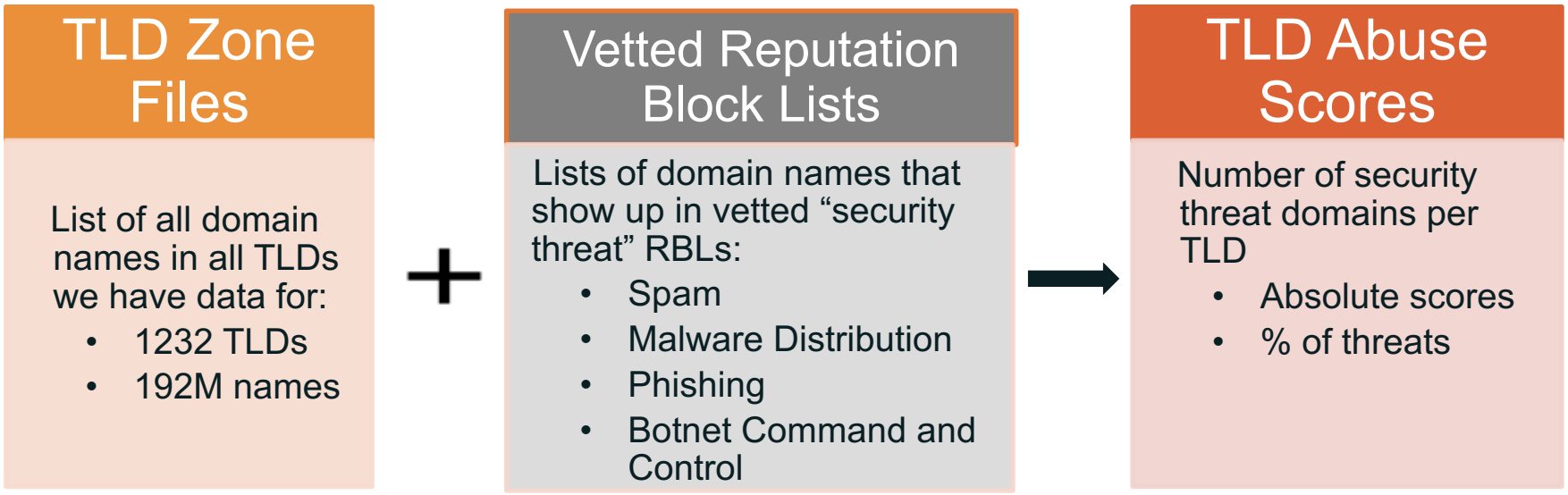
Dr. Samaneh Tajalizadehkhoob
Lead Security, Stability & Resiliency Specialist
ICANN Office of CTO

At Large Advisory Committee (ALAC)
25 August 2021

DAAR Project Goals, Uses, and Limitations

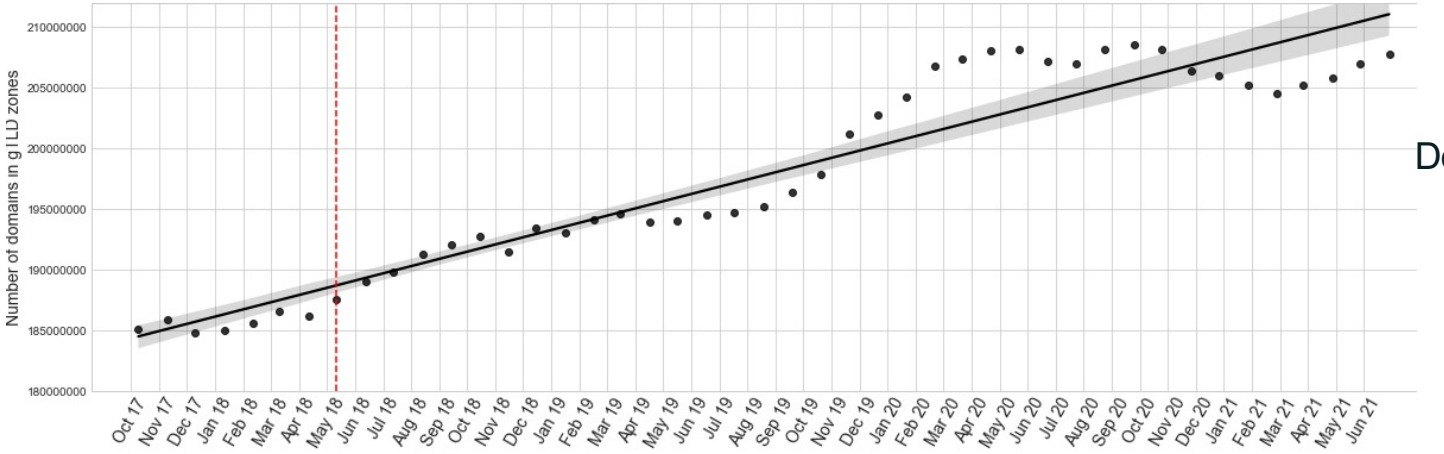
- Be a robust, reliable, reproducible, and replicable methodology for analyzing security threat activity that can then be later used by the ICANN community to facilitate informed policy decisions.
- DAAR data **CAN** be used to
  - Report on threat activity at TLD (or, in the future registrar) level
  - Historical analysis of security threats or domain registration activity
  - Help operators understand their reputations in the DAAR RBLs or the impact of their anti-abuse programs or terms of service
- DAAR data **CANNOT** be used to
  - Provide info about mitigation
  - Distinguish maliciously registered vs. compromised domains
  - Provide information on individual security threats within domains
  - Rank TLD providers in terms of their security concentrations

DAAR Methodology



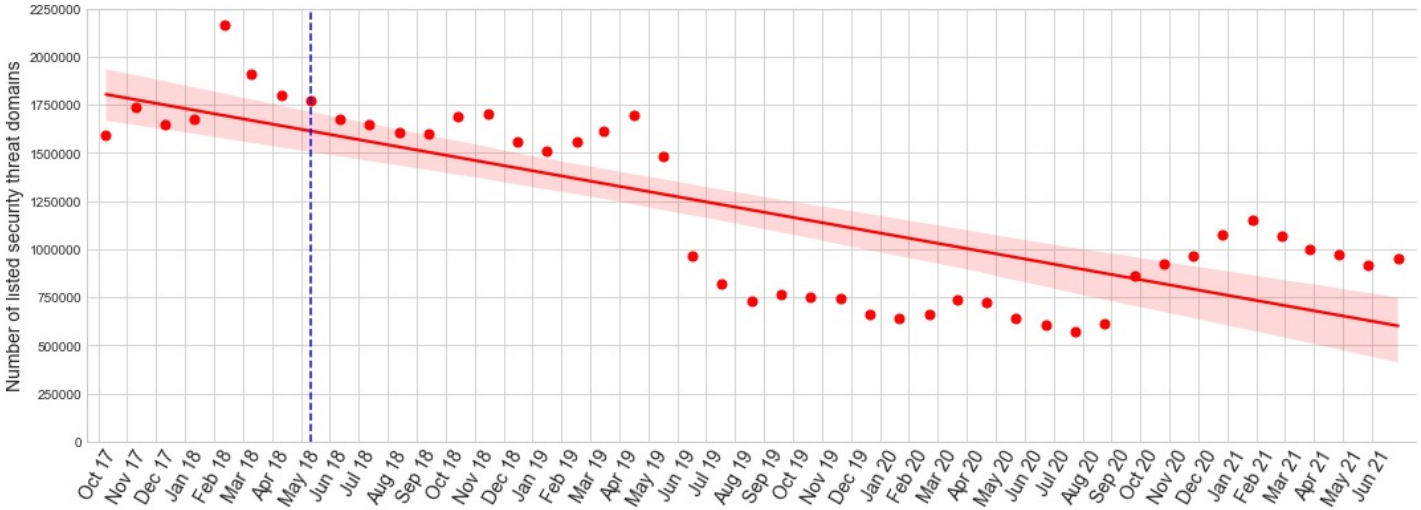
- Monthly reports (from Jan 2018) published at https://www.icann.org/octo-ssr/daar
- Daily scores made available to TLDs via the Monitoring System API (MoSAPI)
  - Allows comparison to monthly statistics

General trends in gTLDs

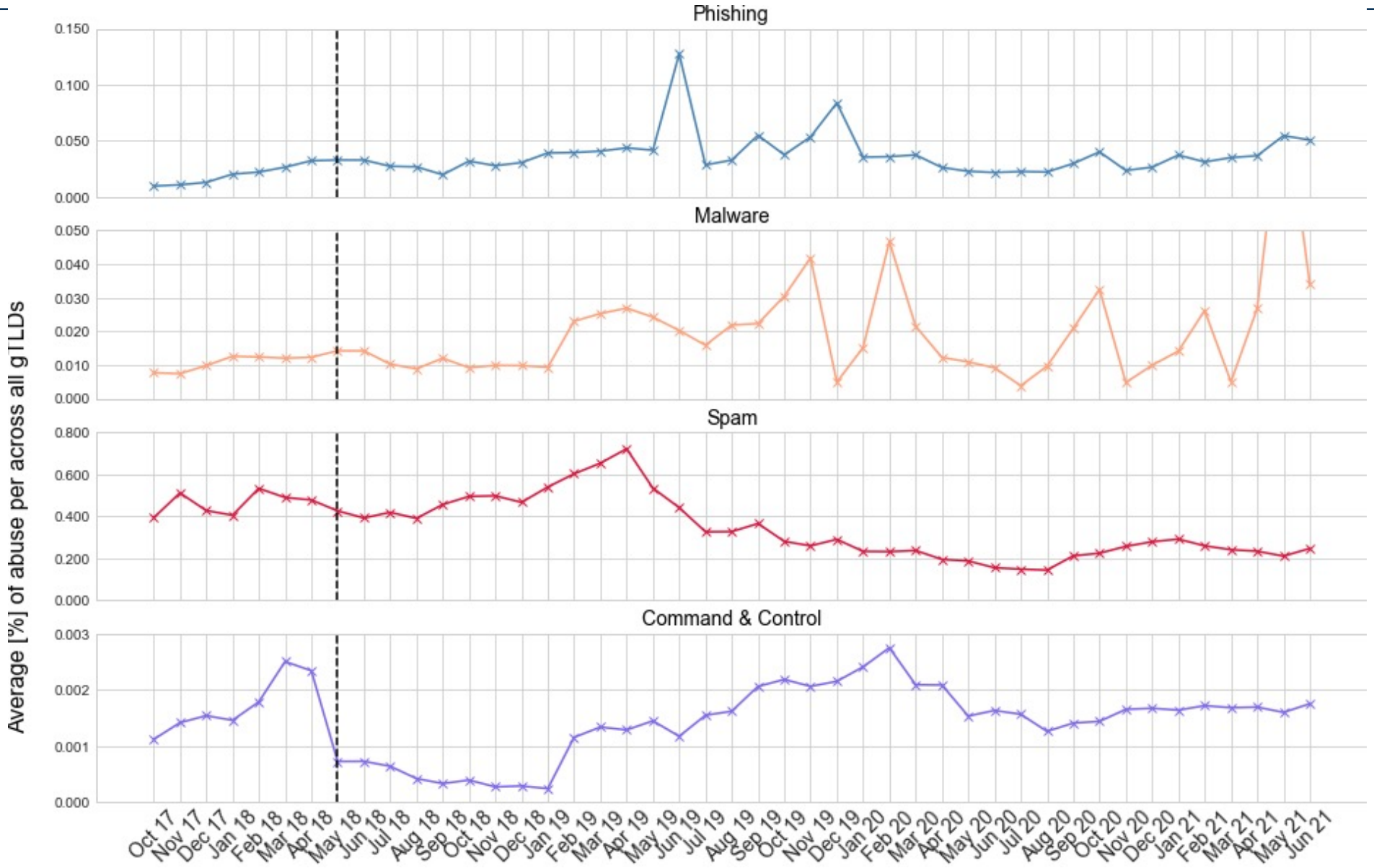


Domains in gTLD zones

Security threat domains in gTLDs



ICANN


Phishing
Malware
Spam
Command & Control
Average [%] of abuse per across all gTLDs
0.150
0.100
0.050
0.000
0.040
0.030
0.020
0.010
0.800
0.600
0.400
0.200
0.003
0.002
0.001
Oct 17
Nov 17
Dec 17
Jan 18
Feb 18
Mar 18
Apr 18
May 18
Jun 18
Jul 18
Aug 18
Sep 18
Oct 18
Nov 18
Dec 18
Jan 19
Feb 19
Mar 19
Apr 19
May 19
Jun 19
Jul 19
Aug 19
Sep 19
Oct 19
Nov 19
Dec 19
Jan 20
Feb 20
Mar 20
Apr 20
May 20
Jun 20
Jul 20
Aug 20
Sep 20
Oct 20
Nov 20
Dec 20
Jan 21
Feb 21
Mar 21
Apr 21
May 21
Jun 21

Modifications Made to DAAR

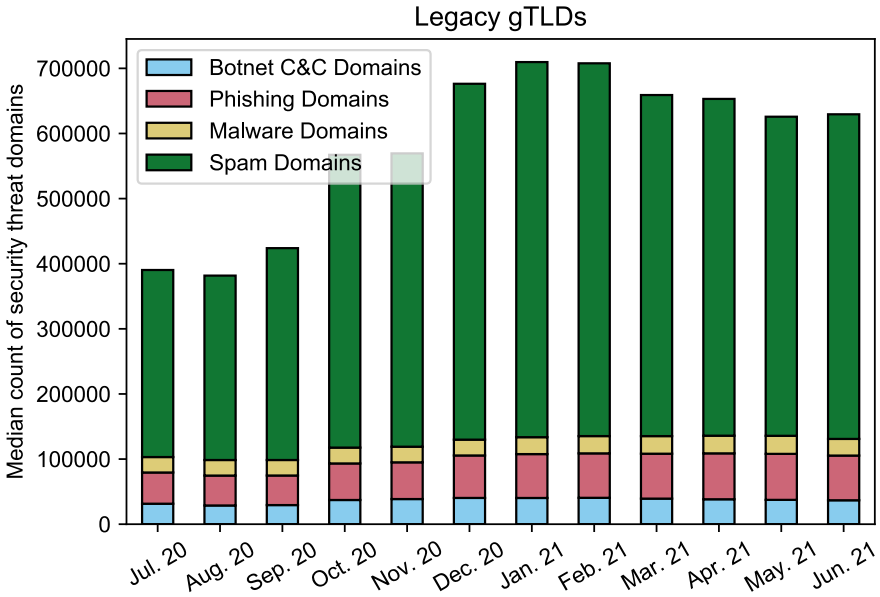
DAAR Monthly Report

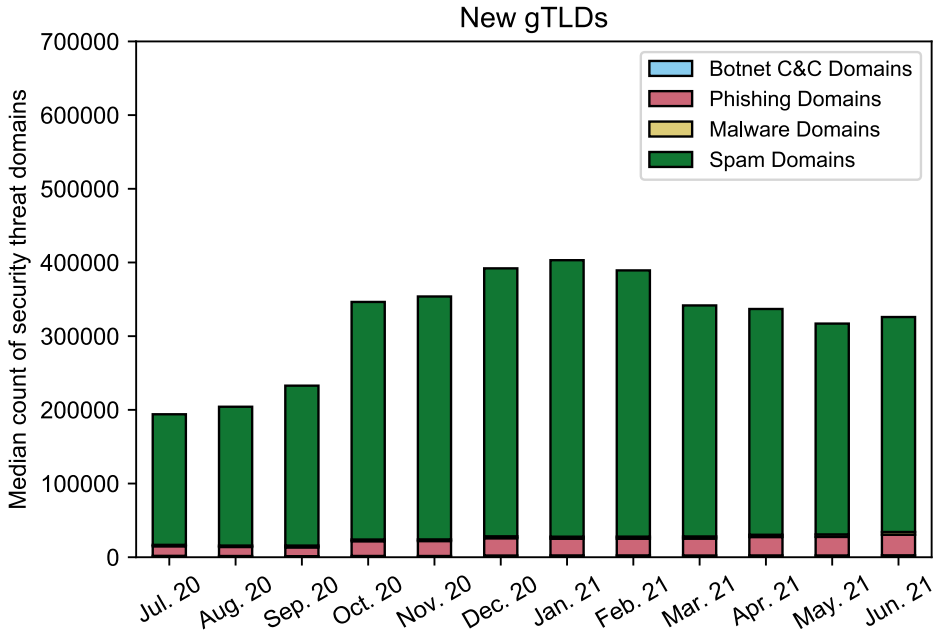
Modifications

- The language throughout the report has been updated. Where applicable, the term [abuse] has been replaced with the term [security threat], as the term [abuse] could include a broader set of threats including those outside ICANN's remit.
- All the point-in-time metrics (metrics created based on the last day of the month) have been updated to averages (median) over a month.
- Most plots that combined multiple types of security threats have been removed from the document, except for those that aim to show the importance of the normalized [percentage of security threat] metric.

Modifications

- New plots have been added to the report which show the percentage of security threats over time and in proportion to total domains in zone files (figures 2 and 3 in the report). Examples below:





DAAR online documentation

Modifications

- The language used throughout the DAAR online web page and FAQ page has been updated. Where applicable, the term [abuse] has been replaced with the term [security threat], as the term [abuse] could include a broader set of threats, including those outside of ICANN's remit. The change will be applied to all of the online documents.
- New text has been added to the DAAR web page to clarify what the DAAR reports and DAAR data can and cannot show. This includes clarifications about Reputation Block List (RBL) feeds, DAAR and its relationship with mitigations, and differences between maliciously registered and compromised domains.
- The online docs are translated in a few languages e.g., Spanish, French, Chinese, Russian, Arabic

DAAR System

CCTLDs in DAAR Since June 2020

14 of 316 ccTLDS are participating in DAAR:

- .au (Australia)
- .se (Sweden)
- .tw (Taiwan)
- .cl (Chile)
- .nu (Niue)
- .ee (Estonia)
- .tz (Tanzania)
- .gt (Guatemala)
- .sv (El Salvador)
- .mw (Malawi)
- .gg (Guernsey)
- .je (Jersey)
- .ch (Switzerland)
- .ke (Kenya)

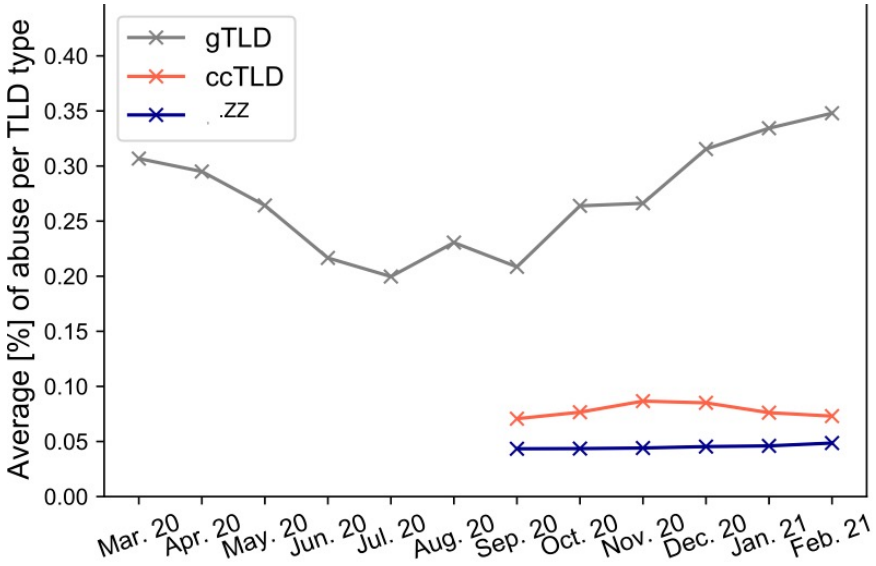
We provide:

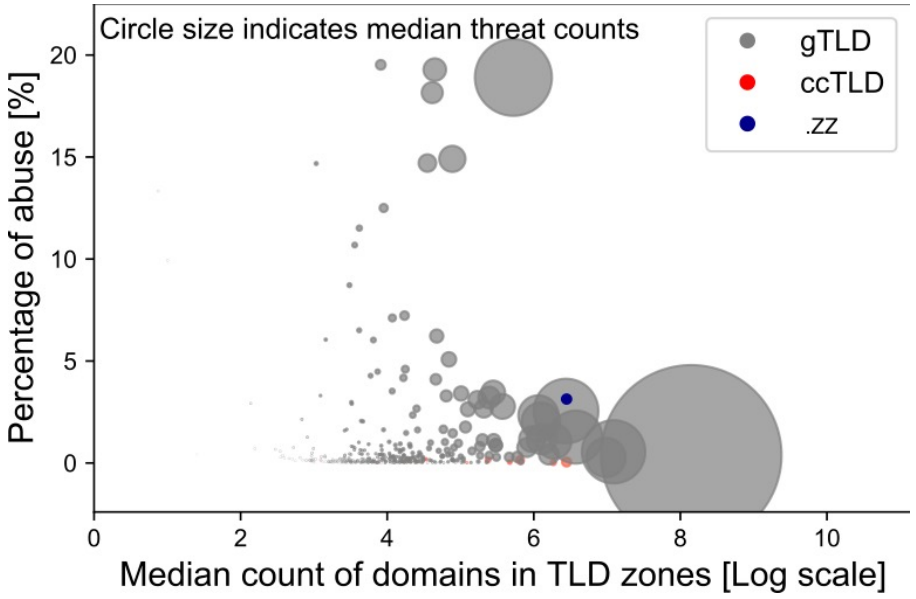
- Daily DAAR stats
- **Individualized** DAAR monthly reports

Latest blog post about DAAR and ccTLDs:

https://www.icann.org/news/blog/daar-activity-project-now-providing-personalized-monthly-reports-for-cctlds

Individualized Report Example: Aggregate Threats over All TLDs





Steps for a ccTLD to join DAAR

1. ccTLD makes a request by sending an email to globalsupport@icann.org.

   Signing an MoU is also possible

2. The global support team will initiate a procedure to confirm the request by sending a couple of emails to both technical and administrative contact of the ccTLD as it is registered in IANA.
3. Once the request is confirmed by all parties, ICANN starts the procedure of taking the zone files in.
4. Once the zone file is in, it will be shared with iThreat Cyber Group, the contractor that maintains the DAAR system.
5. The ccTLDs will be able to access their own DAAR data via ICANN's Monitoring System API (MOSAPI) on a daily basis. For now, the data will be only published via the API to the ccTLDs themselves. We are further working on how to further publish general statistics of participating ccTLDs along with the DAAR personalized monthly reports.

Evolving DAAR

Future Plans

- Adding more ccTLDs
- Provide individualized reports to all DAAR participants
- Publish methodology for RBL evaluations
- Solutions for allowing SSR to use data from Bulk Registration Data Access (BRDA)

DAAR Evolution

- A framework/infrastructure to collect multiple time-series data points
- A dashboard (website) that offers several possible functionalities, namely:
- Extra features/data point on domain names
  - Domain popularity, traffic score (See Tranco or DNS Magnitude for reference)
  - Additional abuse evidence
  - Reverse searches pivoting on name servers, A/AAAA/MX records to identify other malicious domains within a given TLD, or a registrar's portfolio
  - Closeness [similar words in the domain, similar registrar, same host etc.] with other already listed security threat domains
  - Future abuse risk score: a score that we give every domain as an abuse risk prediction based on a set of features - the result of our abuse predictive work will go here
  - Possibility to be connected to ITHI and ICANN Open Data
  - If already compromised, we provide status of malicious vs compromised using COMAR technique

DAAR Evolution

- Possibility to aggregate information on more than one level such as domain name (host), gTLD, name servers, and eventually registrars
- Historical analysis of all features collected
- Visualizations: the dashboard includes predefined filters and visuals that can be selected by users
- An API that can be queried by any authorized user and provides curated data that is collected by the platform
- Create a modular design, meaning that we start with one module (could be the current DAAR) and add additional modules over time. Each module could be a feature from measurements that are done by others (where code is open source), or it could be our own measurements. This way we have the flexibility to start small and extend the platform as we move forward by our own or external measurements.

Thank You and Questions

Visit us at **icann.org**

daar@icann.org

Samaneh.tajali@icann.org

 @icann

 linkedin/company/icann

 facebook.com/icannorg

 slideshare/icannpresentations

 youtube.com/icannnews

 soundcloud/icann

 flickr.com/icann

 instagram.com/icannorg