

DNS Abuse Measurement and Mitigation

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

4th December 2023

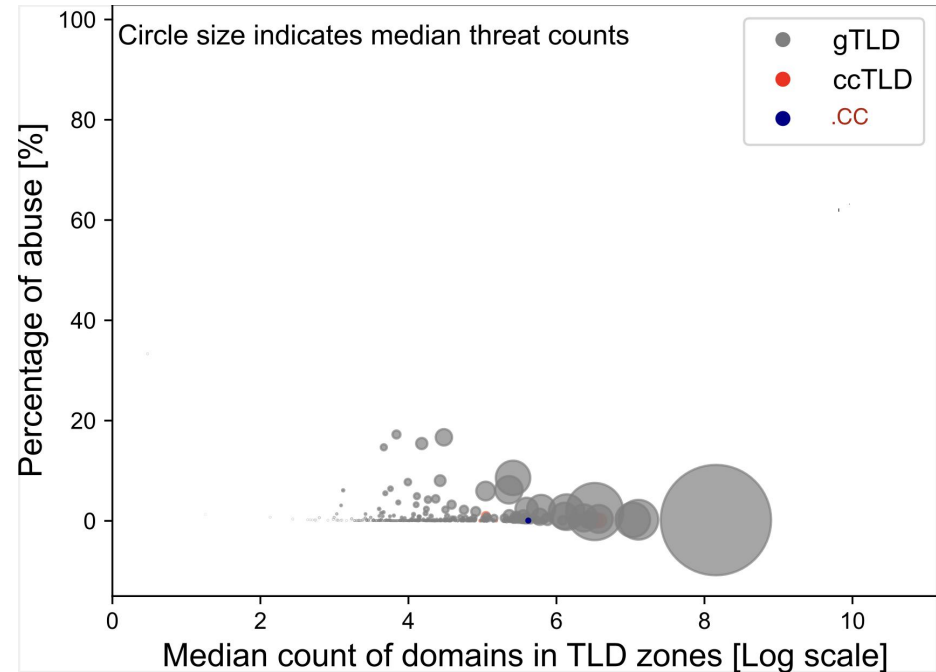
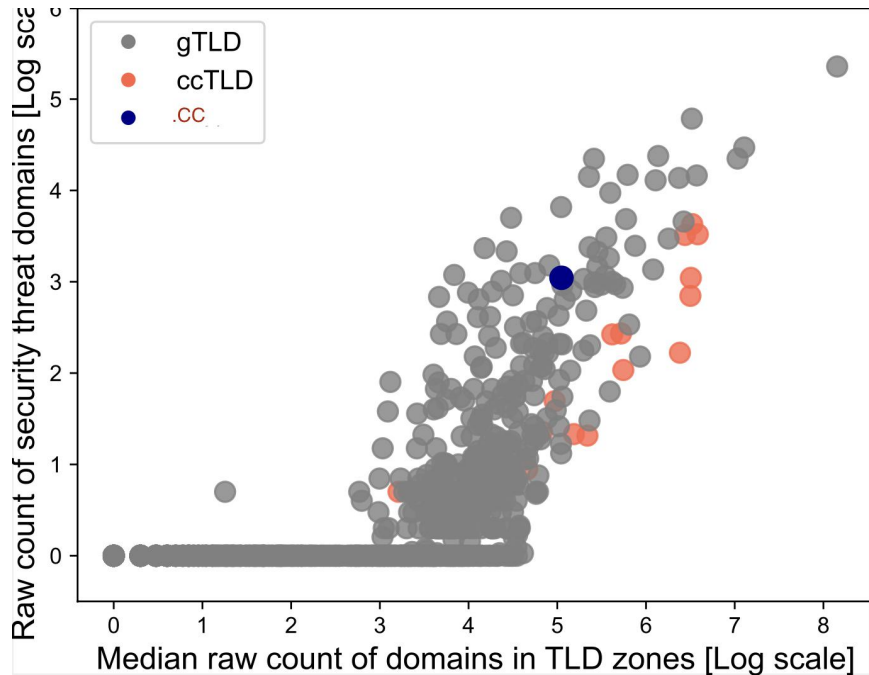


ICANN Security Stability & Resilience (SSR) Group

- Think Tank that mostly do research and development on Internet identifiers
- Our goal is to increase reliability of the metrics that measure (e.g., security, insecurity, abuse, etc.)
- Areas where existing methods and metrics need improvements or we need to develop a method from scratch
- We look to use data and scientific methods to answer questions of interest to the community

Why Metrics Matter?

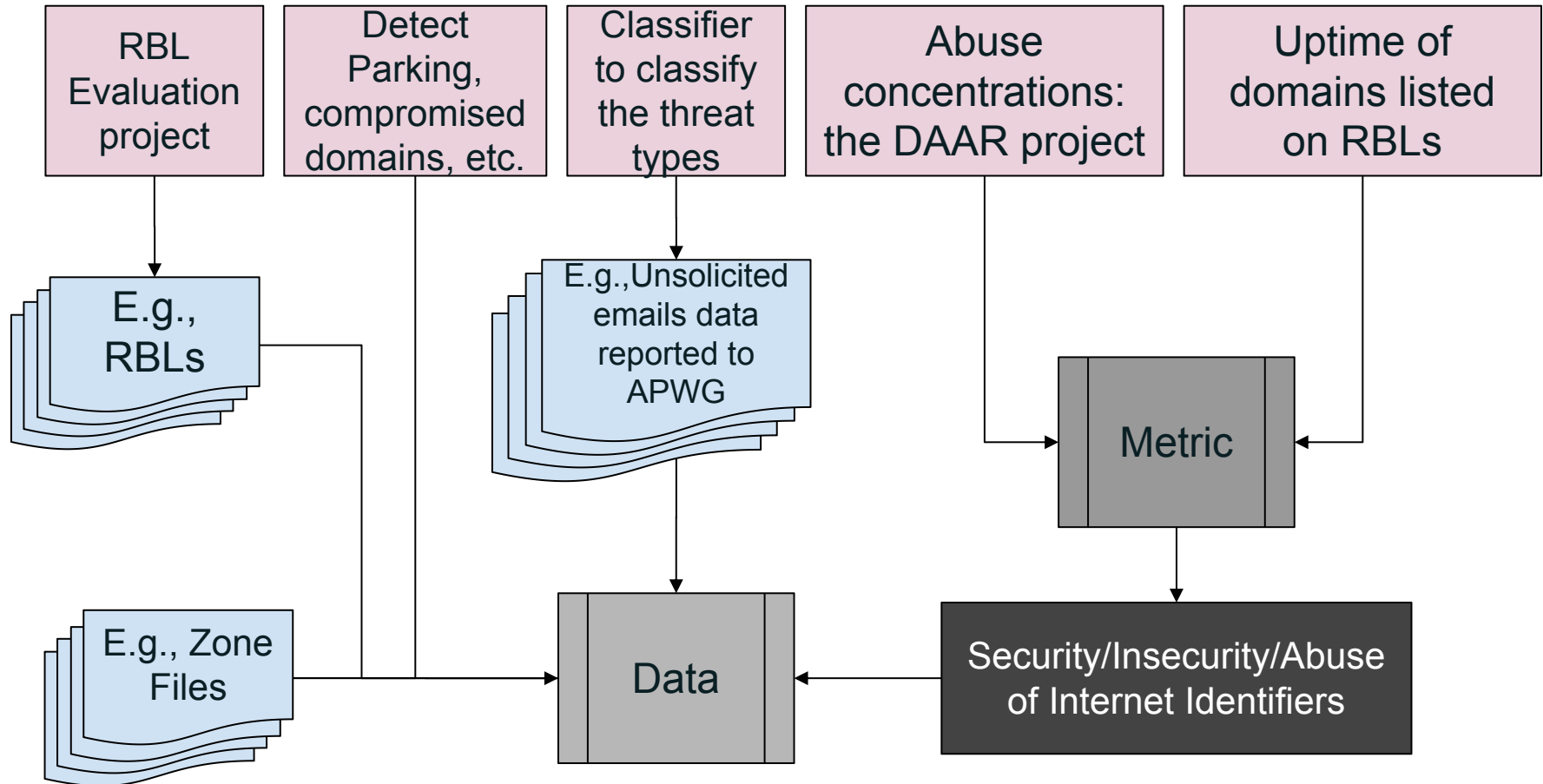
Same Data - Two different ways of showing it



What Makes a Better Metric?

- **Higher quality data** → data with fewer false positives
- **More precise definitions of what is measured** → e.g.,
Spam as a unsolicited email vs Spam as a delivery
mechanism for malware
- **Incorporating Measurement Errors** → acknowledging
limitations of the metric used

Towards Better Metrics



Domain Abuse Activity Reporting (DAAR)



DAAR (Domain Abuse Activity Reporting)

- Aggregate data from **RBLs** at TLD level (**count per TLD**)
- Combine with **count of domains** from **zonefile**
- Maintain **consistent** methodology since October **2017**
- **Monthly** reports
- **Daily** access through the API
- Longer term trends

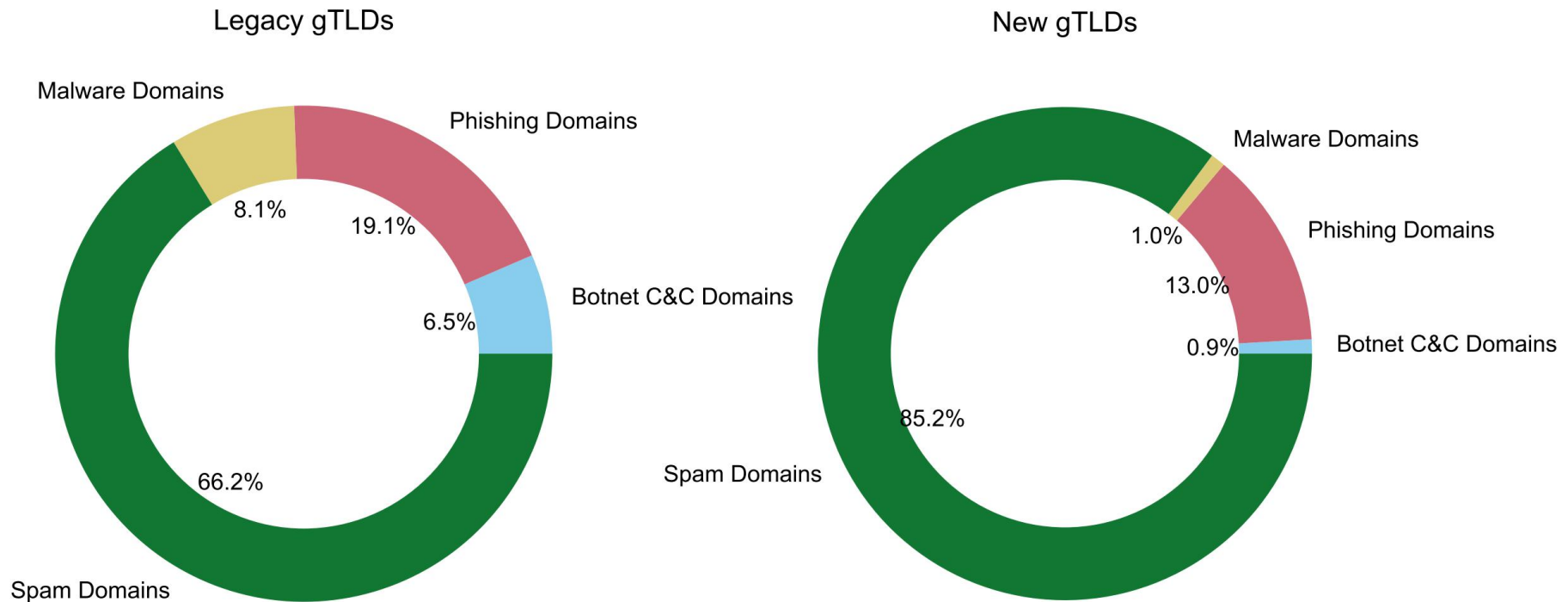
<https://www.icann.org/octo-ssr/daar>

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

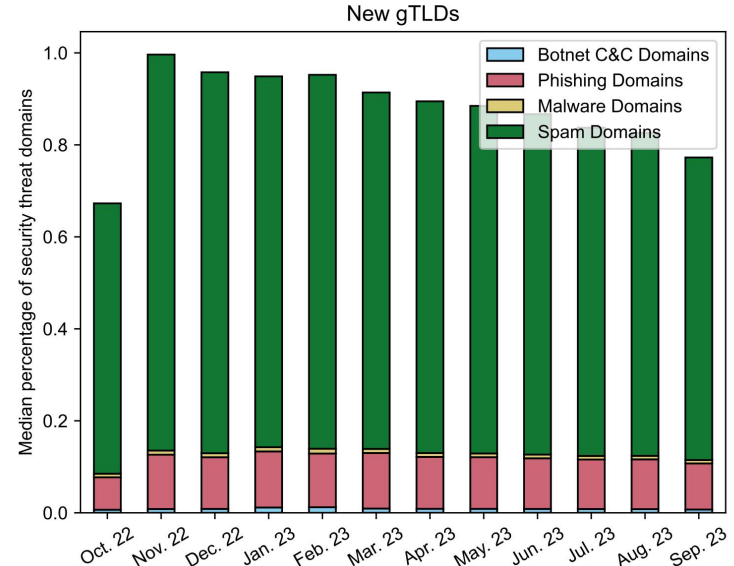
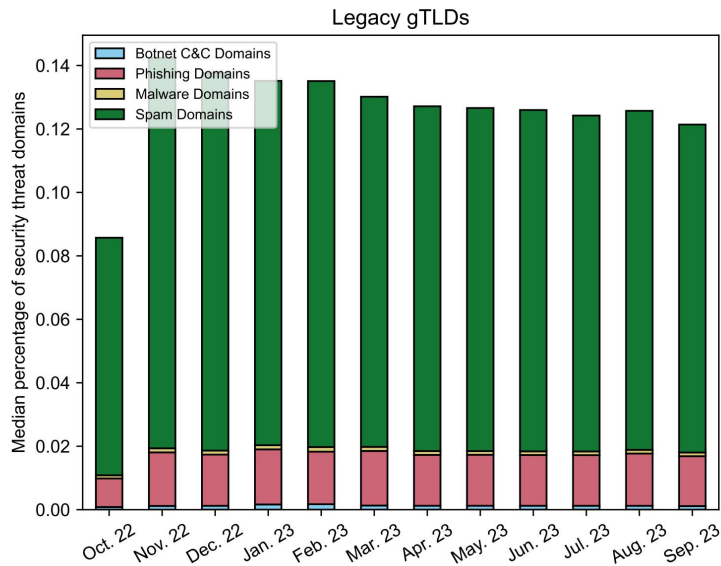
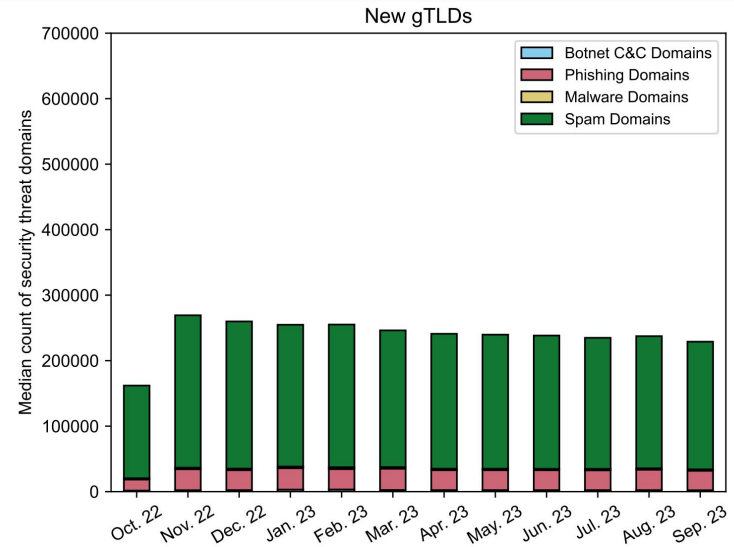
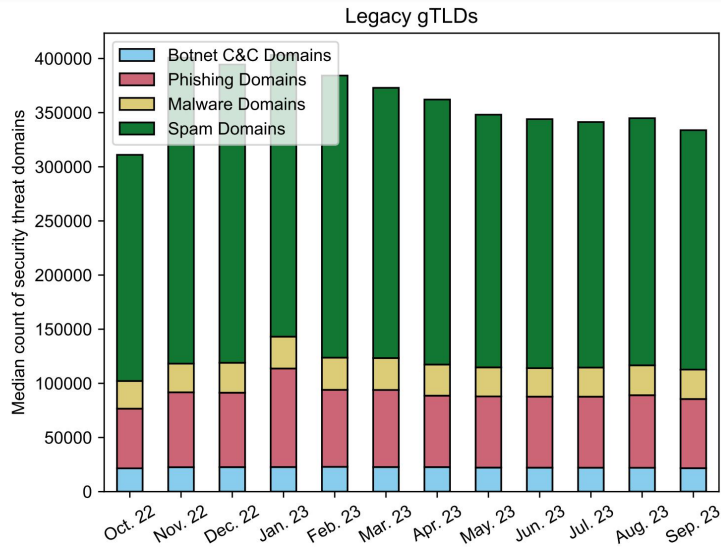
DAAR Monthly Report

Overview

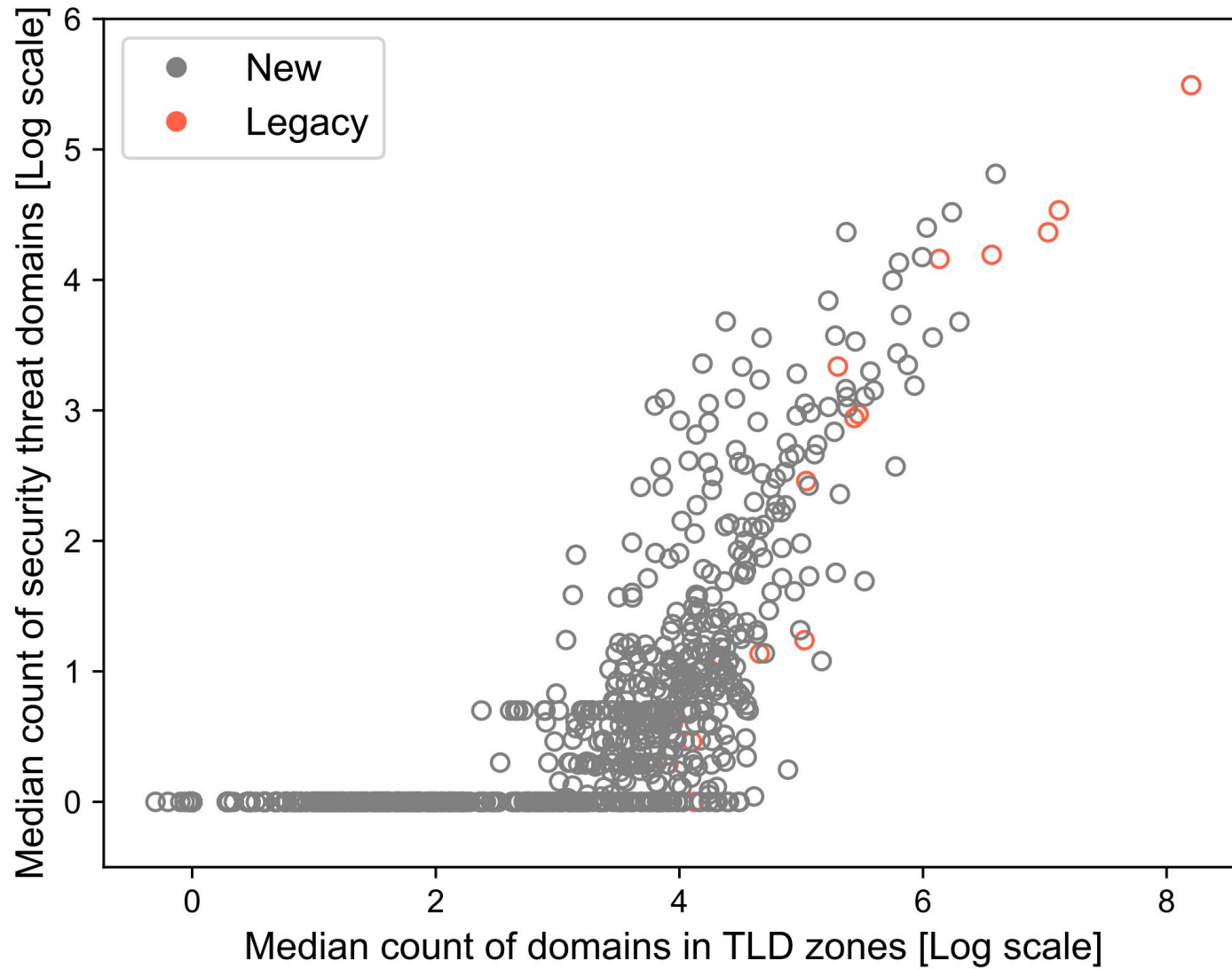


(Legacy gTLDs are those delegated pre-2010)

12-month trends

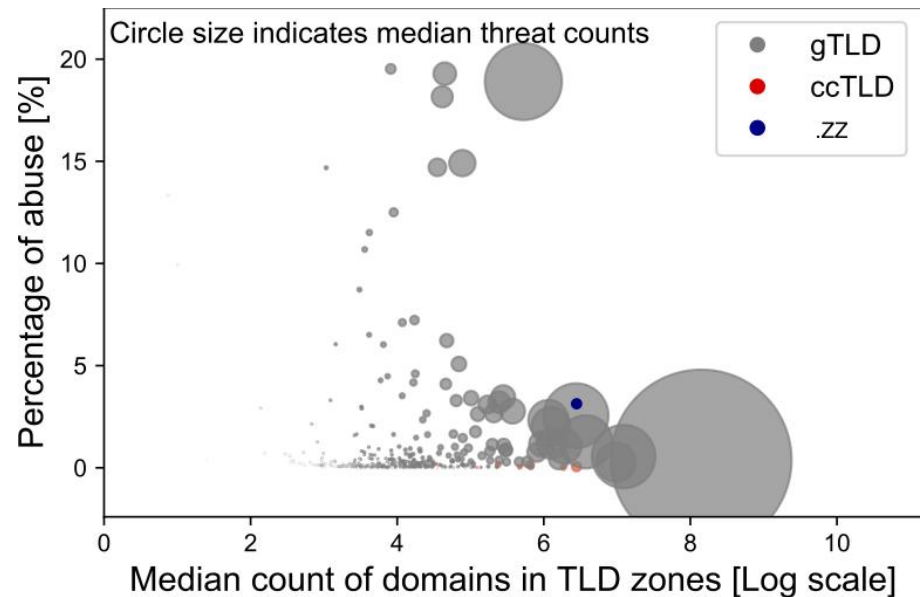
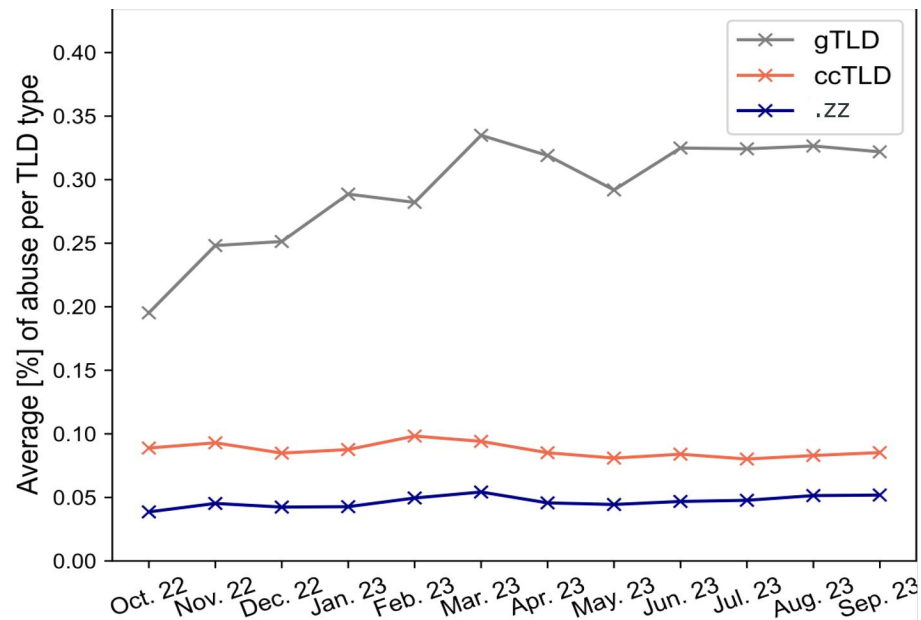


Per TLD



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



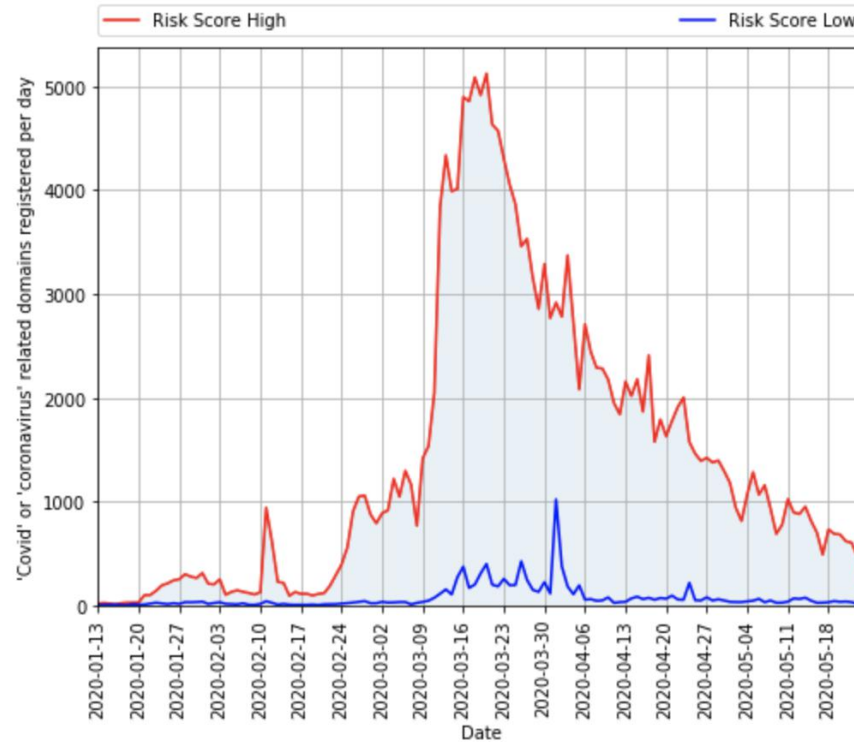
(Spoiler alert!)

- ⦿ 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

TLP: White

Domain trends update

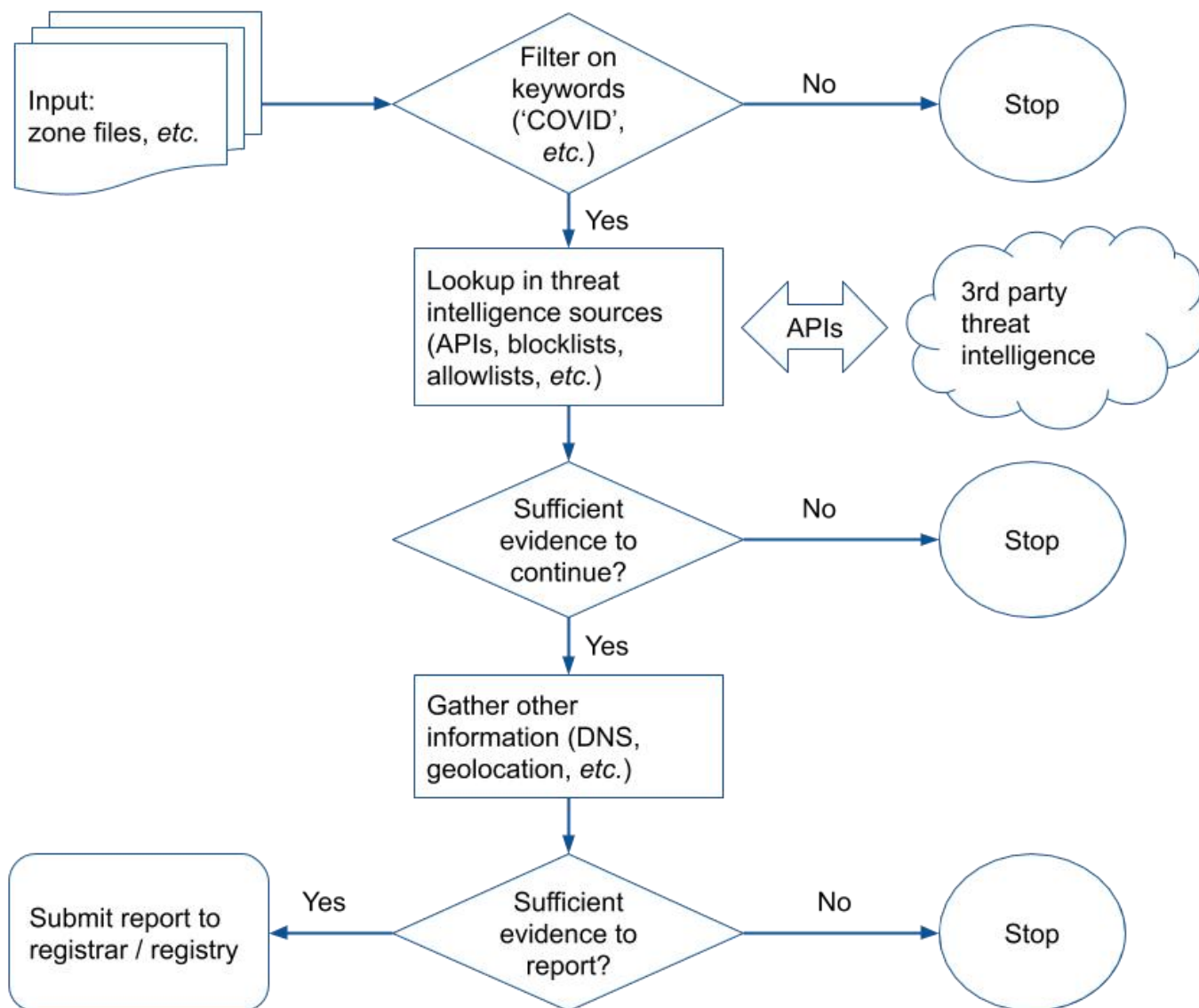


(Source: [John Conwell](#), DomainTools)

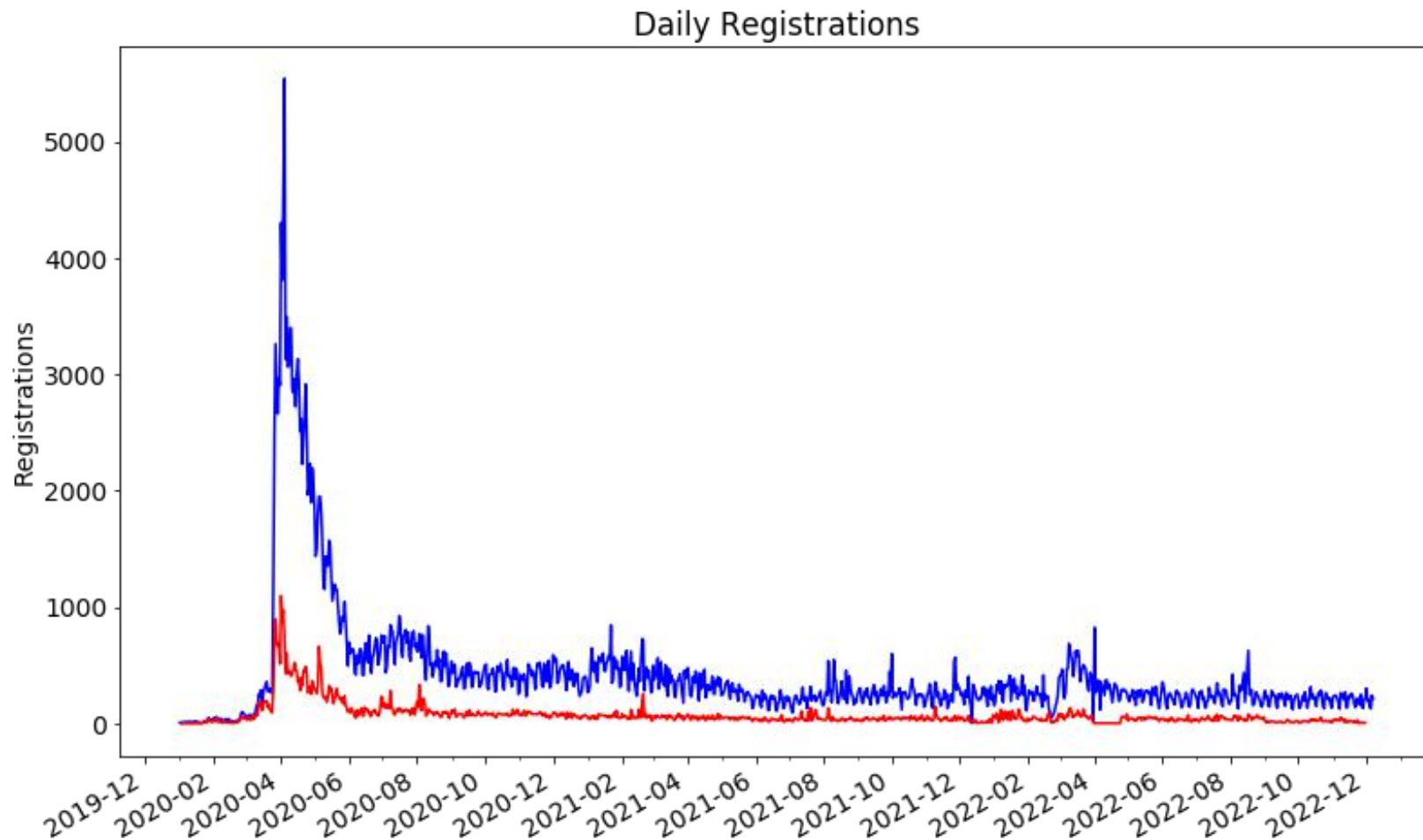
- ◉ Many articles talked about “suspicious” or “potentially malicious” registrations
- ◉ Some looked at full URLs, some at domains, some at certificates...
- ◉ Wanted a clear, published methodology
- ◉ Get good intelligence to the right people
- ◉ April 2022 – added terms related to conflict in Ukraine

Methodology

DNSTICR - Data to Intelligence



Results



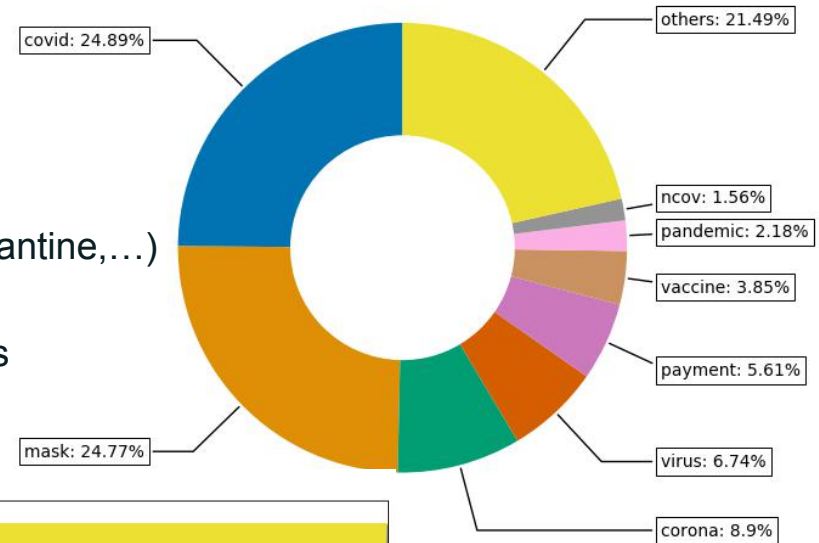
Registrations per day matching one or more of our filter terms (blue line) plus those which had one or more third-party reports (red line). Dates in DD-MM-YYYY format.

What keywords do these domains contain?

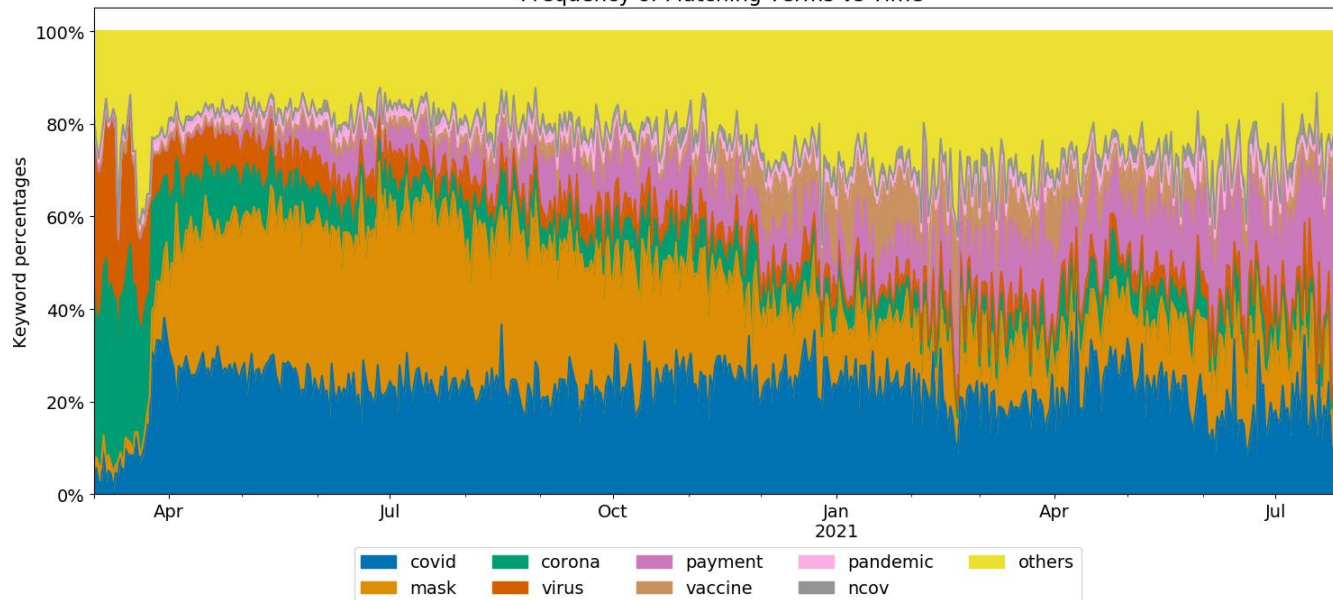
In the first 18 months:

- 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

Frequency of Matching Terms

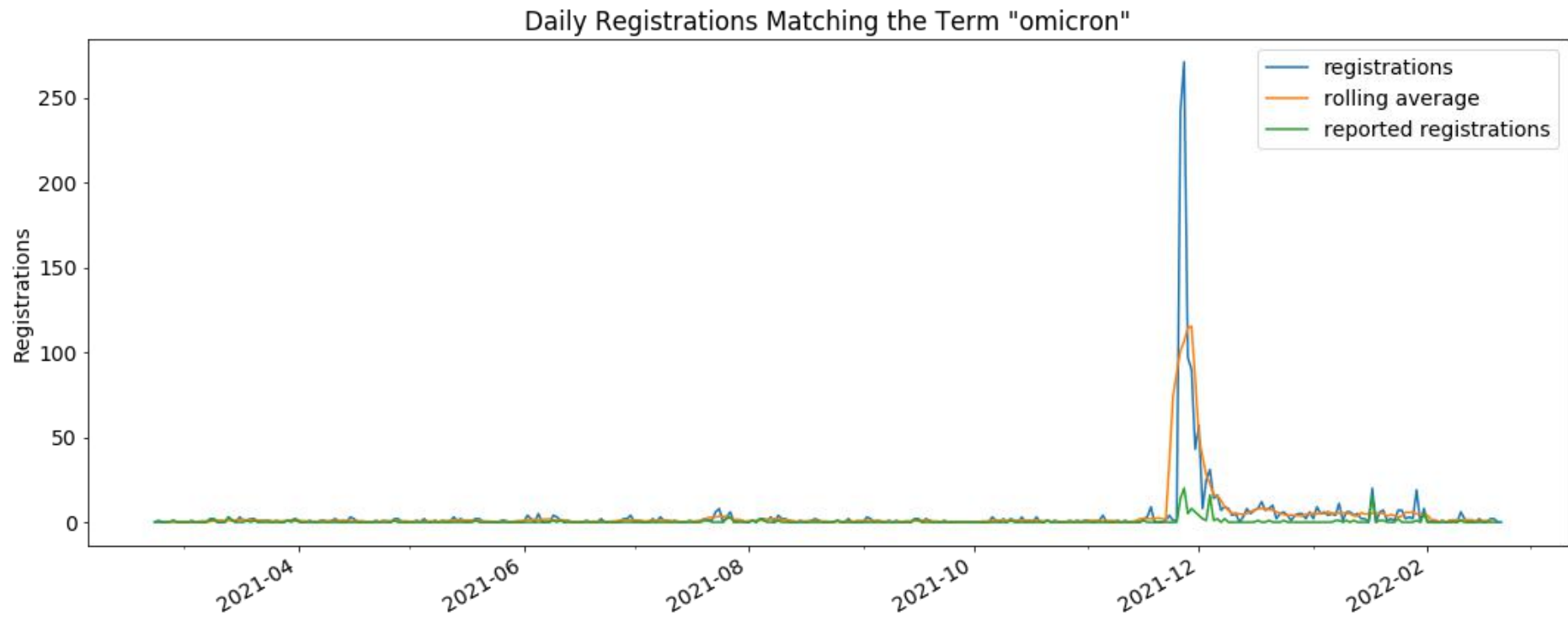


Frequency of Matching Terms vs Time

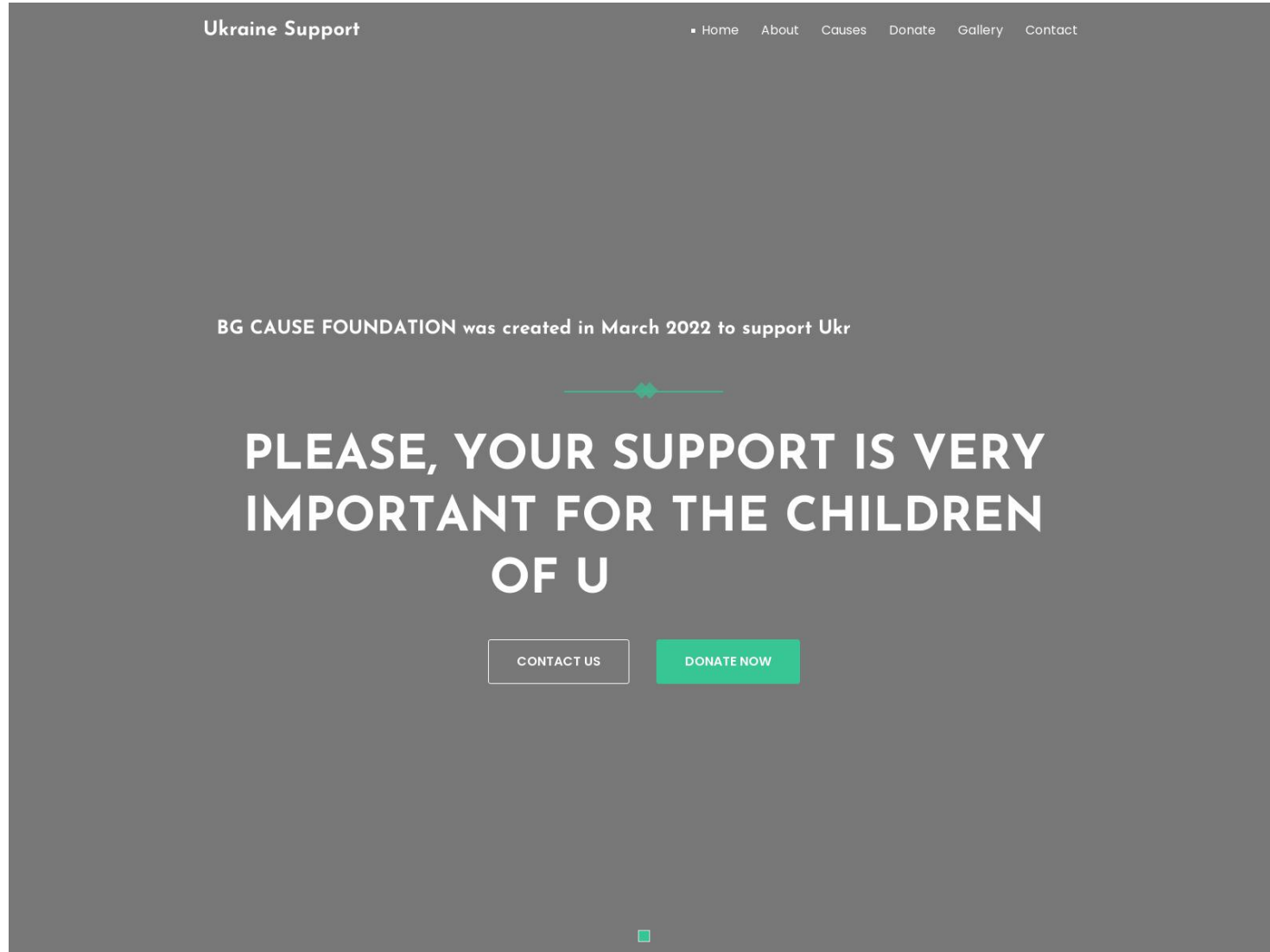


New search terms

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



- ⦿ 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






Єдиний Компенсаційний Центр

Повернення Невиплачених Грошових Коштів

[Головна](#) [Важливі новини](#) [Коментарі громадян](#) [Отримати компенсацію](#)

 Ви знаходитесь на офіційному сайті вповноваженого підрозділу по фінансовому захисту населення.

Ви вже отримали компенсацію?

Отримати компенсацію ПДВ від 7 000 грн до 90 000 грн можливо не пізніше 21 червня 2022 г. Сума нараховується за останні 36 місяців.

Перевірте наявність компенсації ПДВ в вашу адресу


Ведіть ім'я, прізвище та 6 останніх цифр банківської карти якою користуєтесь найчастіше та натисніть кнопку "Перевірити свою компенсацію"

>>>>>> <<<<<<<<

Якщо ви уже зареєстрували анкету на нашому сайті, введіть повторно gmail та 6 останніх цифр банківської карти, після чого натисніть кнопку «Перевірити свою компенсацію»

Якщо ви уже зареєстрували анкету на нашому сайті, введіть повторно gmail та 6 останніх цифр банківської карти, після чого натисніть кнопку «Перевірити свою компенсацію»

Згідно постанові 28/9329к, направленої на підтримку імпортозаміщення та підвищення благоустрою громадян, кожен громадянин може отримати грошову компенсацію витрат на оплату товарів іноземного виробництва. Розрахунок суми компенсації та виплата коштів здійснюється за період з 01.01.2016р. Сроку подачі заяв на отримання виплати по компенсації ПДВ за придбані товари іноземного виробництва обмежений.

 **УКП**

[Інструкція](#) [Онлайн чат](#) [Відгуки](#) [Подати заяву](#)

Компенсаційна Програма

Отримайте компенсацію від ЄС у вигляді кешбеку за всіма операціями вашої банківської карткою.

[ПОДАТИ ЗАЯВУ](#)



 **Вже отримали компенсацію**
25.00 тис+ людей

 **Виділено на УКП**
1 млрд+ гривень

 **Вже компенсовано**
748.00 млн+ гривень

Як отримати компенсацію

01. Заполните заявку

Вкажіть ваші ПІБ, номер картки та натисніть кнопку "Почати розрахунок" компенсації за вашою картою. Це займе не більше 1 хвилини

02. Розрахуйте виплату

Наш робот розрахує суму виплати за вашою картою. Це займе не більше 1 хвилини


03. Отримайте виплату

Виконуйте інструкції фахівця для отримання Вашої компенсації. Це не займе понад 5 хвилин


[Подати заяву](#)





| 29

 gov.ua

Державні послуги онлайн



 Людям із порушенням зору


 In English


Стара версія


Урядовий портал


Державні послуги онлайн

Головна / Виплата за COVID-19









Увага громадяни!

До 1 березня проводиться виплата на кожного громадянина України

Опис послуги

Виплата покладена кожному у зв'язку з сепарацією ООН і складною ситуацією в світі з 2020 року.

Президент України, Володимир Олександрович Зеленський підписав проєкт який встановлює і регулює дані виплати.

Розмір виплати становитиме індивідуальні суми до **30 000** гривень.

Для отримання гарантованої виплати натисніть на кнопку нижче.

Отримати виплату

Спосіб електронної ідентифікації: Електронний цифровий підпис


Як отримати послугу


Подати електронну заяву особисто через Електронний кабінет платника.


Мапа порталу

Власність Секретаріату Кабінету Міністрів України. Проєкт реалізовано Фондом Східна Європа та Державним агентством з питань електронного урядування України у межах програми міжнародної технічної допомоги "Електронне урядування задля підзвітності влади та участі громади" (EGAP) , за фінансової підтримки Швейцарської агенції розвитку та співробітництва


In English







Людям із порушенням зору





Thank You and Questions

Visit us at icann.org

sion.lloyd@icann.org



[@icann](https://twitter.com/icann)



linkedin/company/icann



facebook.com/icannorg



slideshare/icannpresentations



youtube.com/icannnews



soundcloud/icann



flickr.com/icann



instagram.com/icannorg