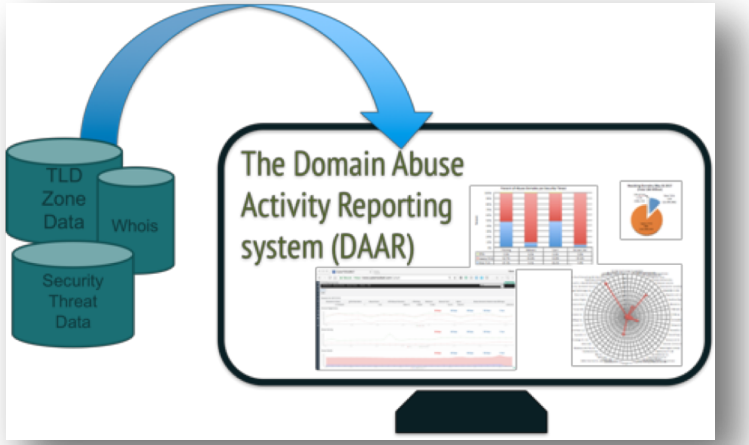

ICANN
COMMUNITY FORUM
64
KOBE
9–14 March 2019
MOSAIC

Domain Abuse Activity Reporting (DAAR)

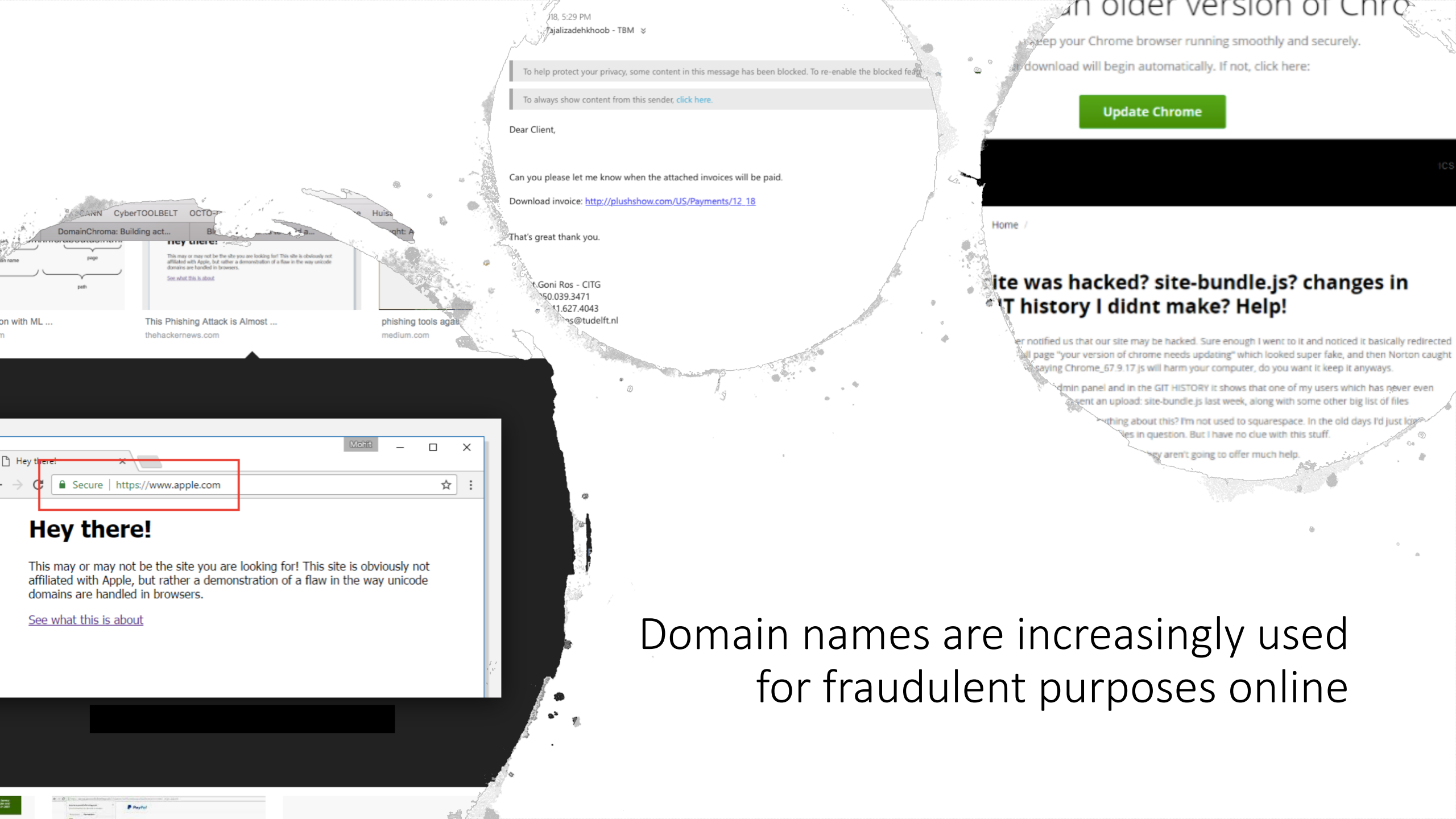
Dr. Samaneh Tajalizadehkhoob
Lead Security, Stability & Resiliency Specialist
ICANN Office of Chief Technology Officer (OCTO)

March 2019



Who Am I?

- Since October 2018 **Lead Security, Stability & Resiliency Specialist** @ ICANN Office of Chief Technology Officer (OCTO)
- DAAR **project owne**r – Research on **DNS, Identifier Security**
- Located in the **Netherlands**
- **Electrical Engineer** by training, PhD in **Web Security and Advance Analytics**
- Strong research background in Internet Measurements, Economics of Web Security, Security of Internet Identifiers, Banking Security, Advance Statistical Analysis, and Machine Learning



Domain names are increasingly used for fraudulent purposes online

Therefore …

- A **growing** need for proactive detection and mitigation strategies by providers

Currently Heterogenous Anti-Abuse Measures:

- Some providers are very active
- Others lack of knowledge about abuse concentrations in **own networks**

and

perform in **comparison to their peers**

Why Abuse is not Regularly Monitored?

Abuse not monitored mainly because:

- Thin profit margins therefore little space for extra costs
- No unified methodology for abuse monitoring/reporting
- **Mainly** not enough incentives

Domain Abuse Activity Reporting (DAAR)

The Domain Abuse Activity Reporting System

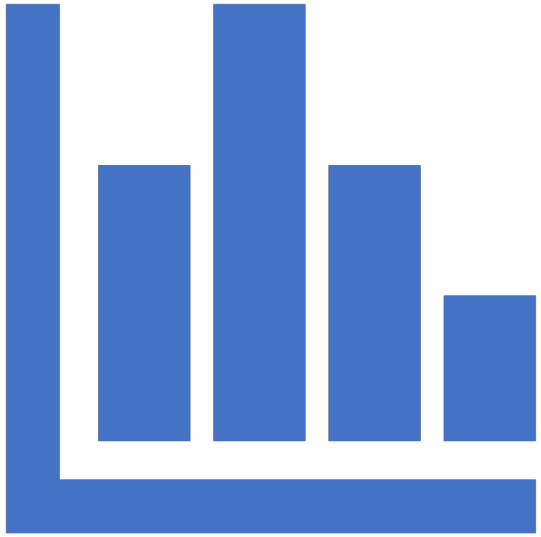
What is the Domain Abuse Activity Reporting system?

A system for reporting on domain name registration and abuse data across TLD registries and registrars

DAAR not the First Abuse Reporting System

How does DAAR differ from other reporting systems?

- Studies all gTLD registries and (registrars) for which we can collect zone and registration data
- Allows historical research
- Studies multiple threats: phishing, botnet, malware, and spam
- Employs a large set of abuse feeds (e.g., blocklists)
- Takes a scientific approach: transparent, reproducible



DAAR data can be used to

- Study malicious registration behaviors
- Report on threat activity at TLD level
- Study historical security threat concentrations
- Assist operational security communities and academic research
- Help operators understand or consider how to manage their reputations, anti-abuse programs, or terms of service

More informed security decision making and policy

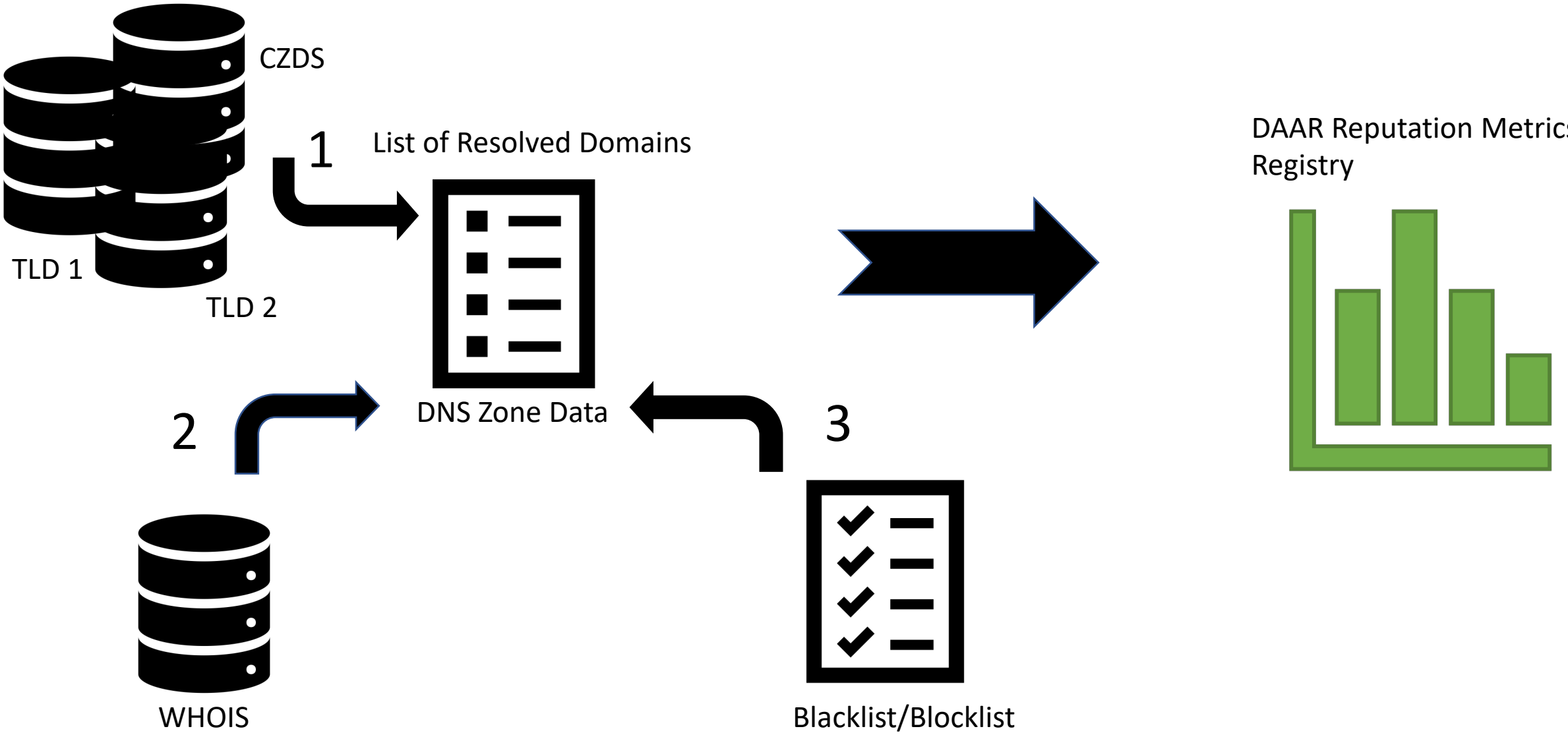
DAAR Methodology & Data

Data Sources

I. DNS zone data
II. WHOIS data
III. Open source or commercial abuse threat (RBL) data*

*Certain data feeds require a license or subscription

Methodology



Reputation Block Lists : Identifying Threats

Security Threat Types

DAAR collects domain data for

- Phishing
- Malware
- Spam
- Botnet Command & Control

Does DAAR Identify All Abuse Data/Types?

- **No**. DAAR lists domain names associated with abuse identified by third parties.
- Only those names associated with generic TLDs are measured and only for specific abuse types.

DAAR Criteria for RBL Data Selection

- Threat classification that matches our set of security threats
- Positive reputation in academic literature, in operational and security communities for accuracy, clarity of process
- Broadly adopted across operational security community
  - Incorporated into commercial security systems
  - Used by network operators
  - Used by email and messaging providers

Is DAAR an Abuse List Service?

- ICANN does not compose its own reputation blocklists
  - DAAR presents a composite of the data that external entities use to block threats

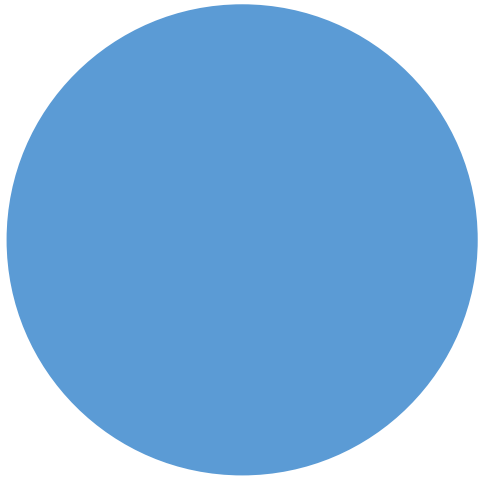
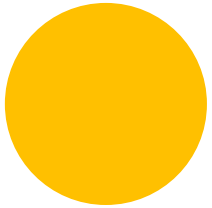
- DAAR collects the same abuse data that is reported to industry and Internet users and is used by
  - Commercial security systems
  - Academia and industry

- Academic studies and industry use validate these datasets exhibit accuracy, global coverage, reliability and low false positive rates

Current Reputation Datasets

Domains only

- SURBL lists (Spam – Phishing - Malware)
- Spamhaus Domain Block List (Spam - Phishing - Malware - Botnet C&C)
- Anti-Phishing Working Group (Phishing)
- Malware Patrol (Malware, Ransomware, Botnet C&C)
- Phishtank (Phishing domains)
- ABUSE.CH (Ransomware tracker, Feodo tracker)

DAAR Monthly Reports

Domain Abuse Activity Reporting

ICANN's Domain Abuse Activity Reporting (DAAR) project is a system for studying and reporting on domain name registration and security threat (domain abuse) behavior across top-level domain (TLD) registries and registrars. The overarching purpose of DAAR is to report security threat activity to the ICANN community, which can then use the data to facilitate informed policy decisions.

DAAR was designed to provide the ICANN community with a reliable, persistent, and reproducible set of data from which security threat (abuse) analyses could be performed. The system collects TLD zone data, a very large body of registration data, and complements these data sets with a large set of high-confidence reputation (security threat) data feeds. The data collected by the DAAR system can serve as a platform for studying or reporting daily or historical registration or abuse activity.

Domain Abuse Activity Reporting FAQ

Domain Abuse Activity (DAAR) Monthly Reports

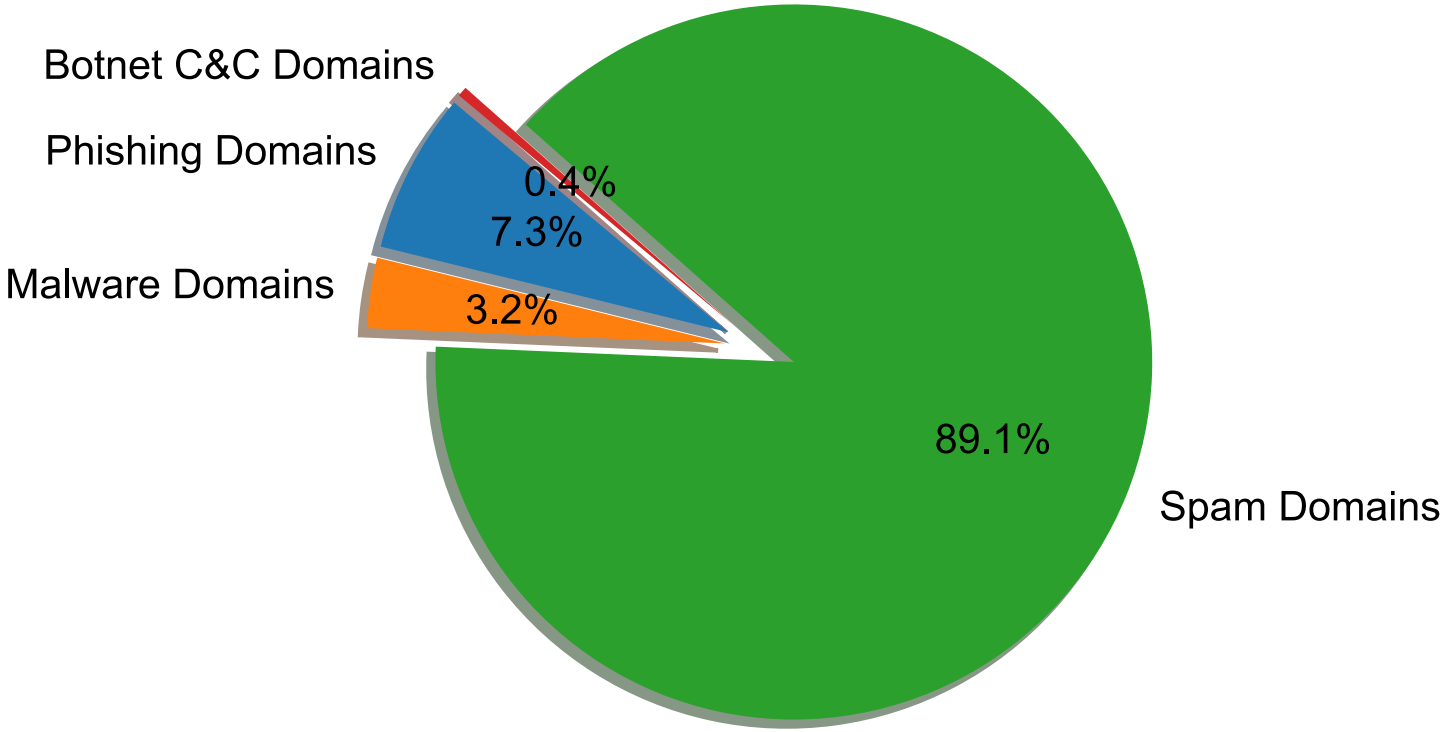
Context Document: Understanding the DAAR Monthly Report [PDF, 72 KB]

2018

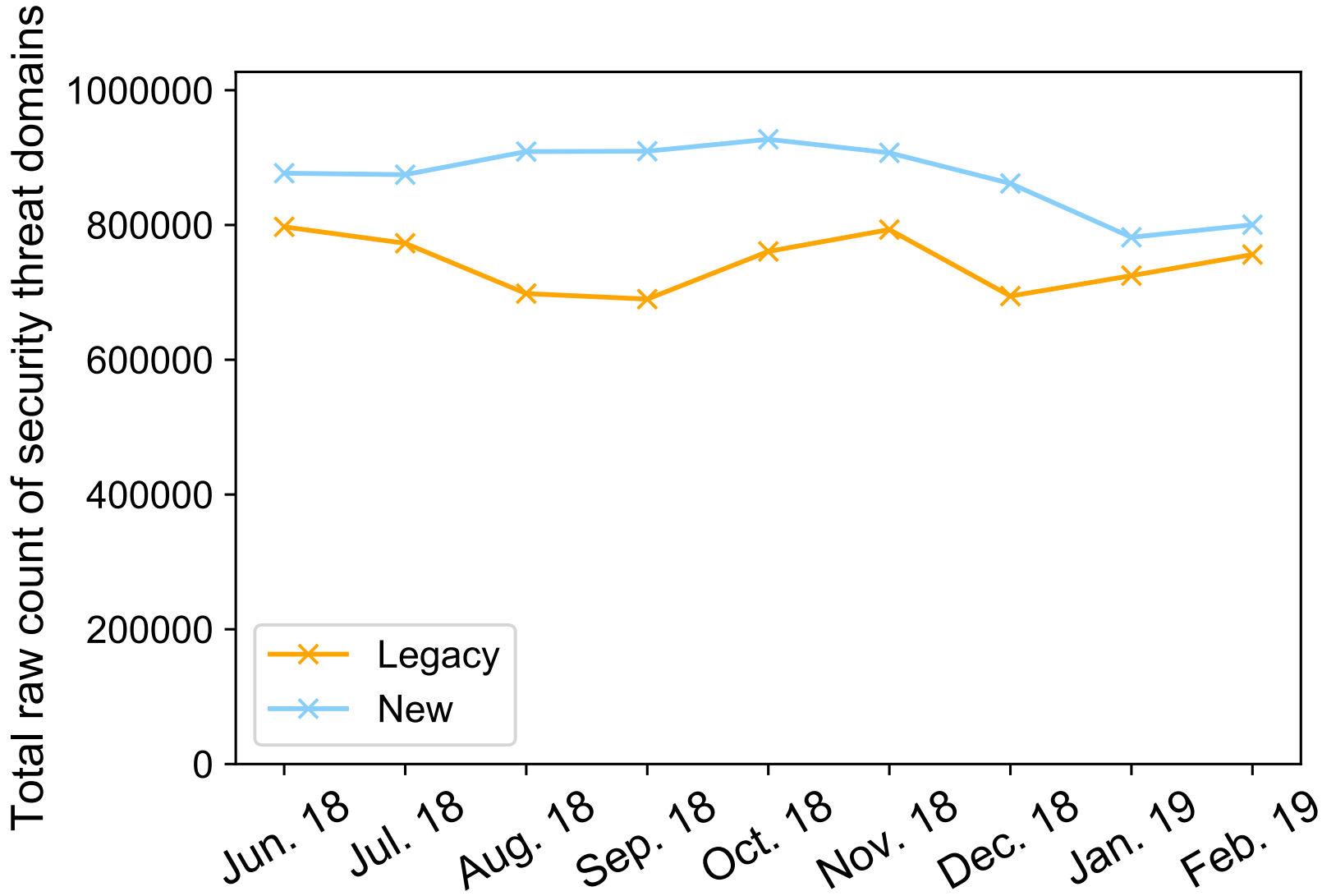
- January 2018 DAAR Monthly Report [PDF, 824 KB]
- February 2018 DAAR Monthly Report [PDF, 511 KB]
- March 2018 DAAR Monthly Report [PDF, 526 KB]
- April 2018 DAAR Monthly Report [PDF, 526 KB]
- May 2018 DAAR Monthly Report [PDF, 517 KB]
- June 2018 DAAR Monthly Report [PDF, 527 KB]

https://www.icann.org/octo-ssr/daar

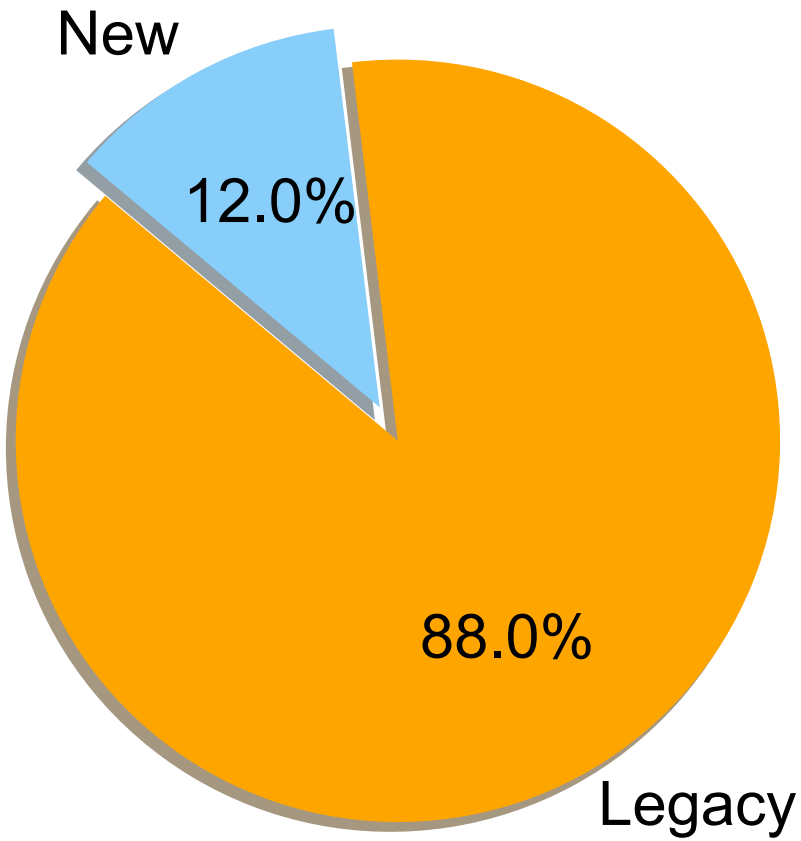
Overall Abuse Distribution in DAAR Data (Jan. 2019)



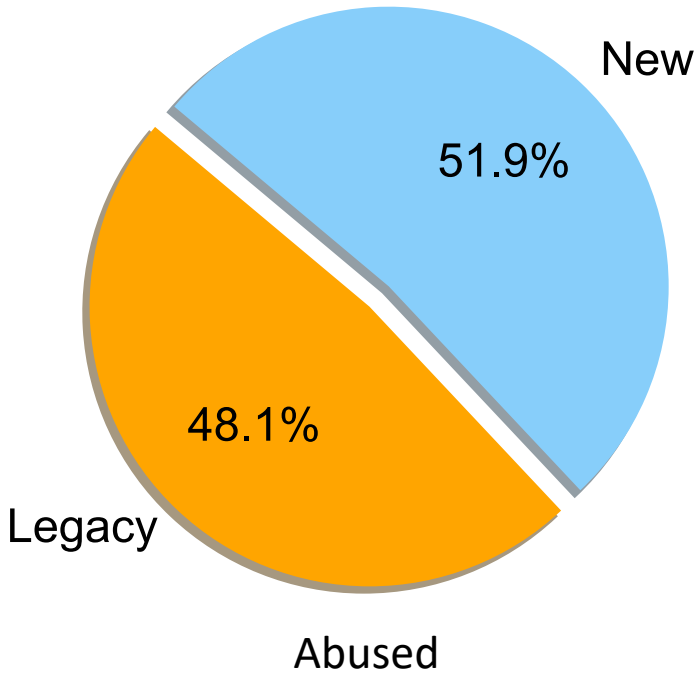
Total Number of Domains Identified as Security Threat

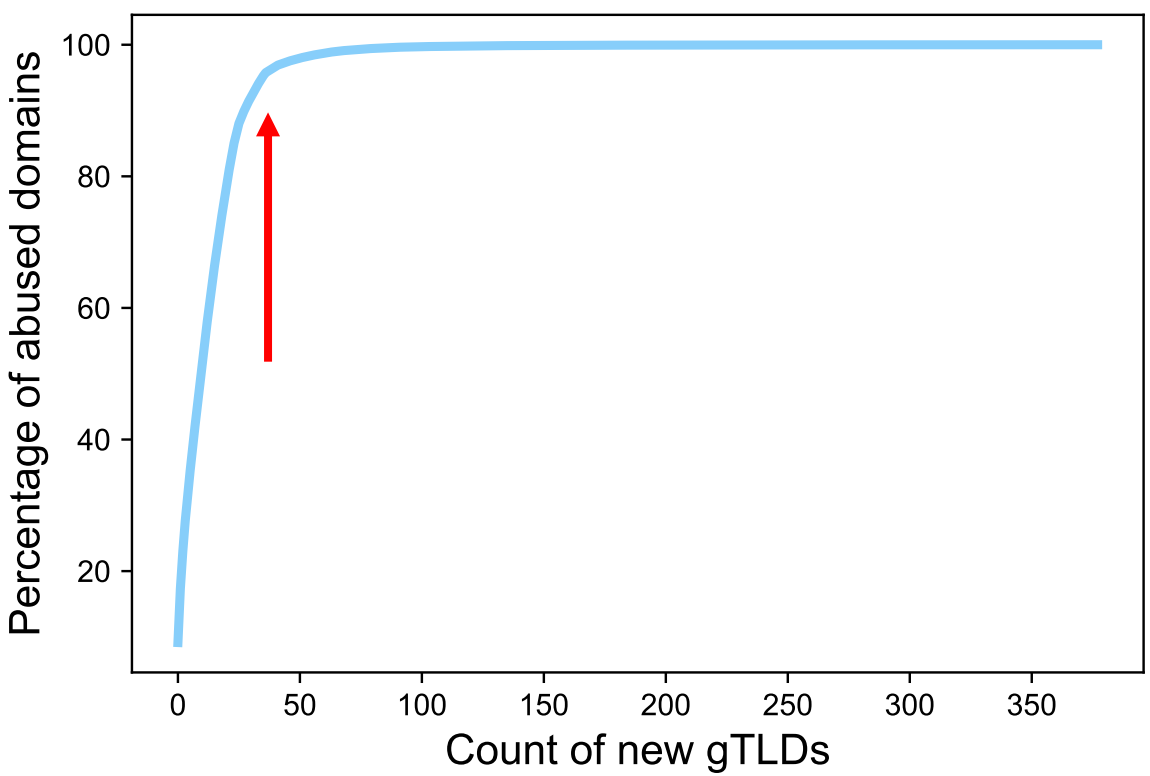


Distribution of Resolved Domains in gTLDs

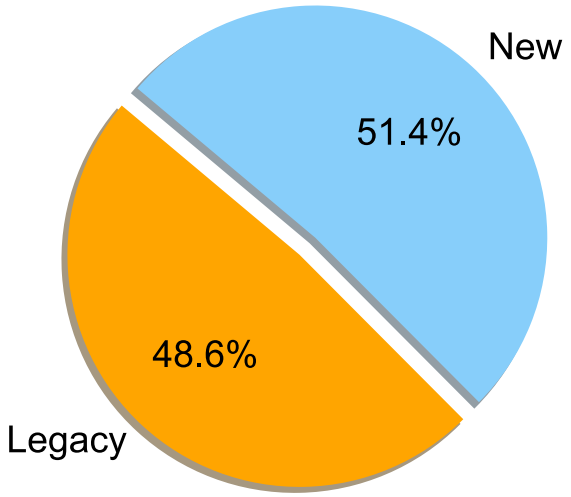


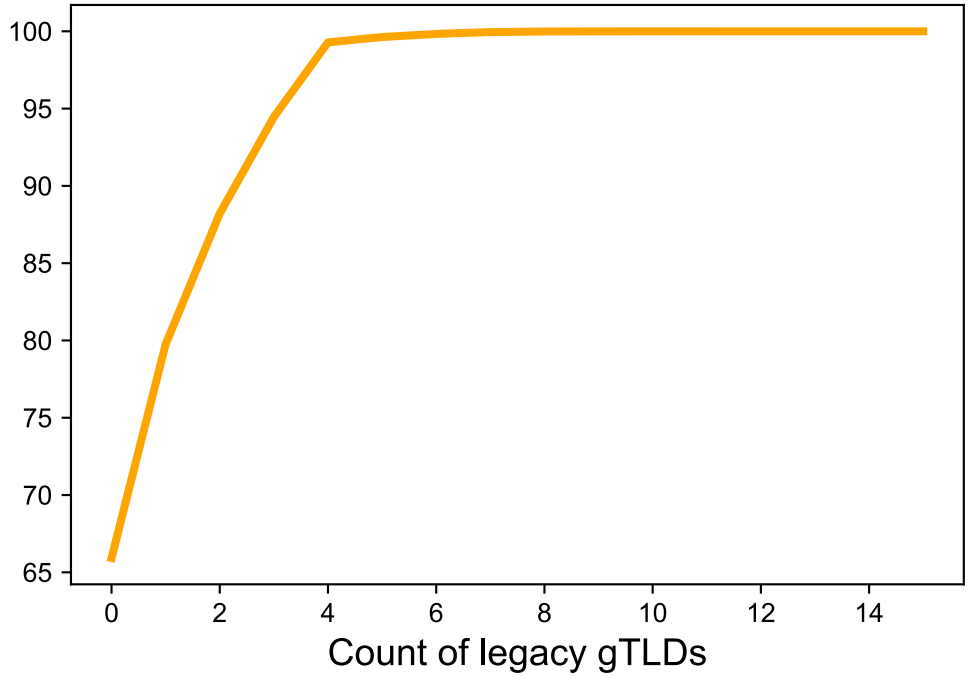
How Many gTLDs are Driving the Bulk?



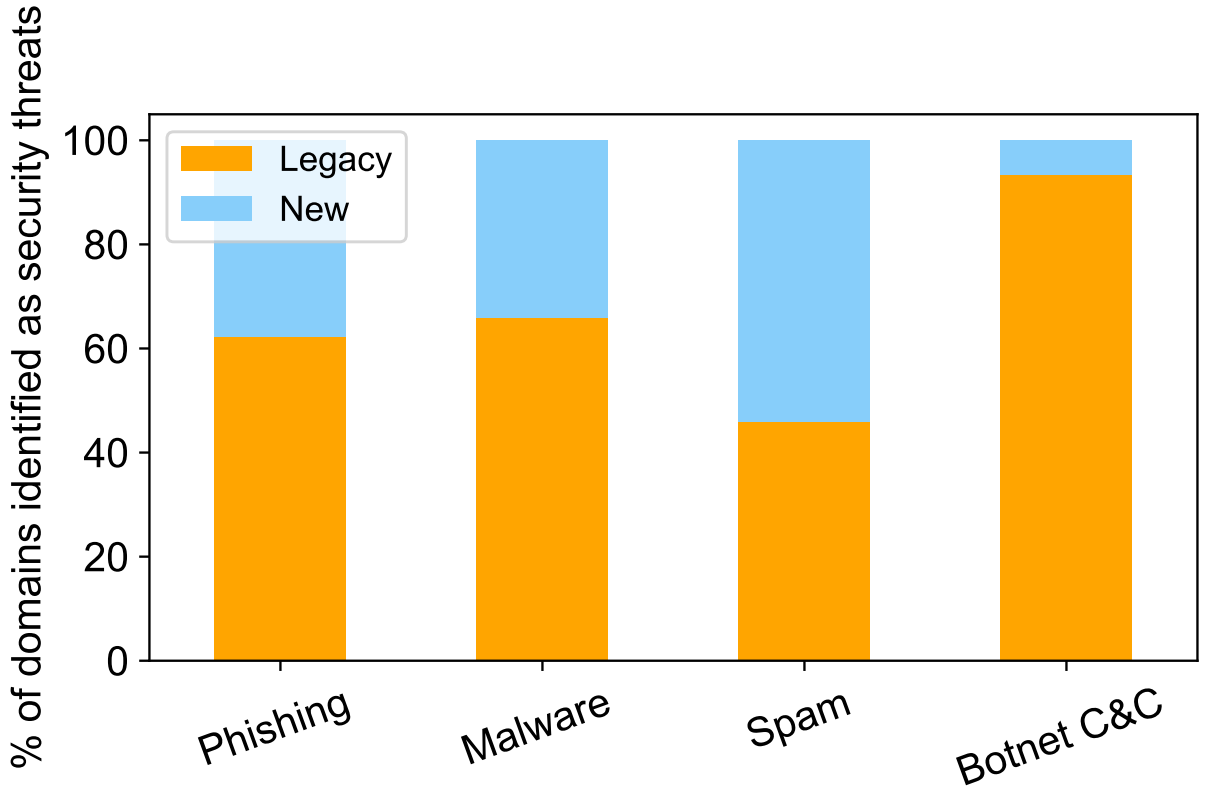


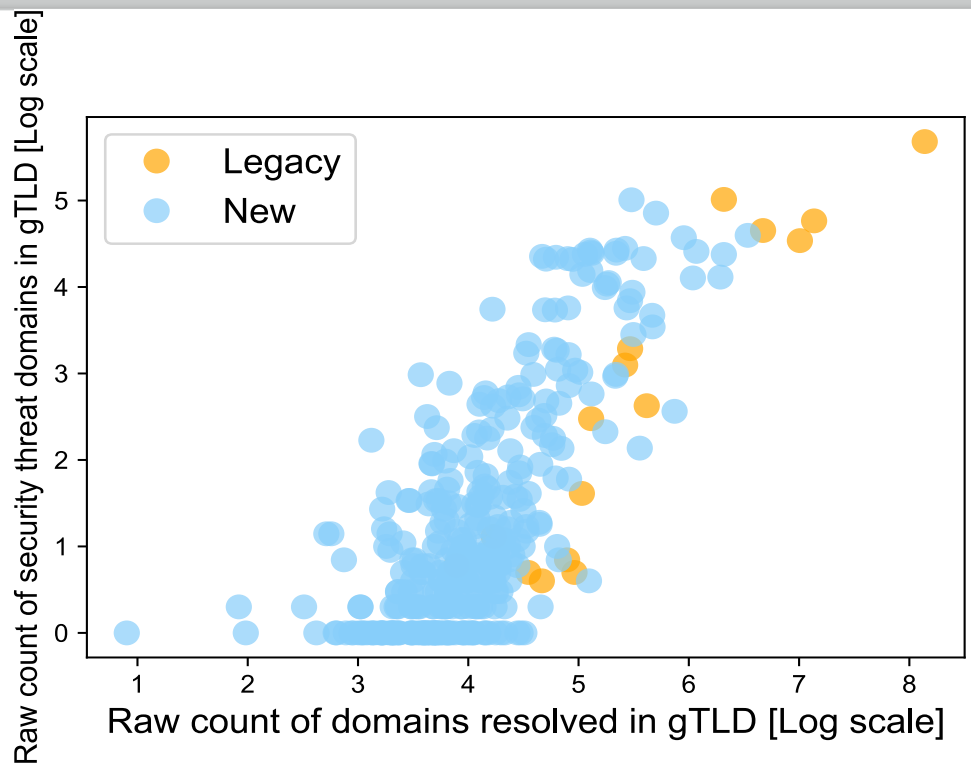
How Many gTLDs are Driving the Bulk?

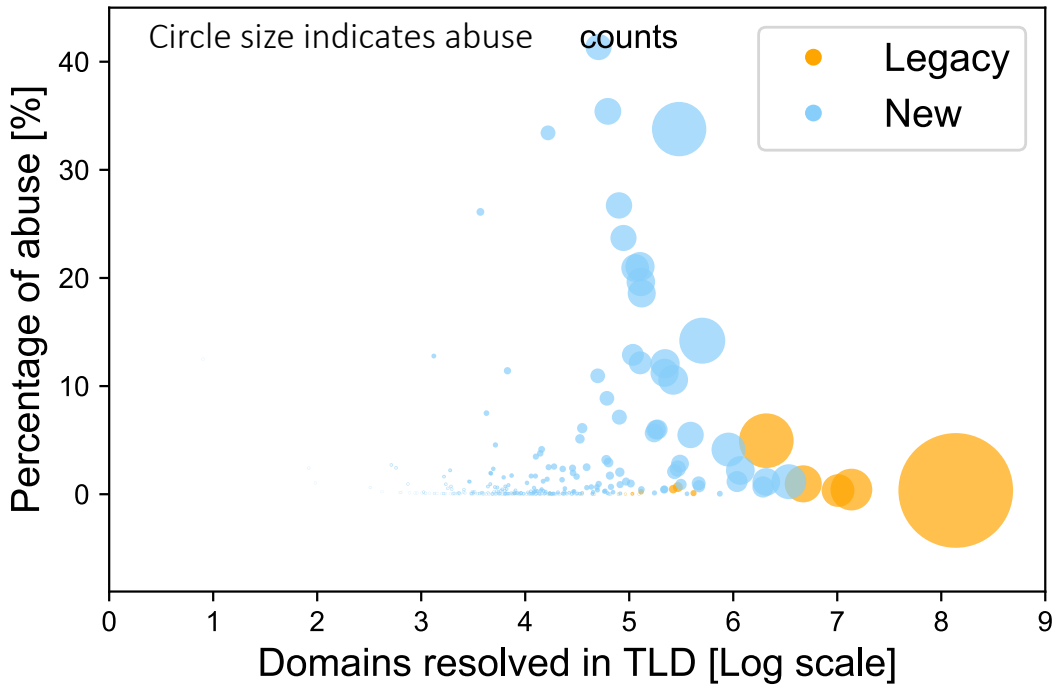




Distribution of Domains with Different Abuse Types in gTLDs

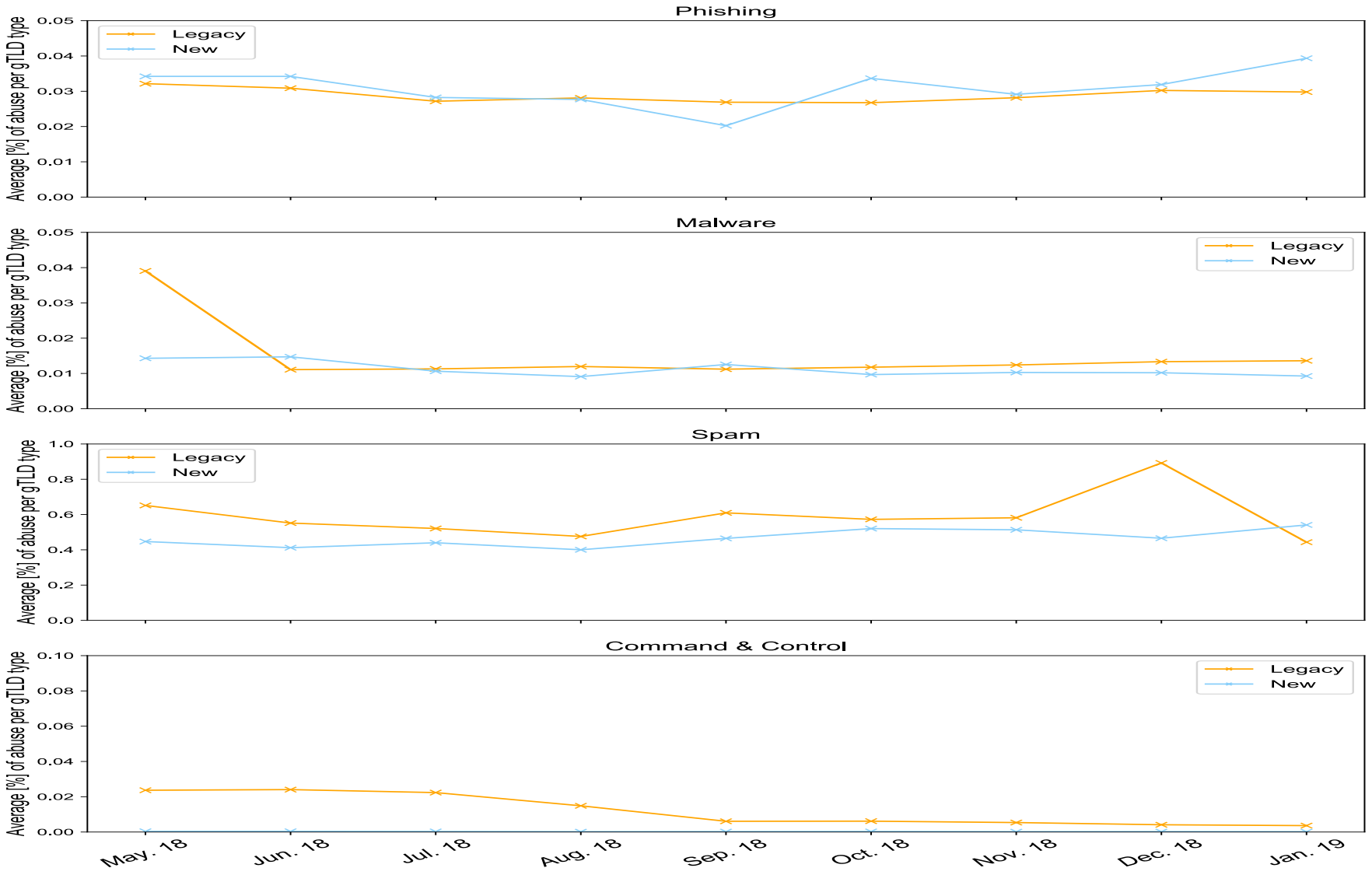


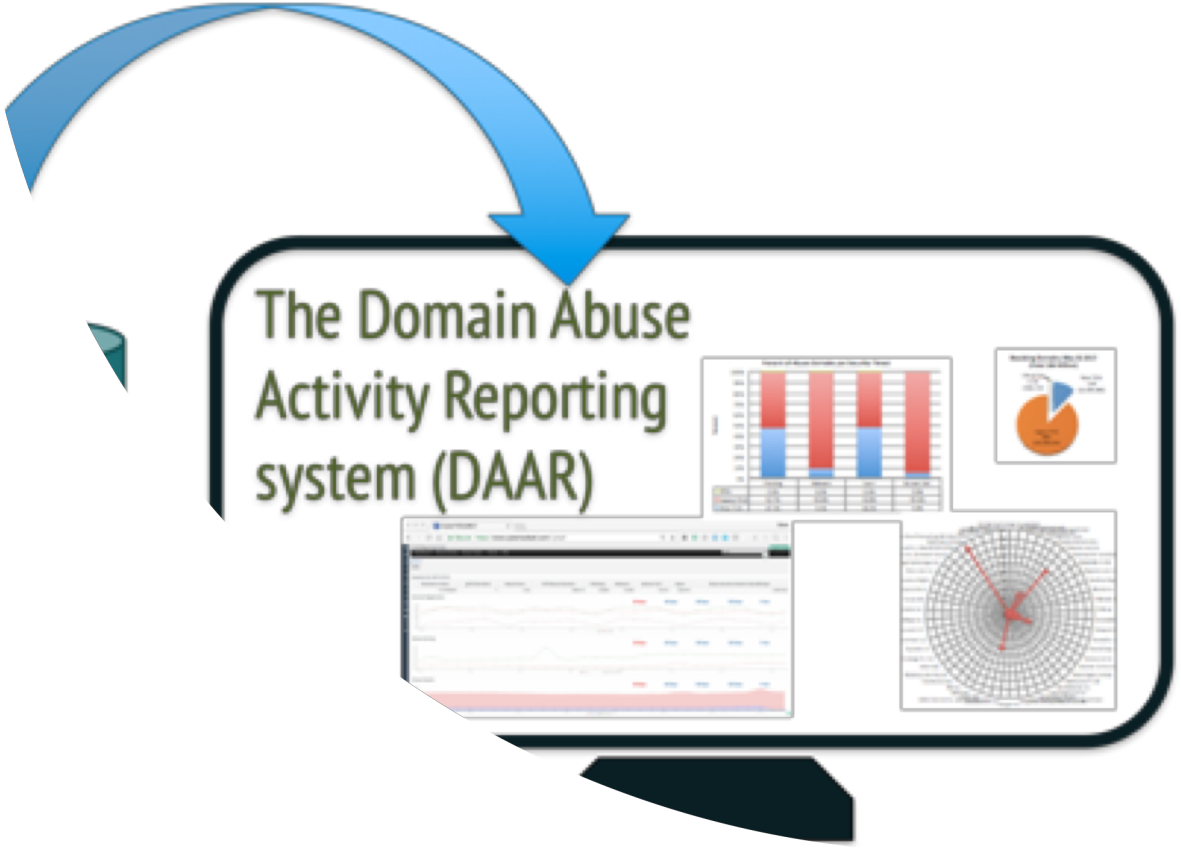




Abuse: raw counts vs normalized counts

Average Abuse Percentage per gTLD Across All Abuse Types





Project Status

The OCTO Security, Stability & Resiliency (SSR) team

- Put DAAR methodology for public review and input
- Reviewed all the reviews and comments received
- Published SSR responses to DAAR comments on February 1st, 2019

Project Status

- Published the first series of the DAAR monthly reports
  - ICANN published the first monthly report from the DAAR system for January 2019
  - Monthly reports from previous 2018 have made available as well

The data has already enabled constructive and data driven discussions with industry members

This is work in progress

We need your feedback!

We need to know what is most useful for you as the community

Project Next Steps

Methodology

- Improving the system based on comments and reviews
- Developing a process for systematically reviewing feeds
- Distinguishing between maliciously registered domains vs compromised

Data

- Adding more malware feeds
- Discussion about sharing data with registries who are interested in viewing their own data

\

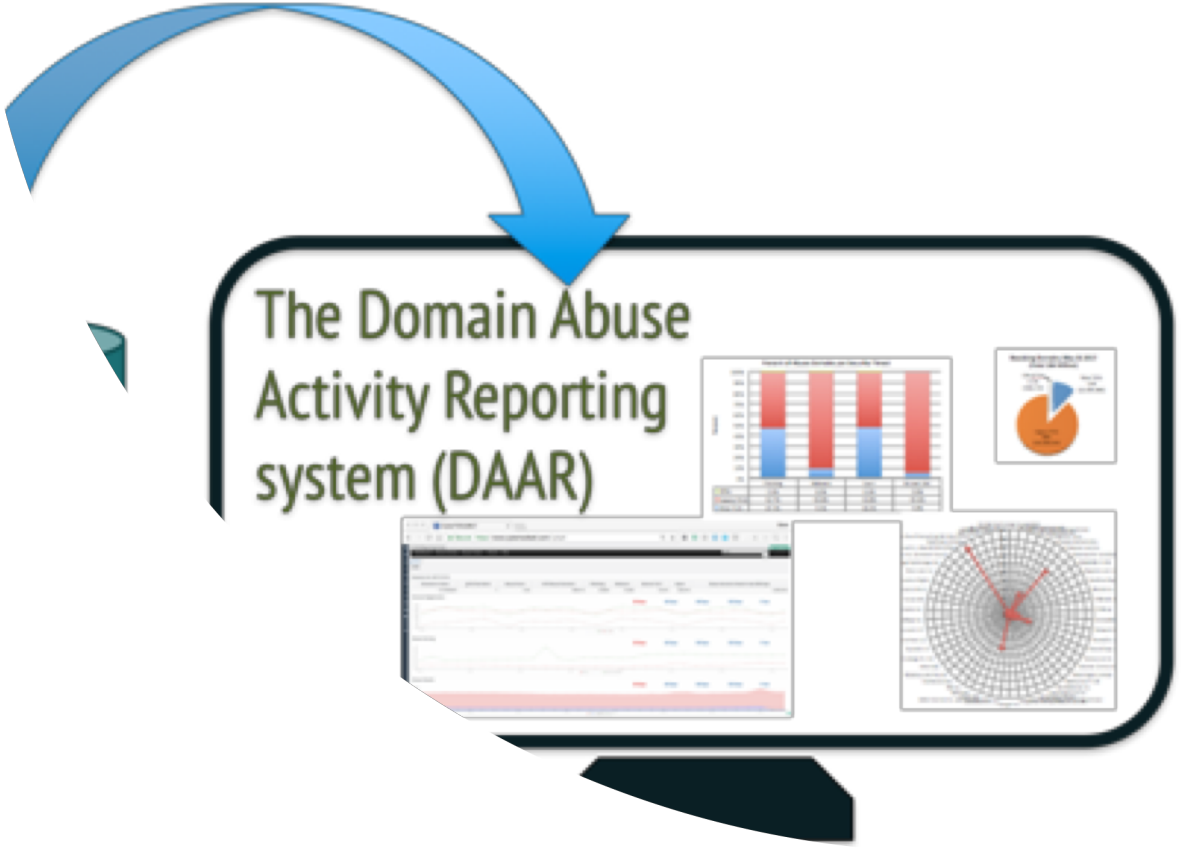
Results

- Developing new metrics and analytics based on DAAR (e.g., looking at other TLD related attributes in addition to legacy and new)?

Challenges Ahead

- Registrar level metrics?
  - WHOIS data collection is hard to scale
- ccTLD level metrics?
  - Lack global ccTLD zone file access
- Remediation metrics?
  - Require domain uptimes (takedown times), a lot more complicated measurements on RBLs that are collected from various sources

\



Where do We Want to Go from Here?

Measuring Abuse

- We are always open to discussion on improvements or other ways the data can be used to help inform discussions around DNS abuse.
- The channel to discuss your concerns is **DAAR@icann.org**
- If you are a ccTLD and would like to input zone files and use the DAAR data, please contact us

The project is aimed to be useful for the community, so step forward and discuss your needs and help improving it together

Discussions on DNS Abuse at IDS (May 10-11)

BANGKOK
10-11 MAY 2019

DNS-OARC
Domain Name System Operations Analysis and Research Center

12-13 May 2019

https://www.icann.org/ids

Questions?

Thank You

Contact Info:

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