Domain Name Security Threat Identification, Collection and Reporting (DNSTICR)

Siôn Lloyd
ICANN SSR

At-Large Consolidated Policy Working Group

11th May 2022

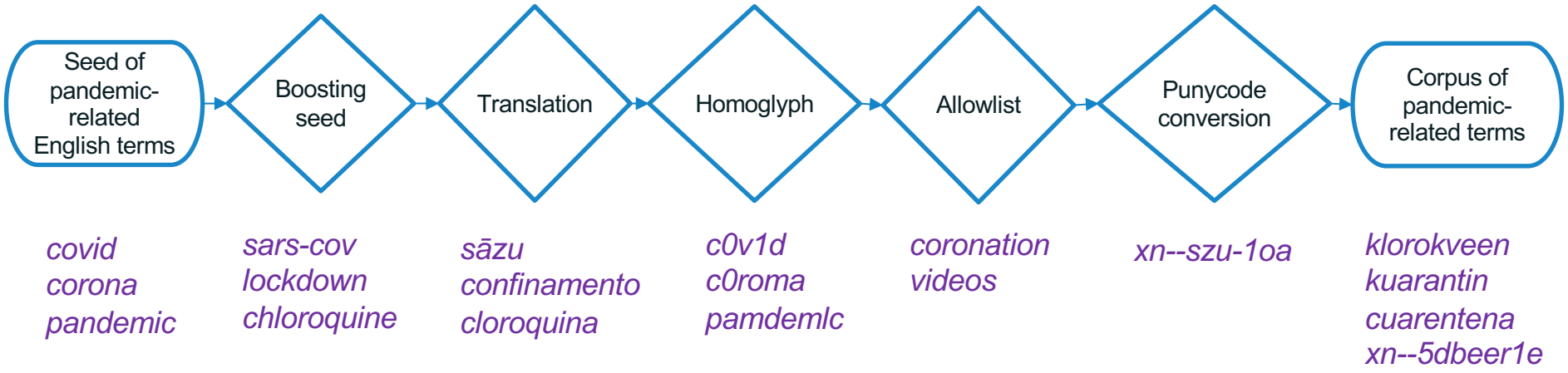
DNSTICR - Context

- Big events have associated bursts of domain name registrations
- COVID-19 no different
  - The extra working from home makes it the perfect storm
- Reports of increased malicious (suspicious?) registrations

- Get good intelligence to the right people

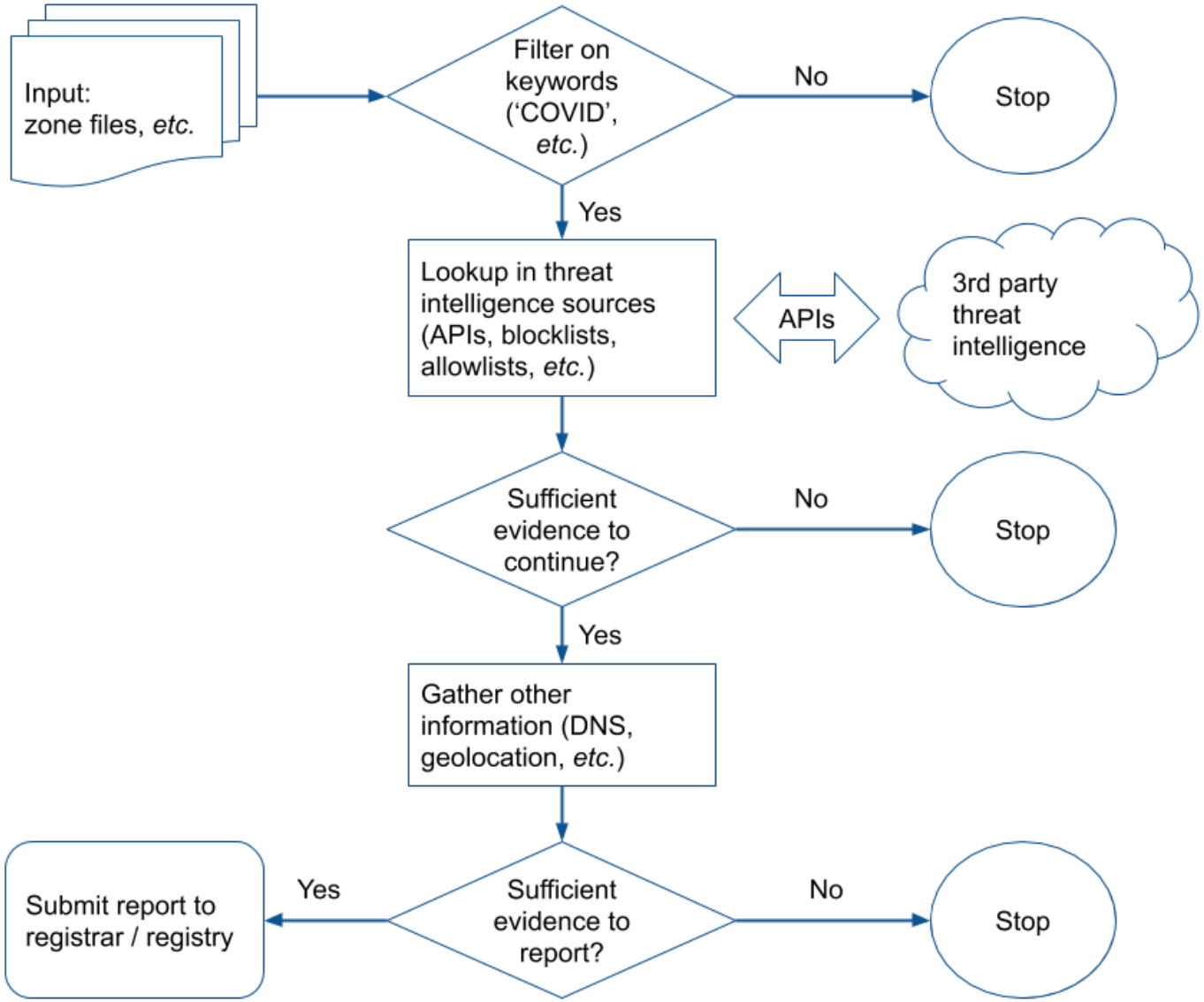
DNSTICR - Identification

- Our approach for identification:
  - Pandemic-related keyword search within zone files (mostly gTLDs)



- The output is **data**, not **intelligence**

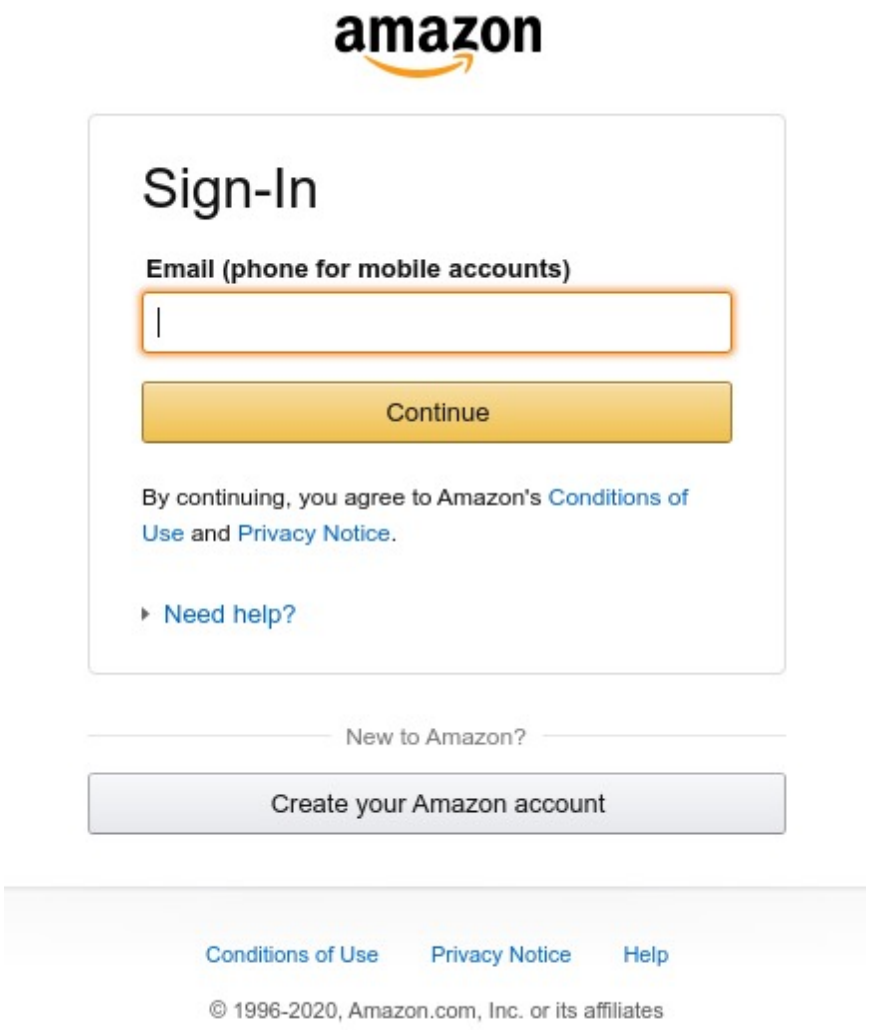
DNSTICR - Data to Intelligence



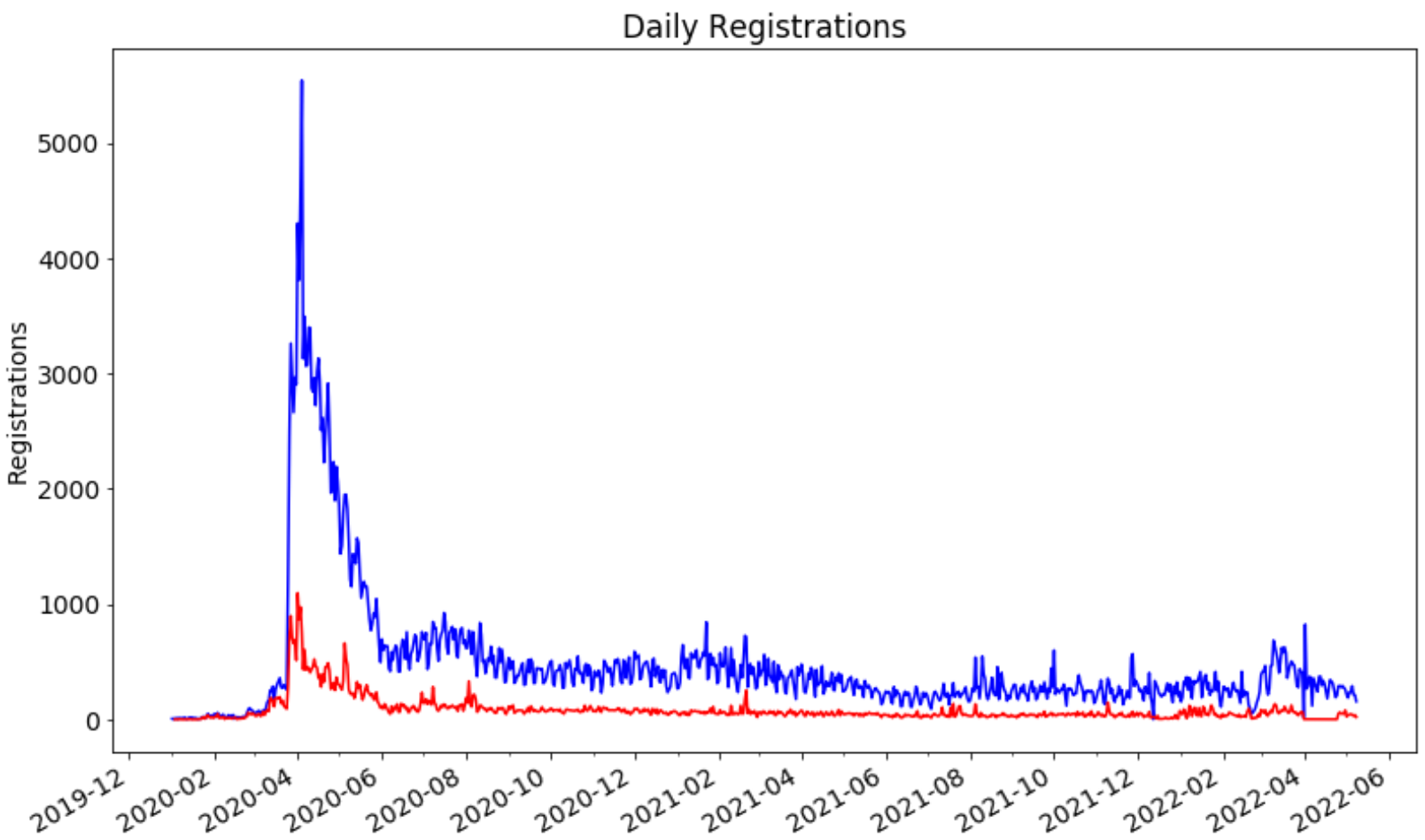
DNSTICR - Reporting

```
## Nature of the Activity ##

This domain is trading on the current COVID-19 outbreak in order to get traffic.
It has been detected to be delivering malware.
It has been detected to be involved with phishing.

## Details ##

### Virus Total URLs ###

Scan date: 2020-07-22 12:28:24
Malicious reports for:
hXXp://h                                  e[[.]]com/

        (see: hXXps://www.virustotal[.]com/gui/domain/h                                  e.com/relations)

### Domain not seen on AlienVault OTX ###

Checked at 2020-07-24

### PhishTank Reports ###

hXXps://h                                  e[[.]]com/
Verified on 2020-07-21 14:27:20
        (See: http://www.phishtank.com/phish_detail.php?phish_id=          )

### Domain reported on Google Safe Browsing ###

Threat type reported:   SOCIAL_ENGINEERING
Platform type reported: ANY_PLATFORM
First seen: 2020-07-22 13:14:00
Last checked: 2020-07-23 14:50:45
```

DNSTICR - screenshots



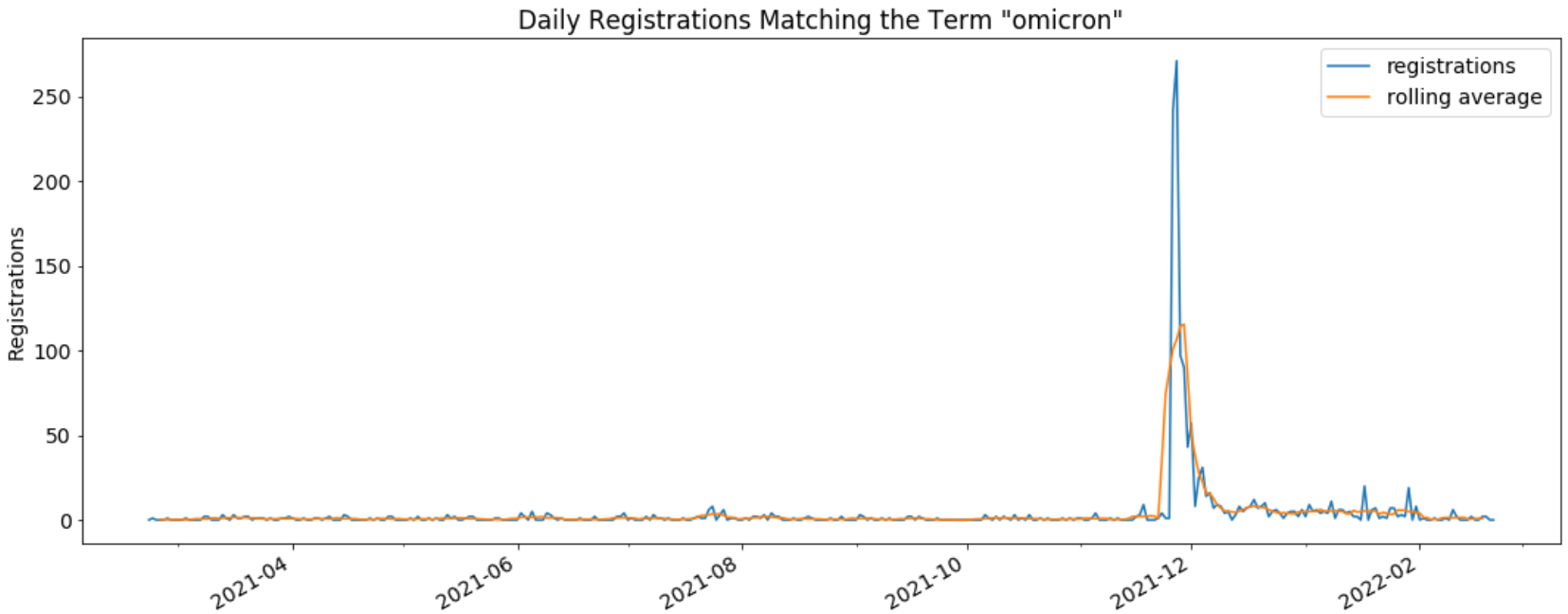
Full Picture



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.

New search terms

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



Statistics

- 2020 – May 9th 2022
  - 579 Search terms
  - 441,764 matched one or more search term
  - 23,758 (5.4%) had third-party reports
  - ~400 reports sent
- 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

Questions?

More information at:

https://www.icann.org/dnsticr-en