DNS abuse mitigation in the gTLD context

Dr. Siôn Lloyd
Lead Security, Stability & Resiliency Specialist
ICANN Office of CTO

Evening Workshop
2nd March 2023

Domain Abuse Activity Reporting (DAAR)

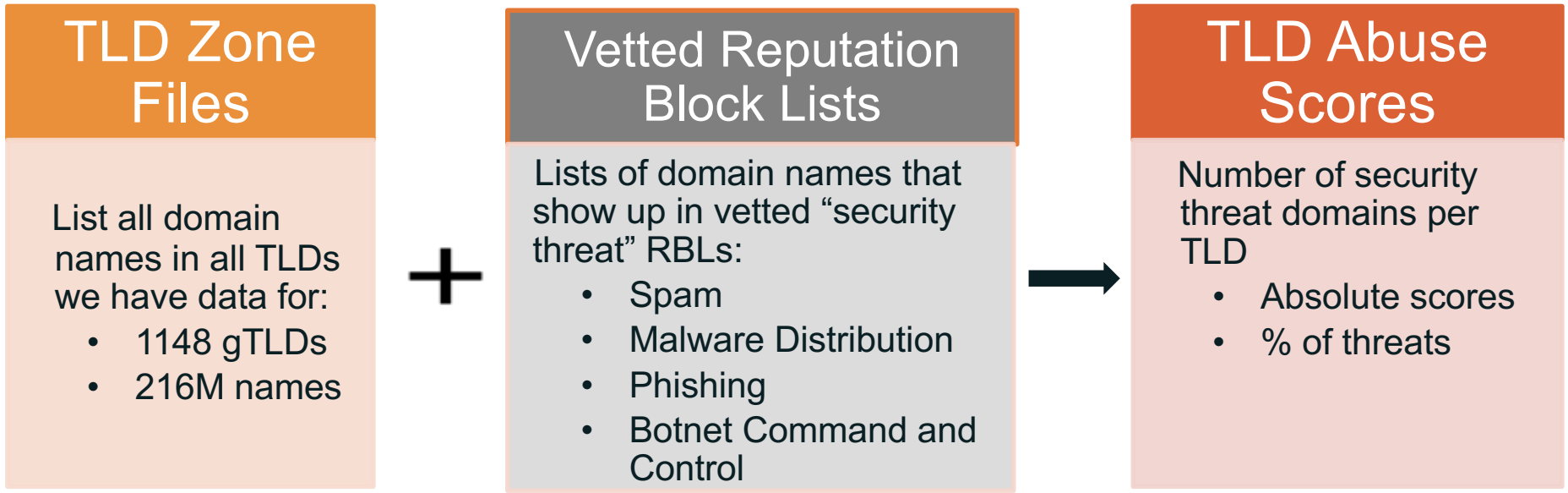
DAAR Project

- A system to study and report on security threats across top-level domains
- Be a robust, reliable, and reproducible methodology for data collection that can then be used by the ICANN community to facilitate informed policy decisions.

Full details can be found at:

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

DAAR Methodology



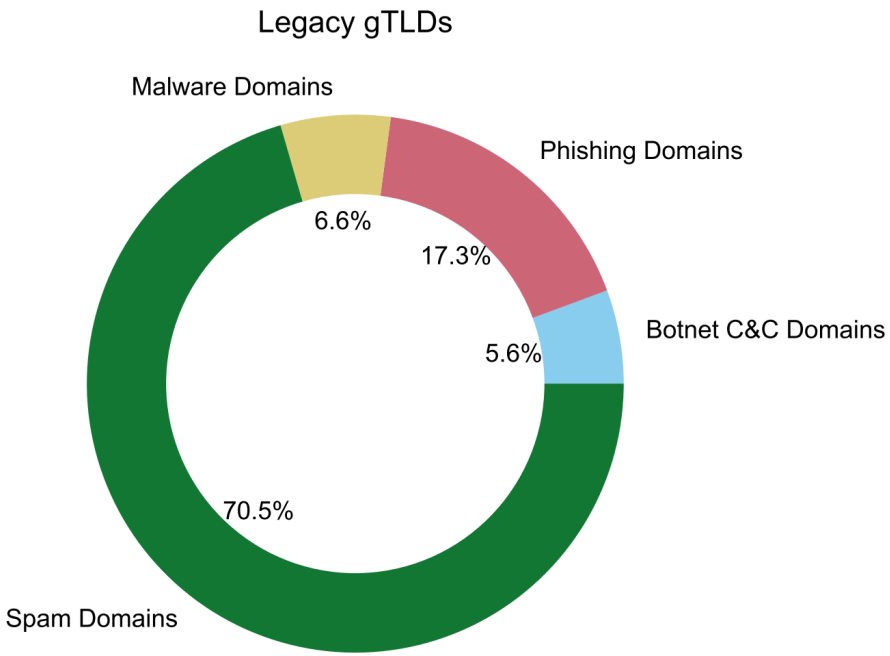
- Monthly reports (from Jan 2018) published at https://www.icann.org/octo-ssr/daar
- Daily scores made available to TLDs via the Monitoring System API (MoSAPI)
  - Allows comparison to monthly statistics

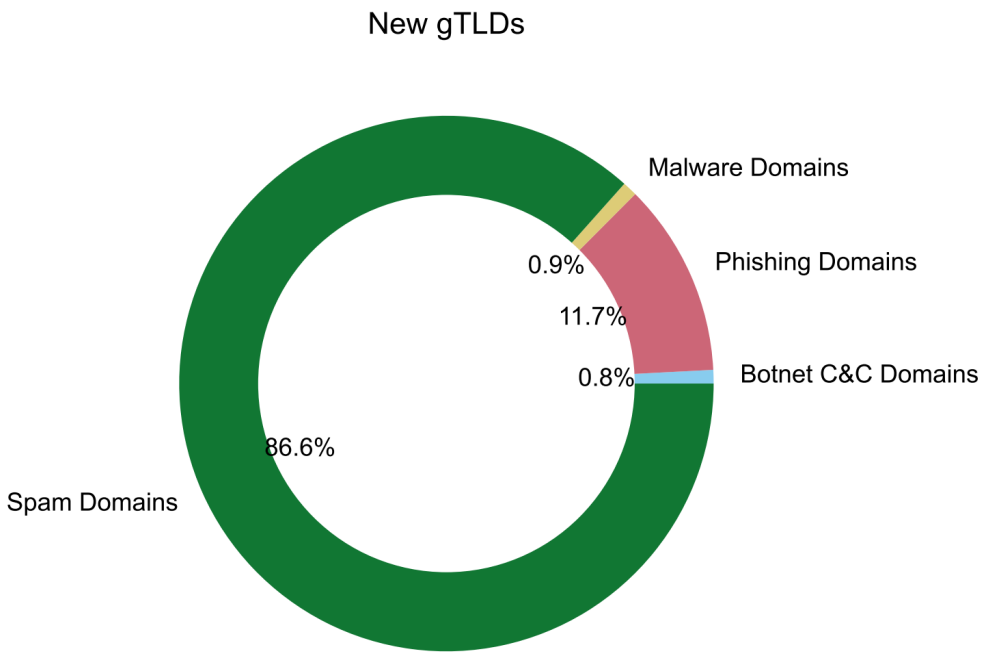
DAAR Project Uses, and Limitations

- DAAR data **CAN** be used to
  - Report on threat activity at TLD 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 Monthly Report

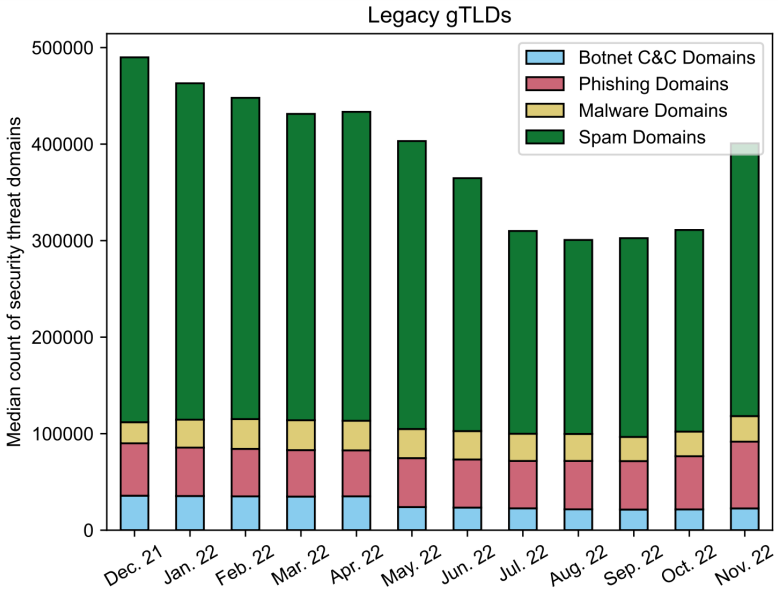
Overview

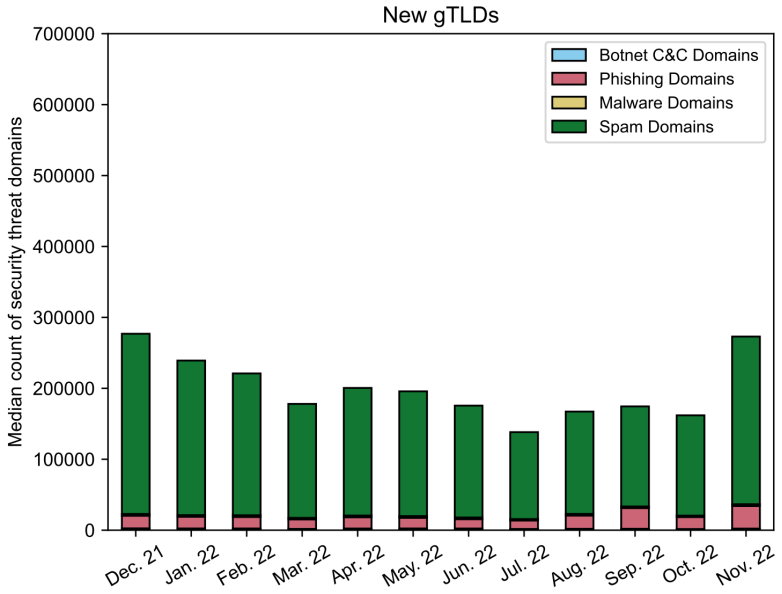


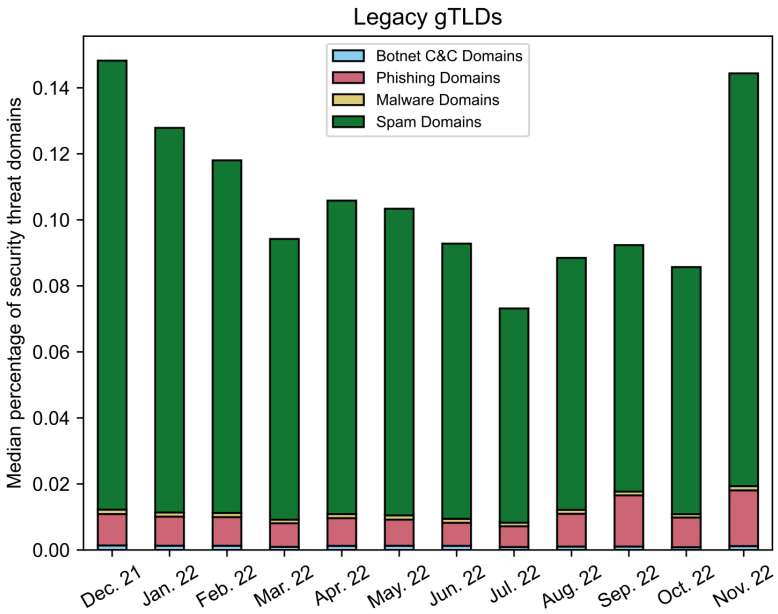


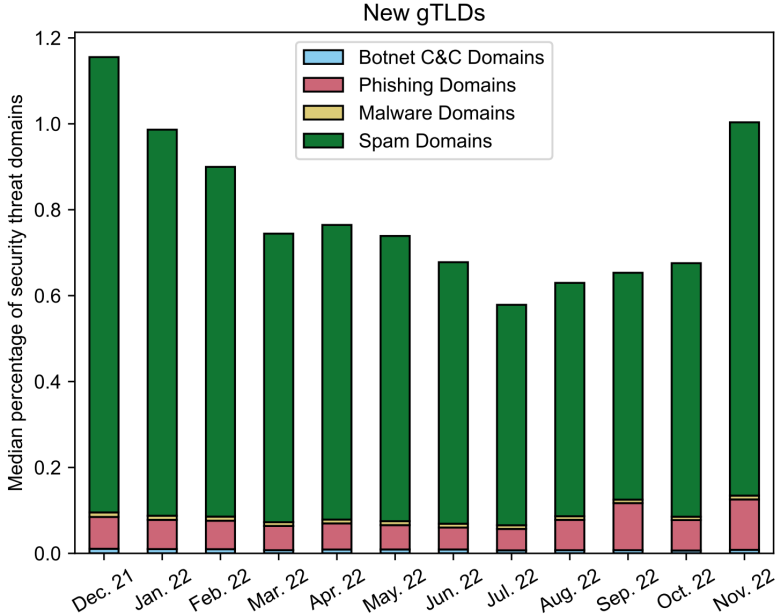
(Legacy gTLDs are those delegated pre-2010)

12-month trends

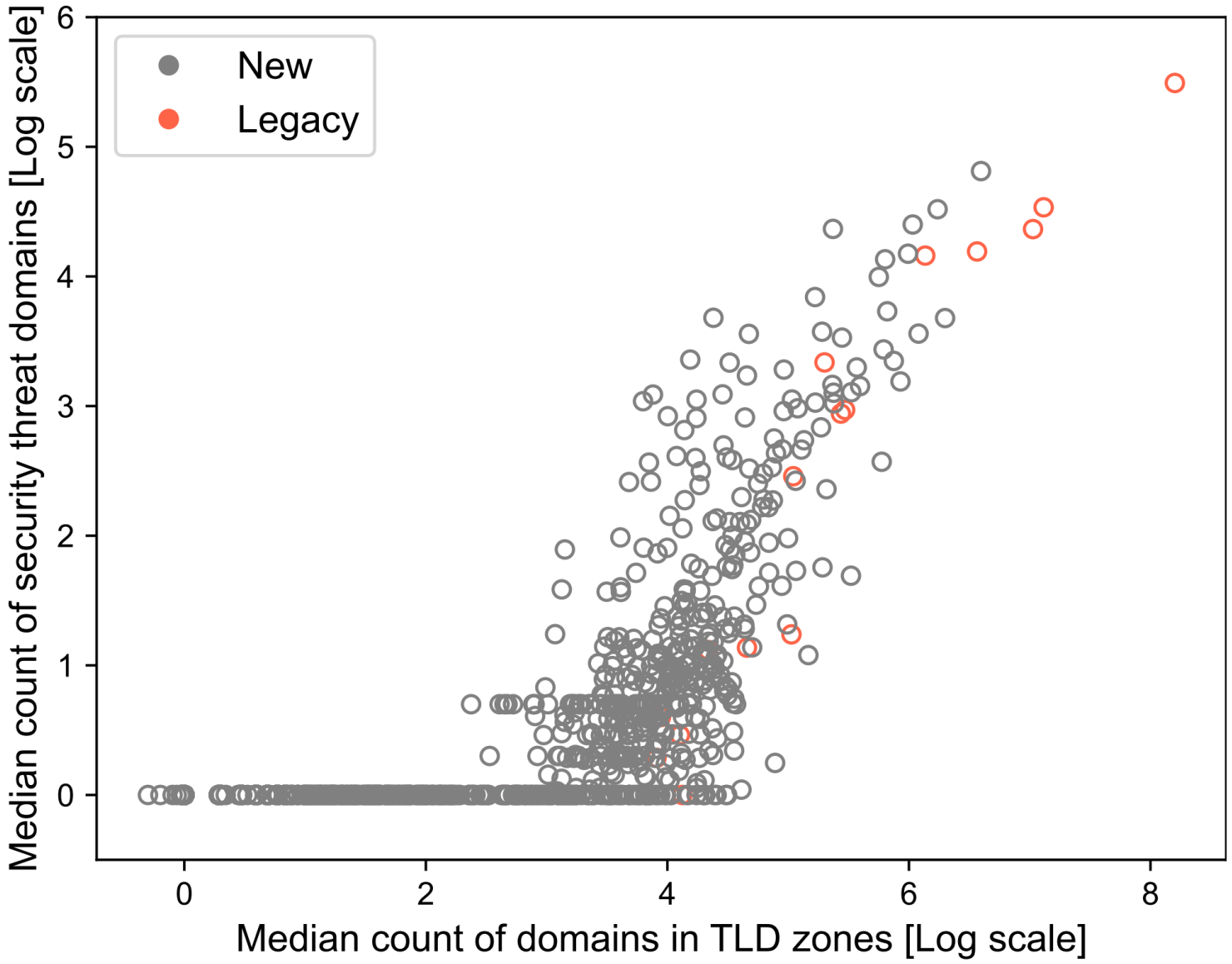






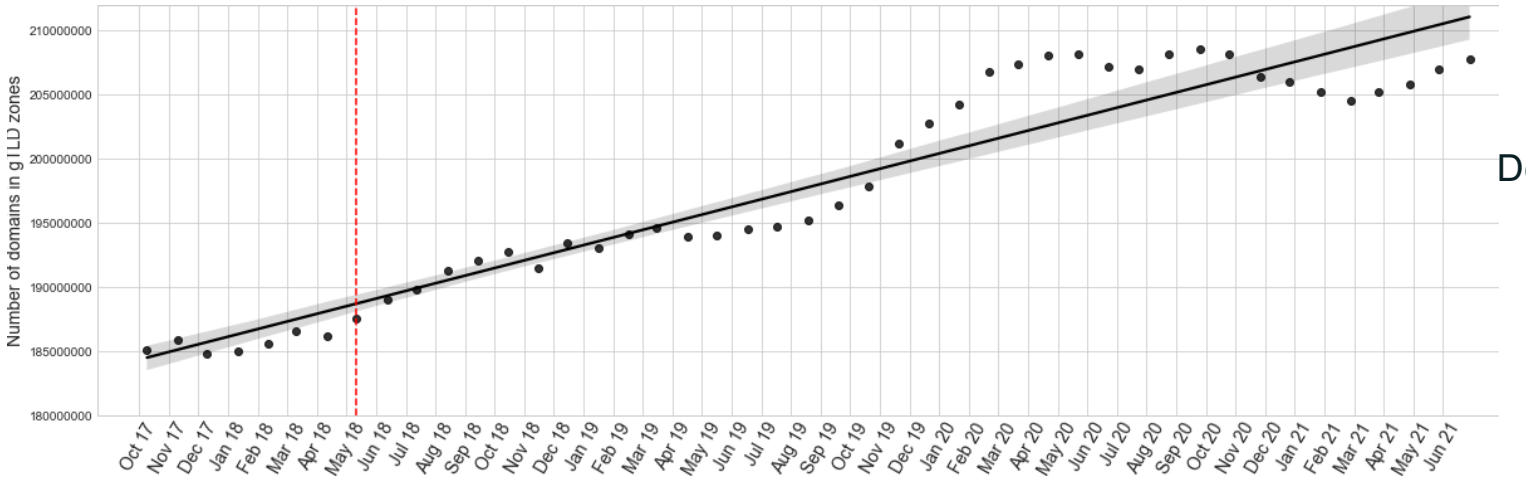


Per TLD


New
Legacy
Median count of security threat domains [Log scale]
Median count of domains in TLD zones [Log scale]
0
1
2
3
4
5
6
0
2
4
6
8

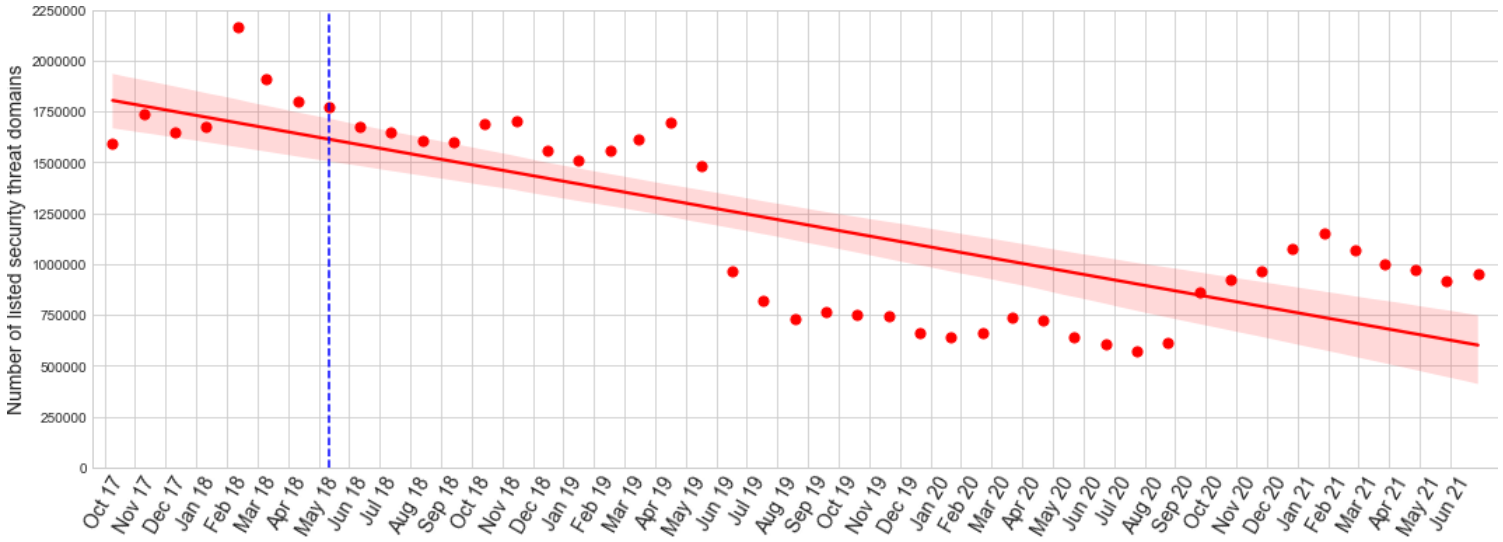
DAAR Longer term trends

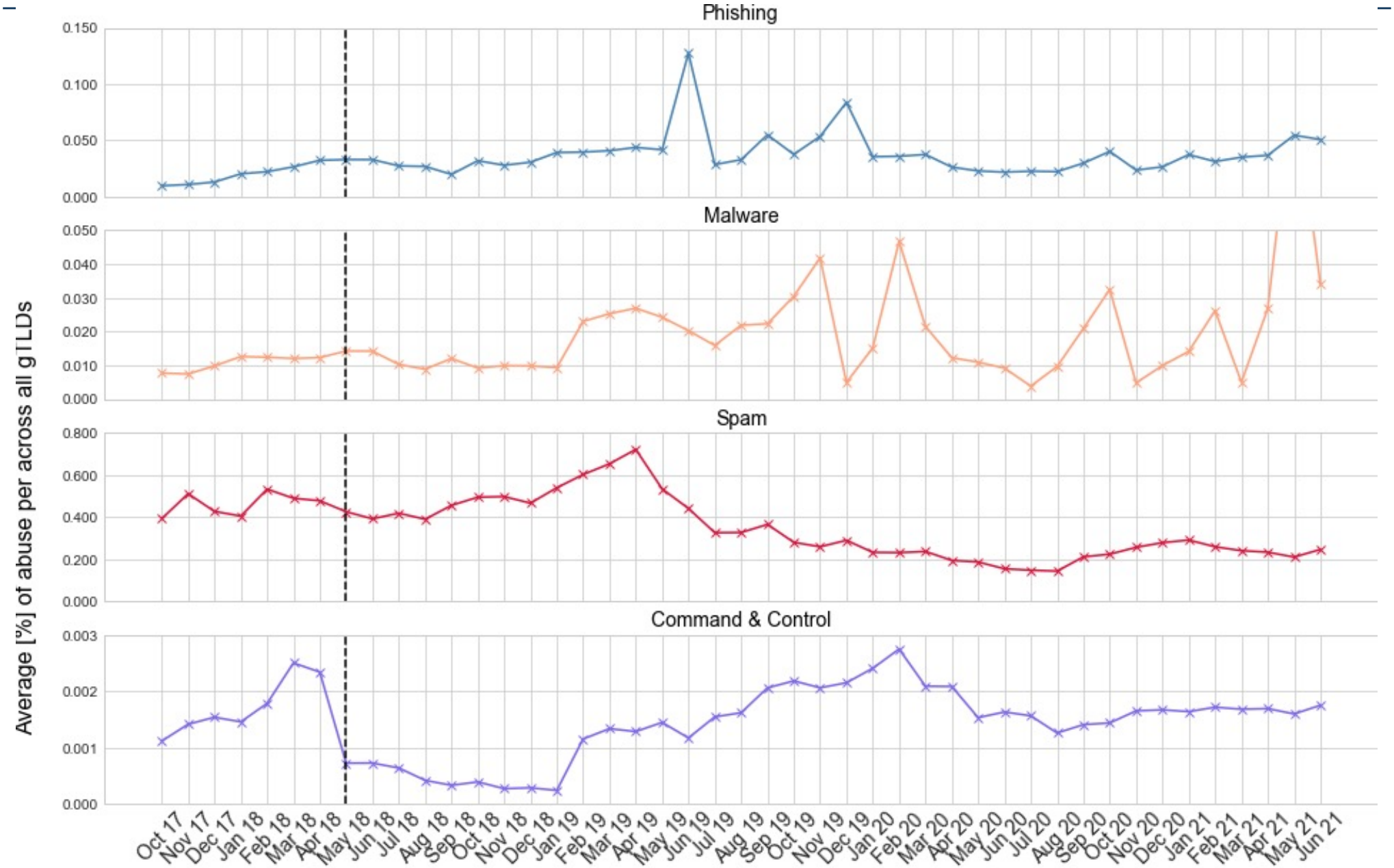
General trends in gTLDs



Domains in gTLD zones

Security threat domains in gTLDs




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

ccTLDs

ccTLDs in DAAR

21 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)
- .in (India)
- .ca (Canada)
- .li (Liechtenstein)
- .co (Colombia)
- .fo (Faroe)
- .fr (France)
- .pt (Portugal)

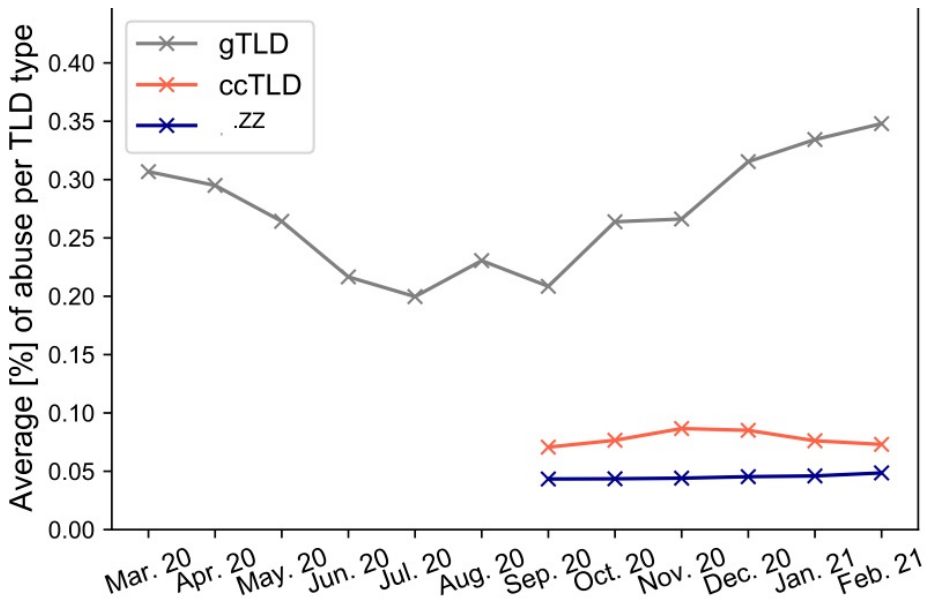
We provide:

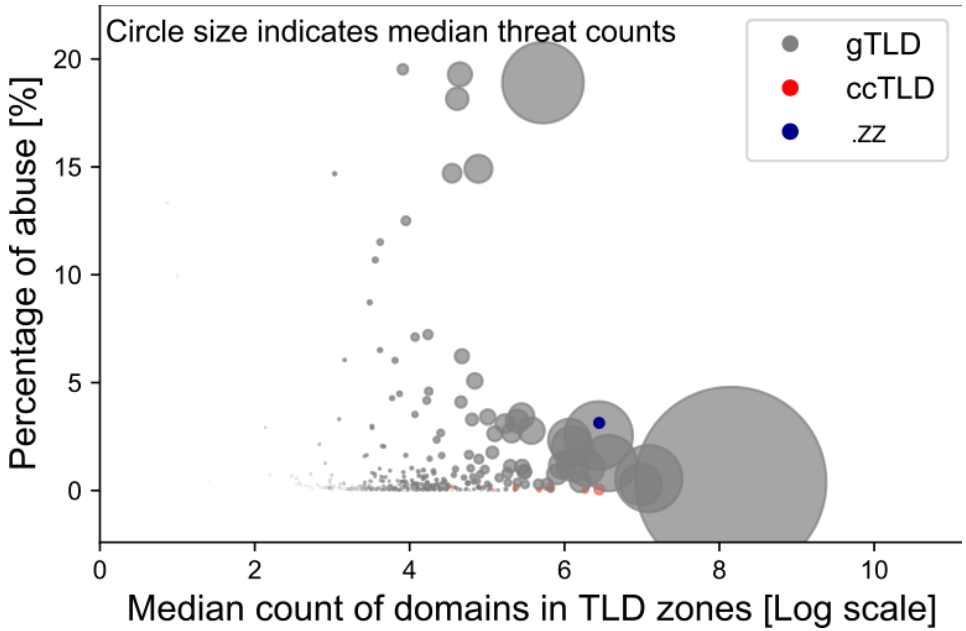
- Daily DAAR stats
- **Individualized** DAAR monthly reports

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





Future Plans

- Adding more ccTLDs
- Provide individualized reports to all DAAR participants
- Publish methodology for RBL evaluations
- DAAR Evolution
  - Provide domain level sharable RBL data
  - Registrar level metrics
  - Uptime (Security Threat Persistence Metrics)
  - Malicious vs. Compromised
  - Security Threat Prediction
  - Dynamic Dashboard
  - API
  - Others …

Domain Name Security Threat Information Collection and Reporting (DNSTICR)

Identification and Reporting of pandemic-related malicious domain names

DNSTICR

(Spoiler alert!)

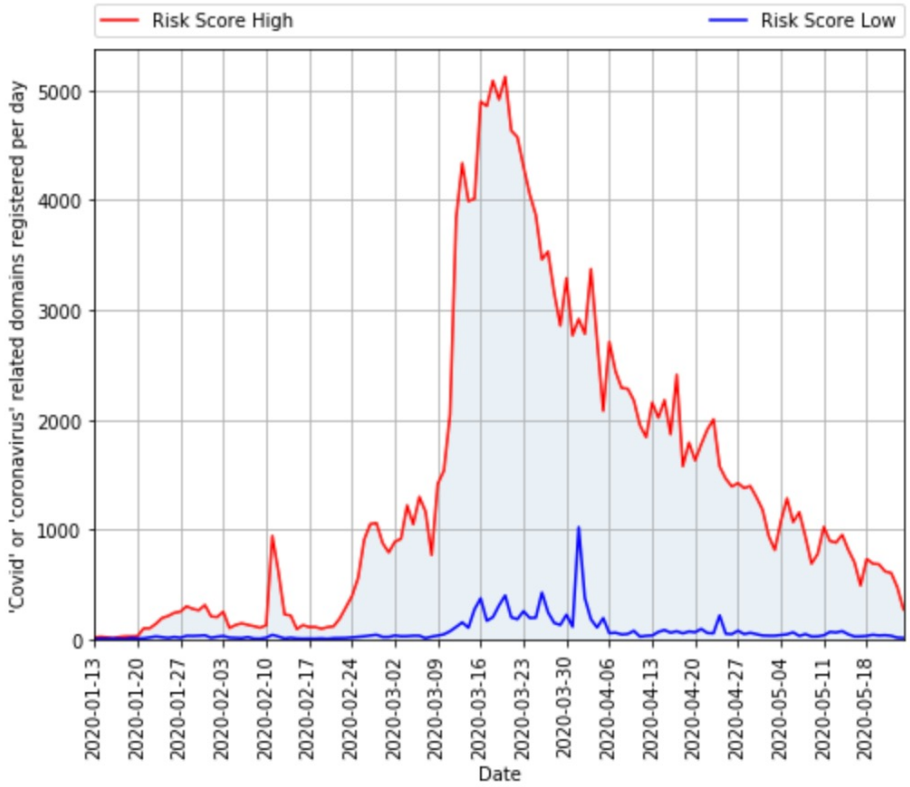
- Criminals use the internet
- Criminals use big events to “hook” victims
- Global event + Internet = Mass audience

- Big events have associated bursts of domain name registration
- COVID-19 no different
  - The extra working from home made it the perfect storm

Context

TLP: White

Domain trends update



(Source: John Conwell, DomainTools)

DNSTICR

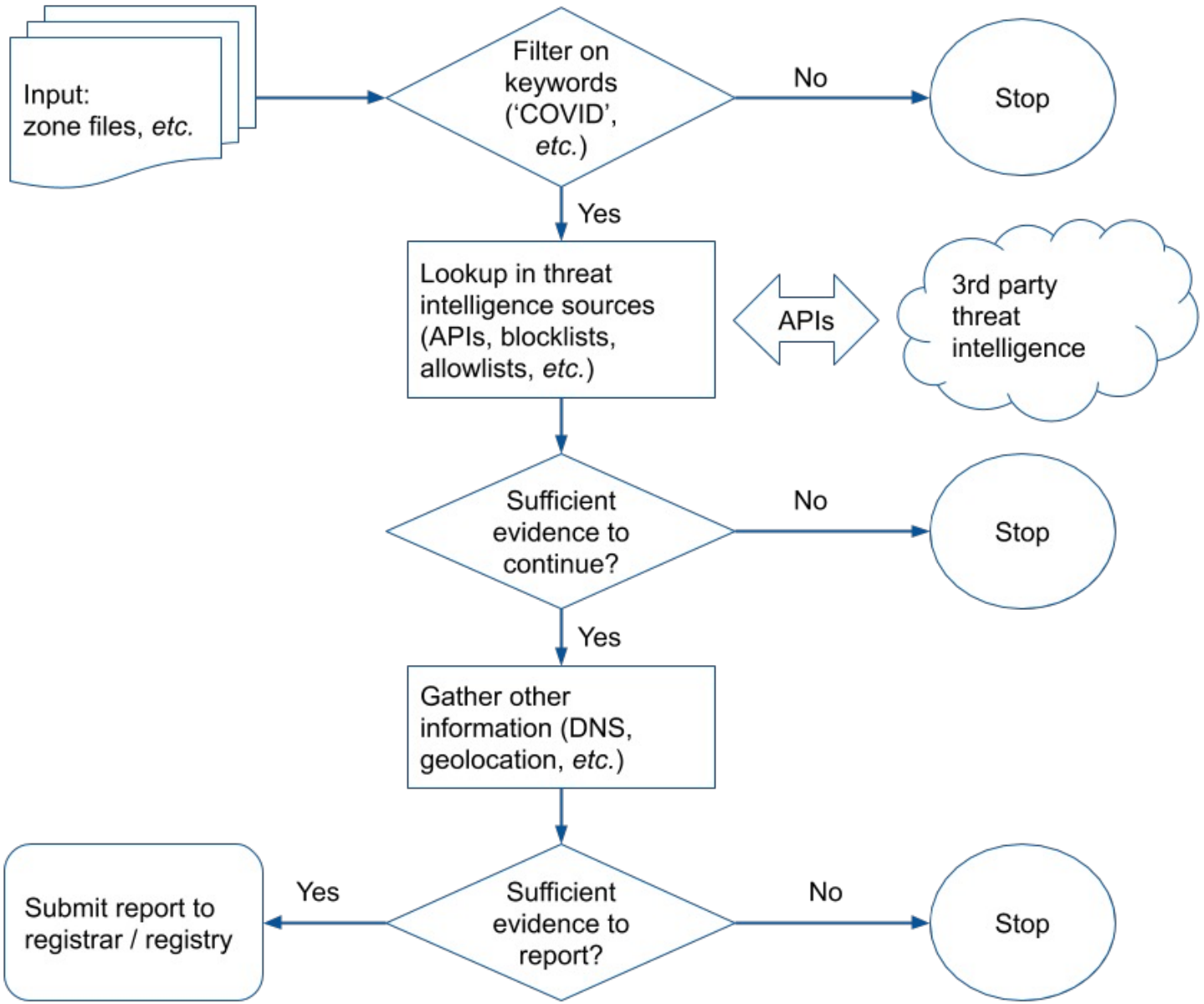
- Many articles talked about “suspicious” or “potentially malicious” registrations
- Some looked at full URLs, some at domains, some at certificates…

- Wanted a clear, published methodology
- Get good intelligence to the right people

- April 2022 – added terms related to conflict in Ukraine

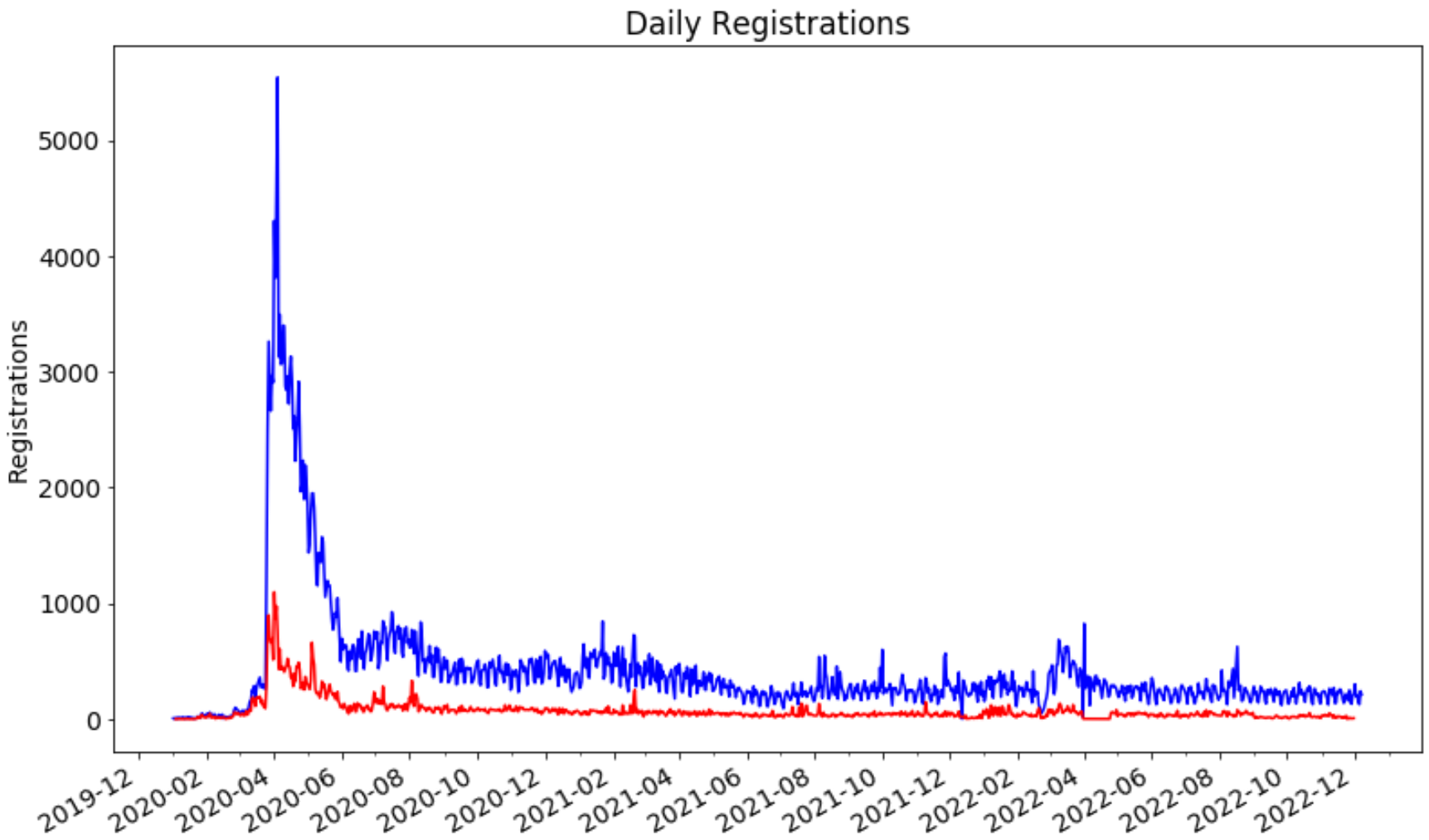
Methodology

DNSTICR - Data to Intelligence



Results

Full Picture

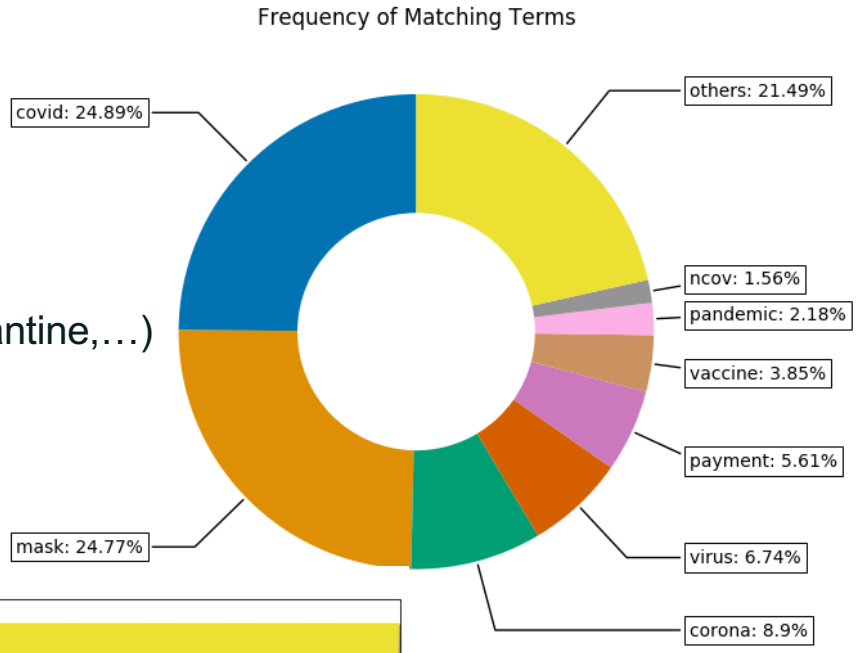


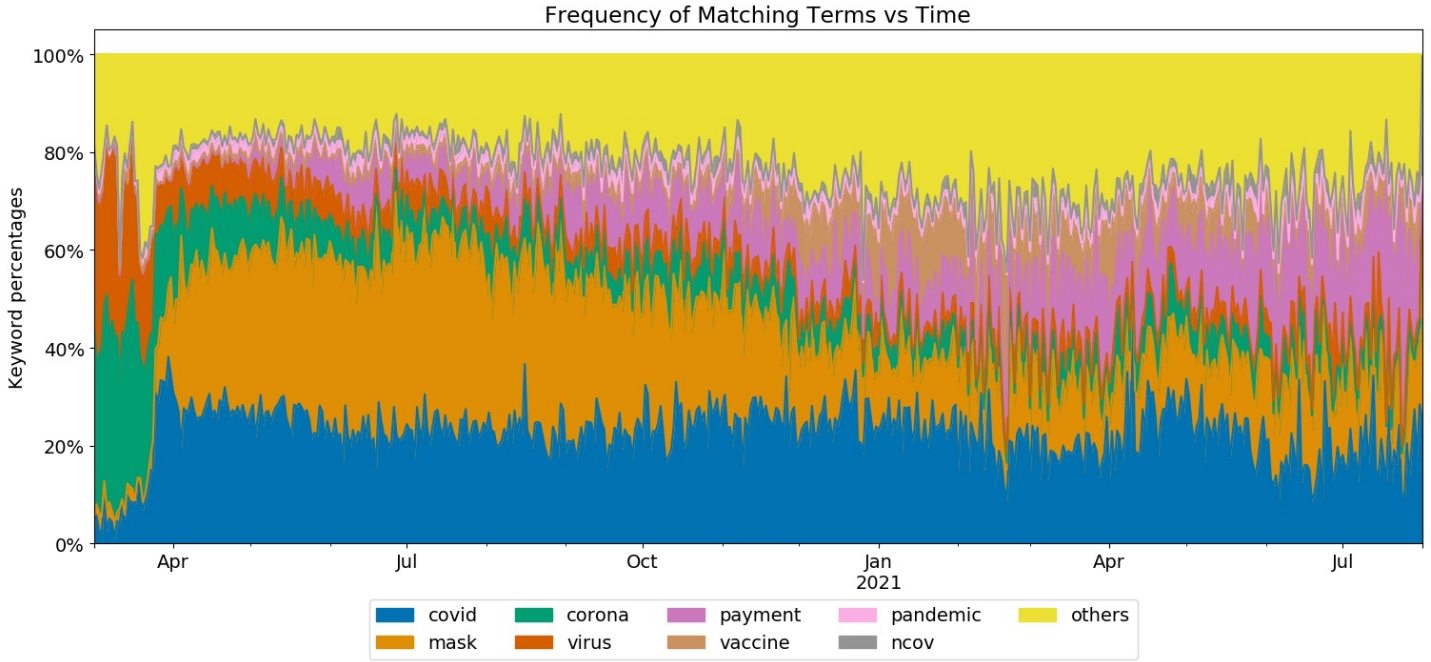
Registrations per day matching one or more of our filter terms (blue line) plus those which had one or more third-party reports (red line). Dates in DD-MM-YYYY format.

What keywords do these domains contain?

In the first 18 months:

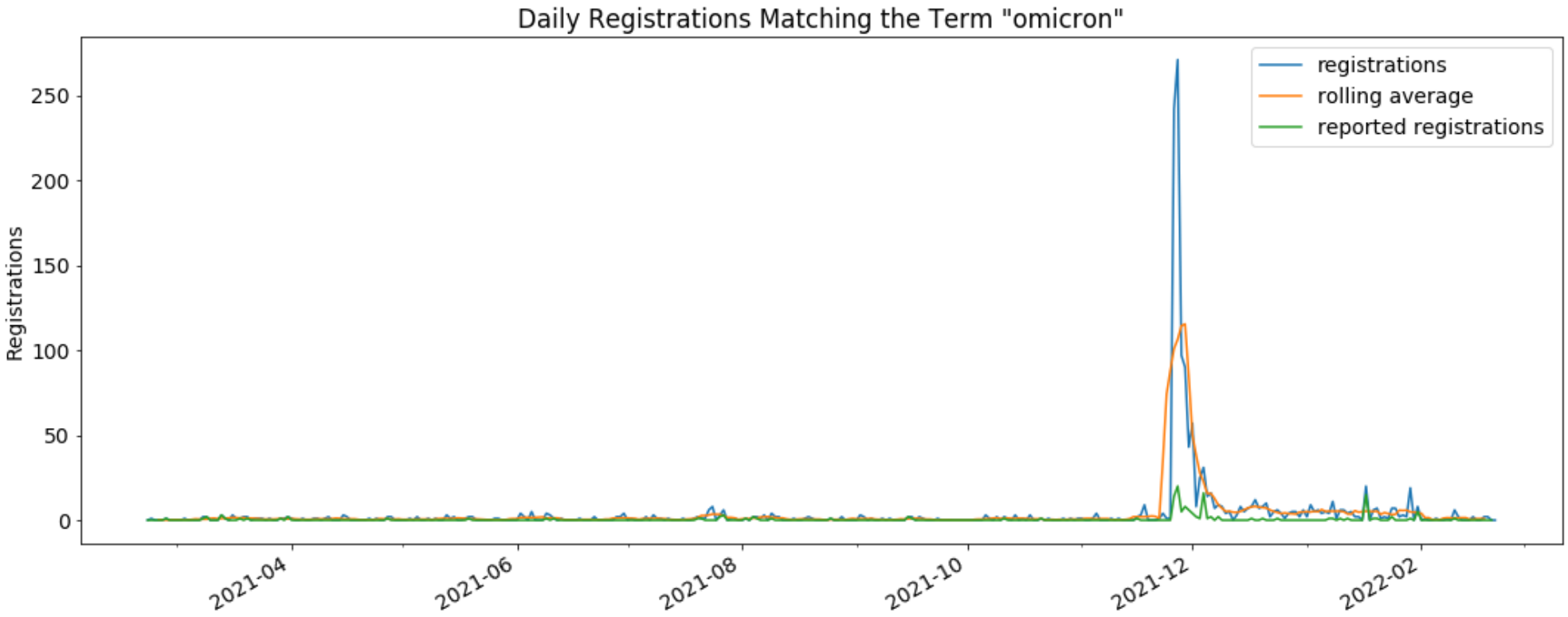
- Top four keywords account for 2/3 of the domains
- Different keywords categories:
  - Disease name (covid, ncov, sars, …)
  - Pandemic countermeasures (mask, lockdown, quarantine,…)
  - Collateral (zoom, webex, conference, …)
- Significant number of domains match non-English terms





New search terms

- New terms added, *e.g.*
  - Passport
  - Immunity
  - Omicron



Statistics

- 2020 – December 2022
  - 579 Search terms
  - 489,169 matched one or more search term
  - 28,411 (5.8%) had third-party reports
- Many matching terms but not covid related
  - “mask” matches “metamask” (crypto wallet) phishing/fraud
  - “payment” matches financial phishing/fraud
- Seeing lots of similar-looking registrations being reported but we see only parked pages

Thank You and Questions

Visit us at **icann.org**

sion.lloyd@icann.org


@icann


linkedin/company/icann


facebook.com/icannorg


slideshare/icannpresentations


youtube.com/icannnews


soundcloud/icann


flickr.com/icann


instagram.com/icannorg