WHAT IS DOMAIN ABUSE ACTIVITY REPORTING (DAAR)?

John Crain
Chief SSR Officer

23 Feb 2021

DAAR Project Goals

- DAAR **was designed to be** used to
  - Study histories of security threat or domain registration activity at gTLD level
  - Help operators understand or consider how to manage their reputations, their anti-abuse programs, or terms of service

- DAAR **was NOT designed to be** used to
  - Provide domain level data on security threat domains
  - Rank gTLD providers in terms of their security concentrations

Data Sources

1. DNS zone data
2. Open source or commercial abuse threat or reputation block list (RBL) data*

*Certain data feeds require a license or subscription

DNS Zone Data

- Uses Domain names in Zone files collected via publicly available methods Centralized Zone Data Service (CZDS)

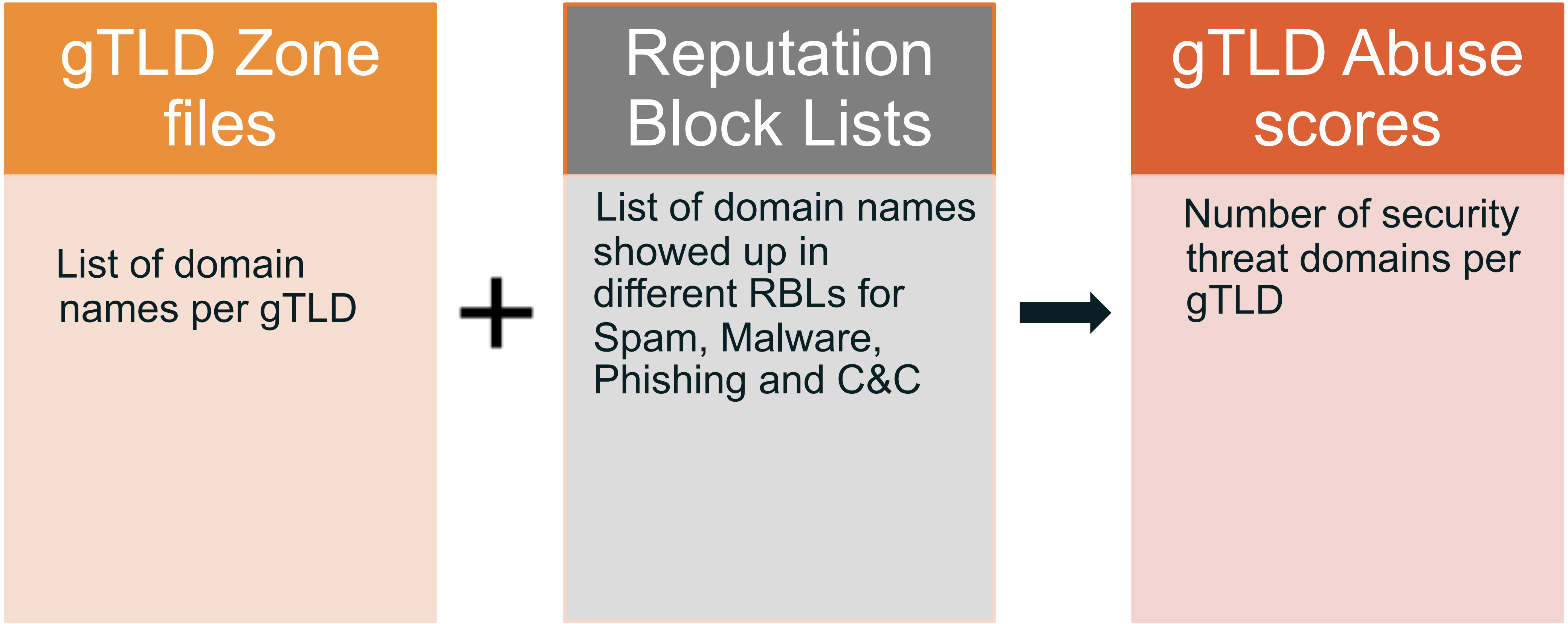
- Collects
    - Approximately 1220 gTLDs
    - Approximately 192 million domain names

Reputation Block Lists: Identifying Threats

DAAR collects domain data for:

- Phishing
- Malware
- Spam (Used to facilitate other threats)
- Botnet Command & Control

Domain Abuse Activity Reporting (DAAR)



gTLD Zone files

List of domain names per gTLD

+

Reputation Block Lists

List of domain names showed up in different RBLs for Spam, Malware, Phishing and C&C

→

gTLD Abuse scores

Number of security threat domains per gTLD

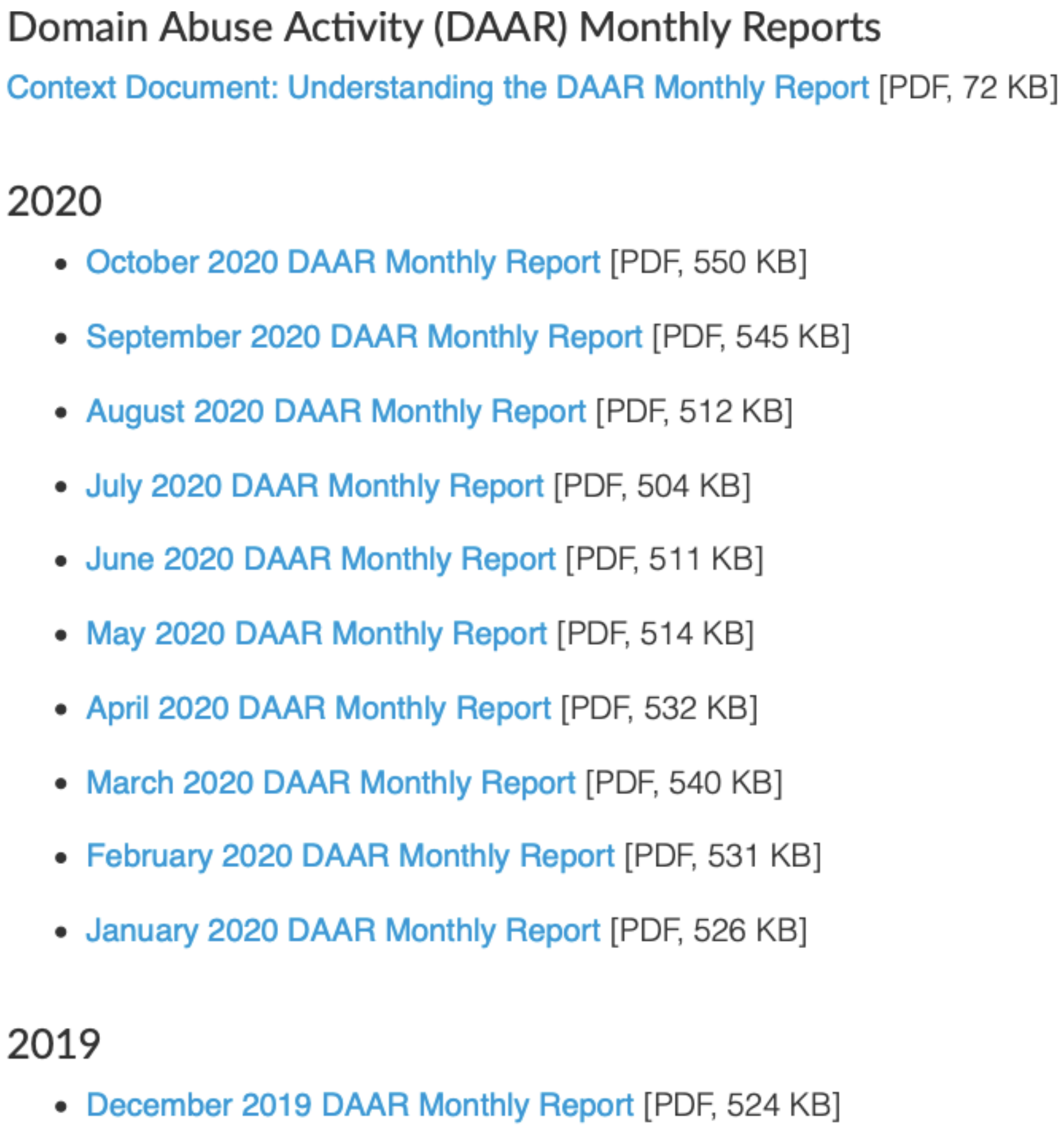
DAAR Analytics & Monthly Reports

Daily scores pushed to registries via MoSAPI

DAAR
Monthly Report

DAAR Monthly Report

- Created within the first week of every month and placed on the ICANN website:
  - https://www.icann.org/octo-ssr/daar
- Goes back to Jan. 2018
- Currently based on Last day of the month
- Contains **anonymous** and **aggregated** analytics based on the DAAR data sheet



Domain Abuse Activity (DAAR) Monthly Reports

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

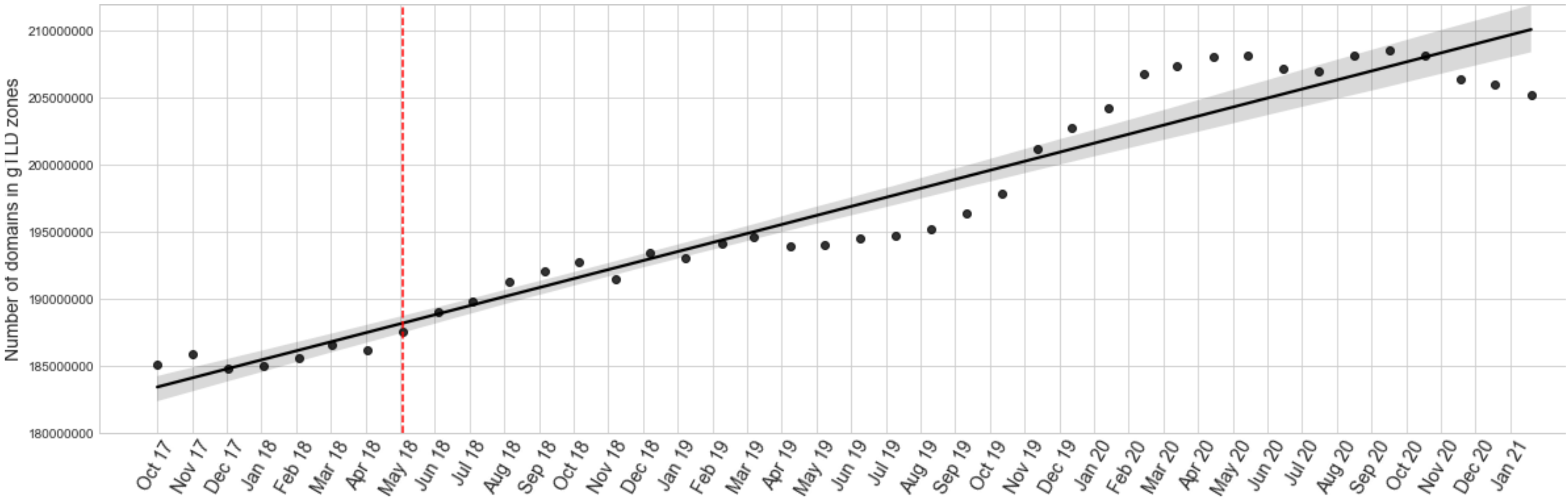
2020

- October 2020 DAAR Monthly Report [PDF, 550 KB]
- September 2020 DAAR Monthly Report [PDF, 545 KB]
- August 2020 DAAR Monthly Report [PDF, 512 KB]
- July 2020 DAAR Monthly Report [PDF, 504 KB]
- June 2020 DAAR Monthly Report [PDF, 511 KB]
- May 2020 DAAR Monthly Report [PDF, 514 KB]
- April 2020 DAAR Monthly Report [PDF, 532 KB]
- March 2020 DAAR Monthly Report [PDF, 540 KB]
- February 2020 DAAR Monthly Report [PDF, 531 KB]
- January 2020 DAAR Monthly Report [PDF, 526 KB]

2019

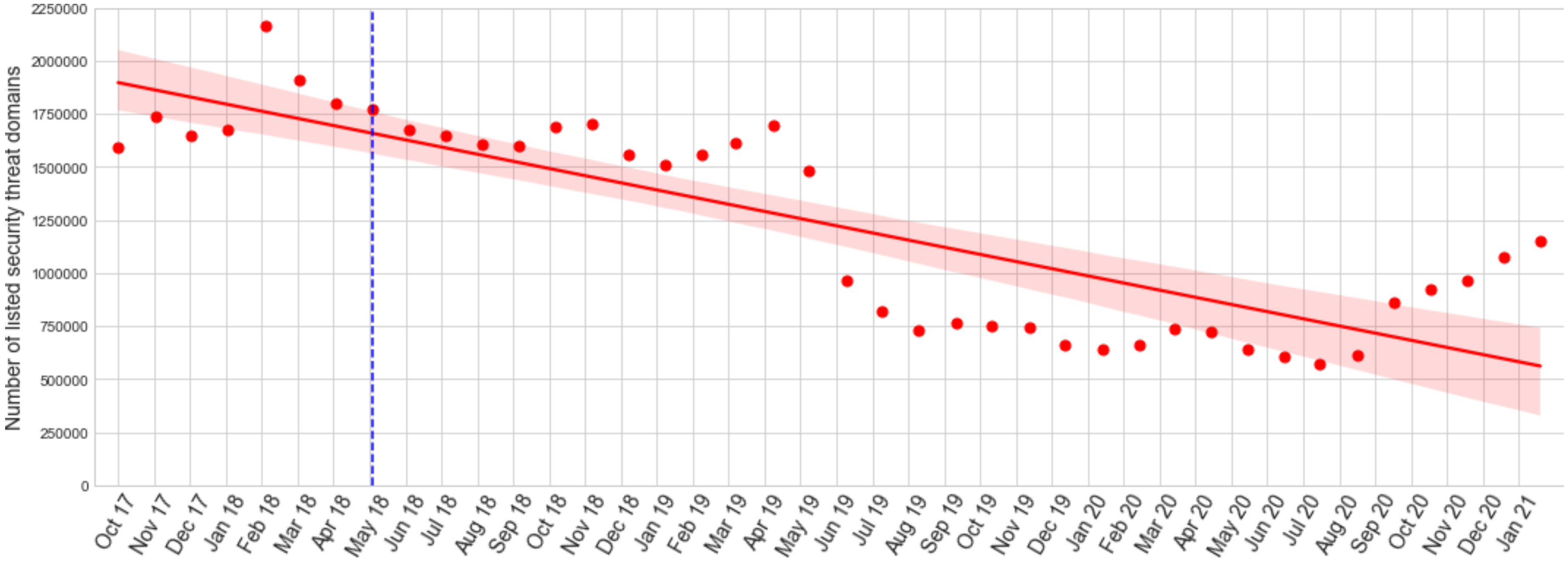
- December 2019 DAAR Monthly Report [PDF, 524 KB]

General trends in gTLDs

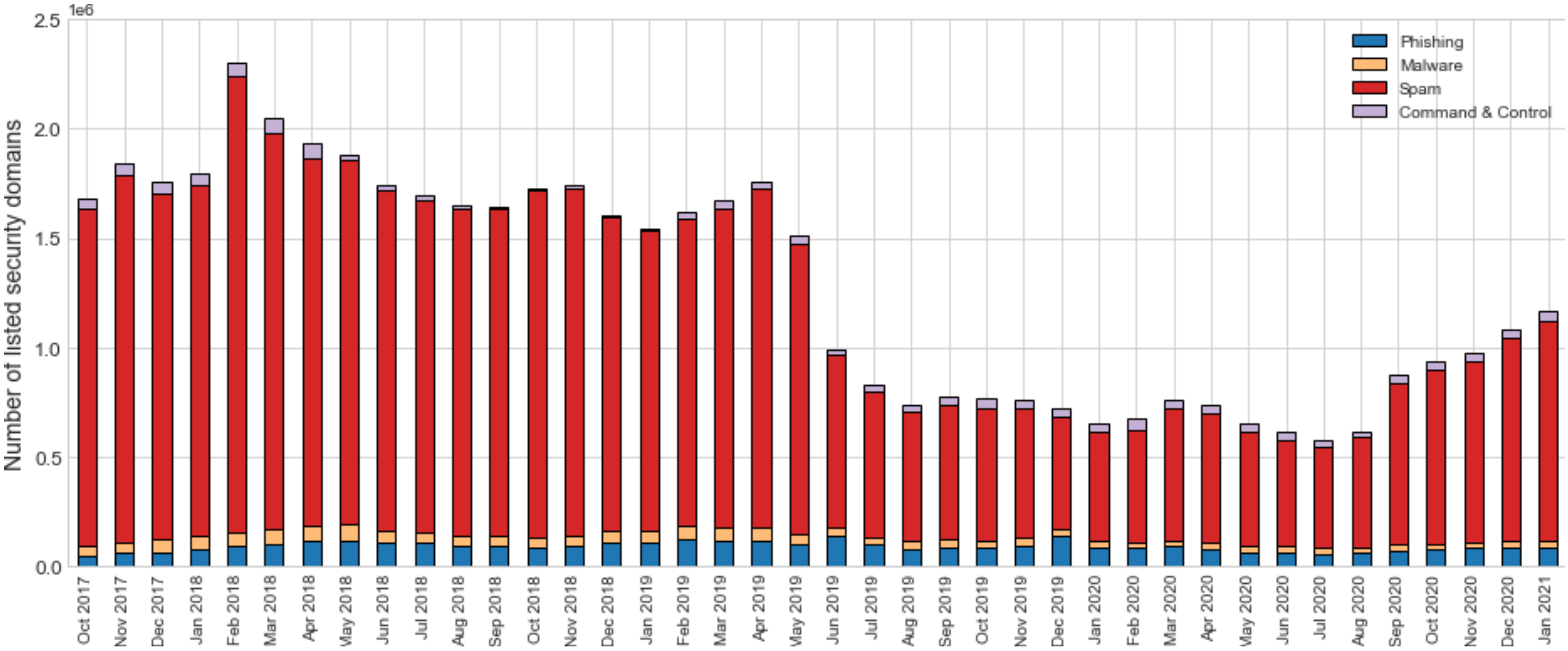


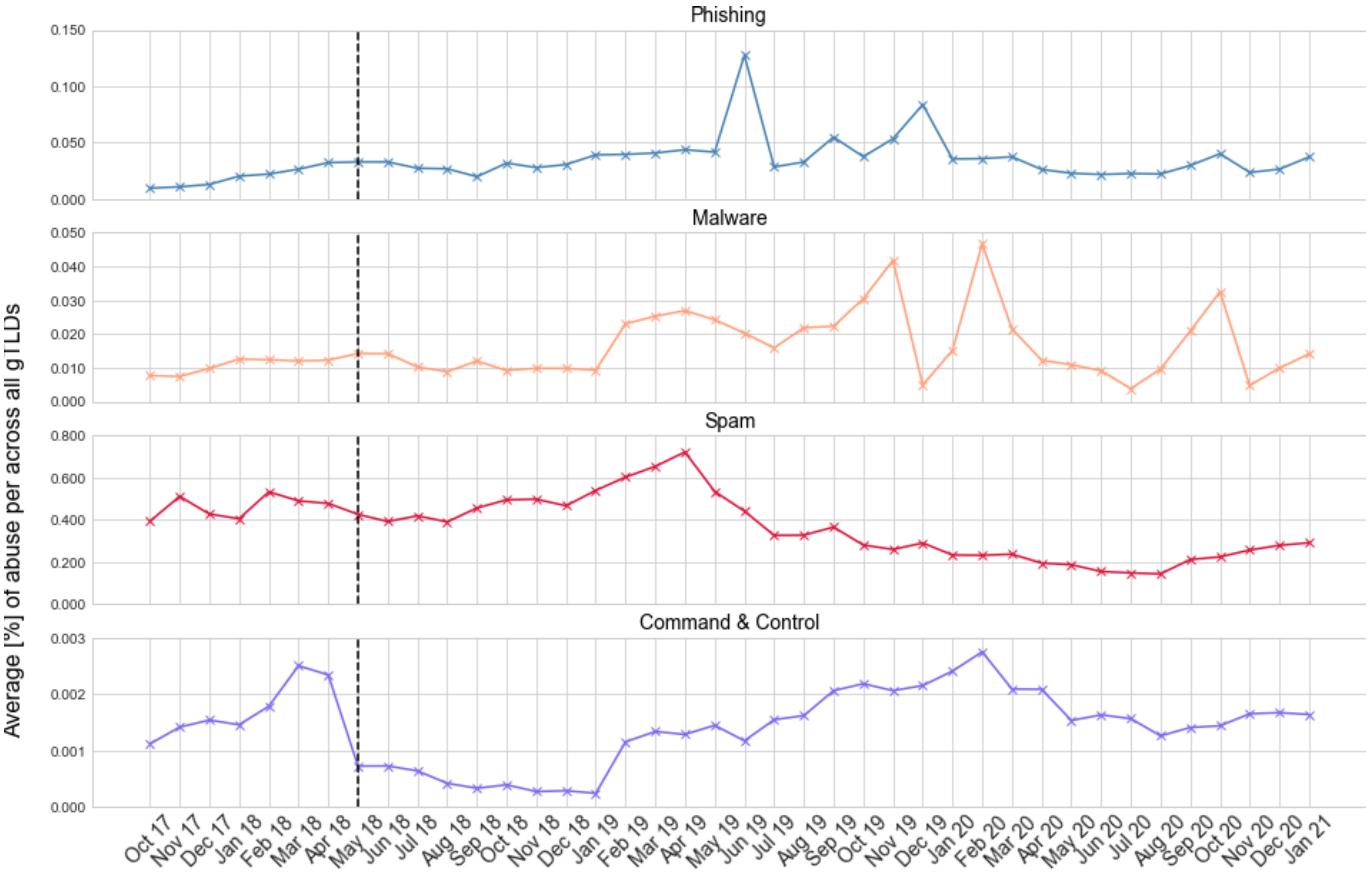
Domains in gTLD zones

Security threat domains in gTLDs



General trends in gTLDs




Phishing
0.150
0.100
0.050
0.000
Malware
0.050
0.040
0.030
0.020
0.010
0.000
Spam
0.800
0.600
0.400
0.200
0.000
Command & Control
0.003
0.002
0.001
0.000
Average [%] of abuse per across all gTLDs
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

CCTLDs in DAAR Since June 2020

13 ccTLDS are participating in DAAR now:

- .au
- .se
- .tw
- .cl
- .nu
- .ee
- .tz
- .gt
- .sv
- .mw
- .gg
- .je
- .ch

We provide them with:

- 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

Steps for a ccTLD to join DAAR

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

Plans Ahead

- Adding more ccTLDs
- Improving visuals and their precision
- Registrar level metrics
  - WHOIS data collection is hard to scale
  - Possible solution: daily WHOIS queries only for blacklisted domains or a random sample of domains

DAAR Contact

DAAR@icann.org