DNS Abuse & the Global Threat Landscape

BCOP Forum

19th December 2025

Background - Meet the SSR team

Example Project - DNSTICR

Local Picture

Example Project - INFERMAL

Final Remarks

Why Does DNS Abuse Exist?

"Security failure is caused at least as often by **bad / misaligned incentives** as by bad design."

"Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail."

Ross Anderson & Tyler Moore. "The Economics of Information Security" science 314.5799 (2006): 610-613.

DNS (in)security / DNS Abuse

Domains and **DNS Infrastructure** and its associated **components** and **processes** are not adequately secured

Opportunities for malicious actors to exploit vulnerabilities and engage in various forms of **DNS abuse**

Domains abused for: **Phishing**, **Malware**, **Botnet Command and Control**

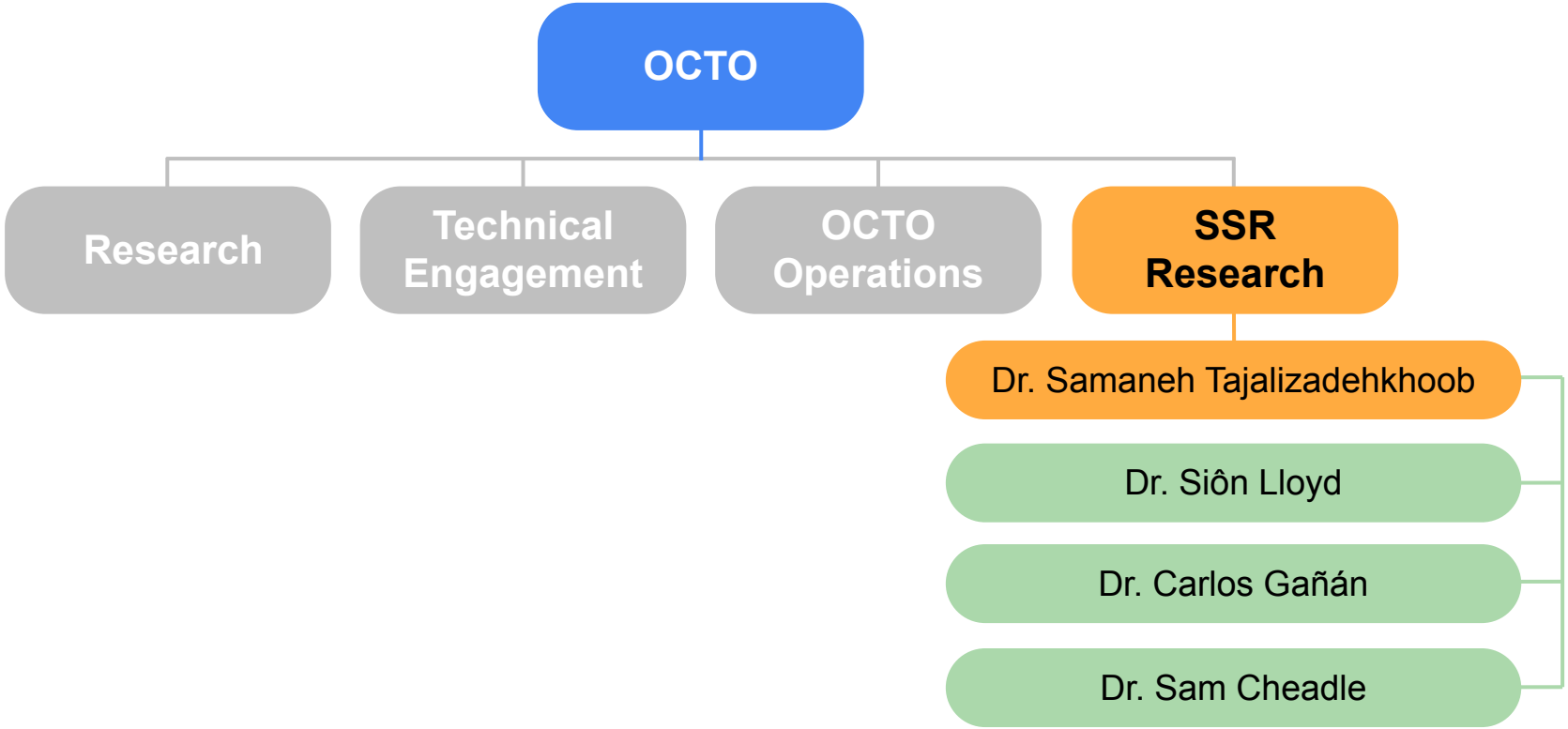
How to Align / Improve Incentives

Simple Answer: High Quality Metrics

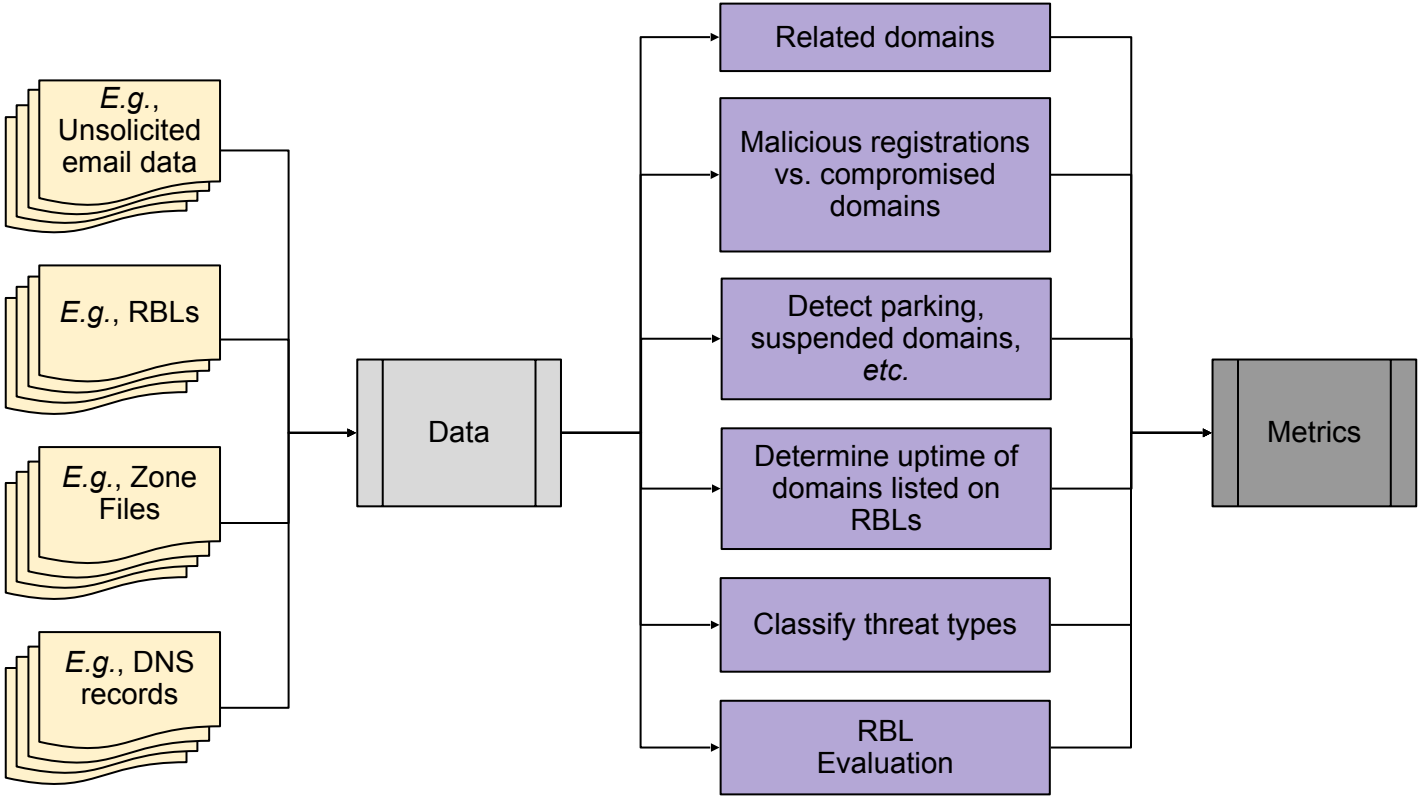
Metrics influence decision-making by **quantifying security performance**, allocating resources, and impacting priorities.

Poorly designed metrics can create **perverse incentives**, leading to unintended consequences and short-term focus.

Security, Stability & Resiliency Research Team



Data into Metrics



Background - Meet the SSR team

Example Project - DNSTICR

Local Picture

Example Project - INFERMAL

Final Remarks

(Spoiler Alert!)

Criminals use the Internet

Criminals use big events to "hook" victims

Global events + Internet = mass audience

Big events create bursts in domain name registrations

COVID-19 was no different

Scale was larger than previously seen

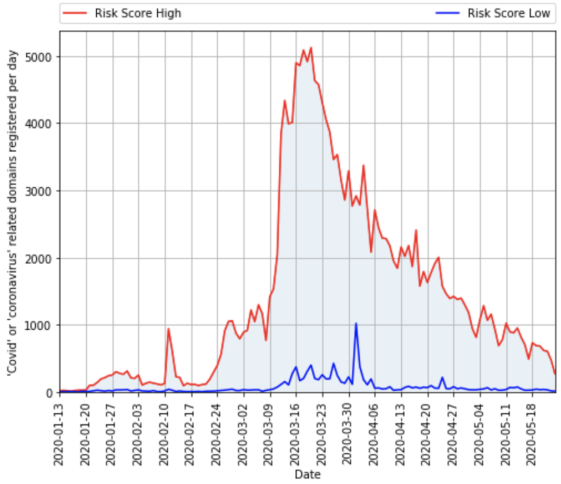
"Perfect storm" due to working from home

Context

Many articles written
about “suspicious” or “potentially malicious” registrations,

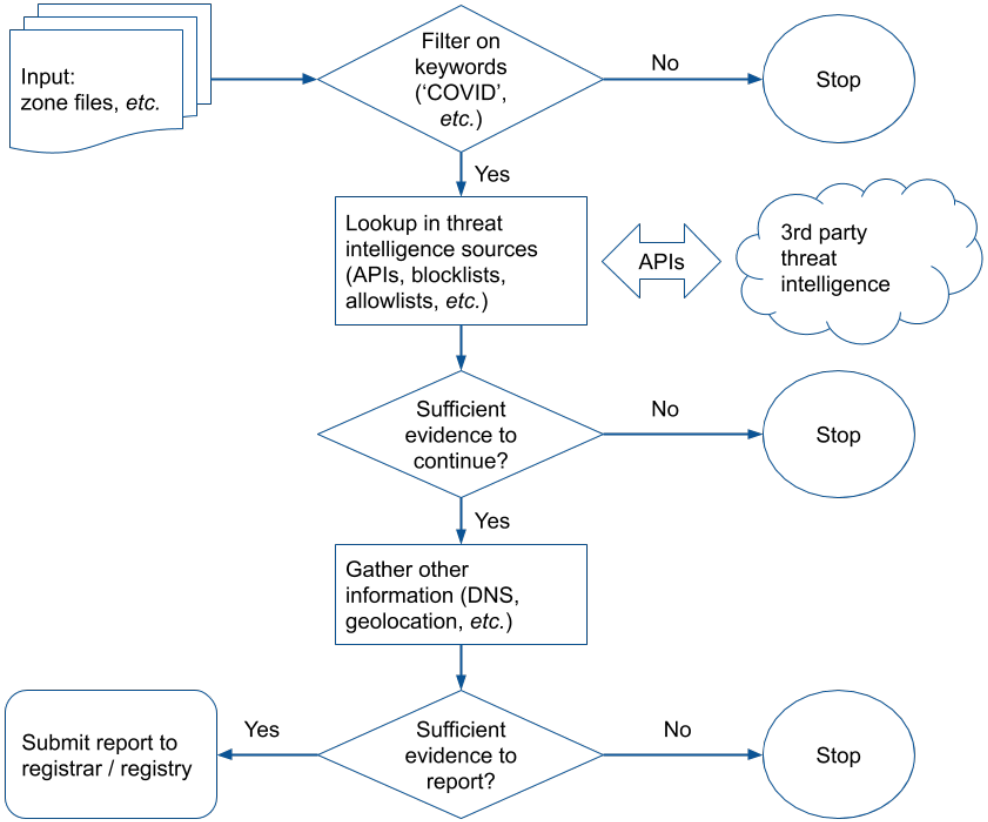
TLP: White

Domain trends update

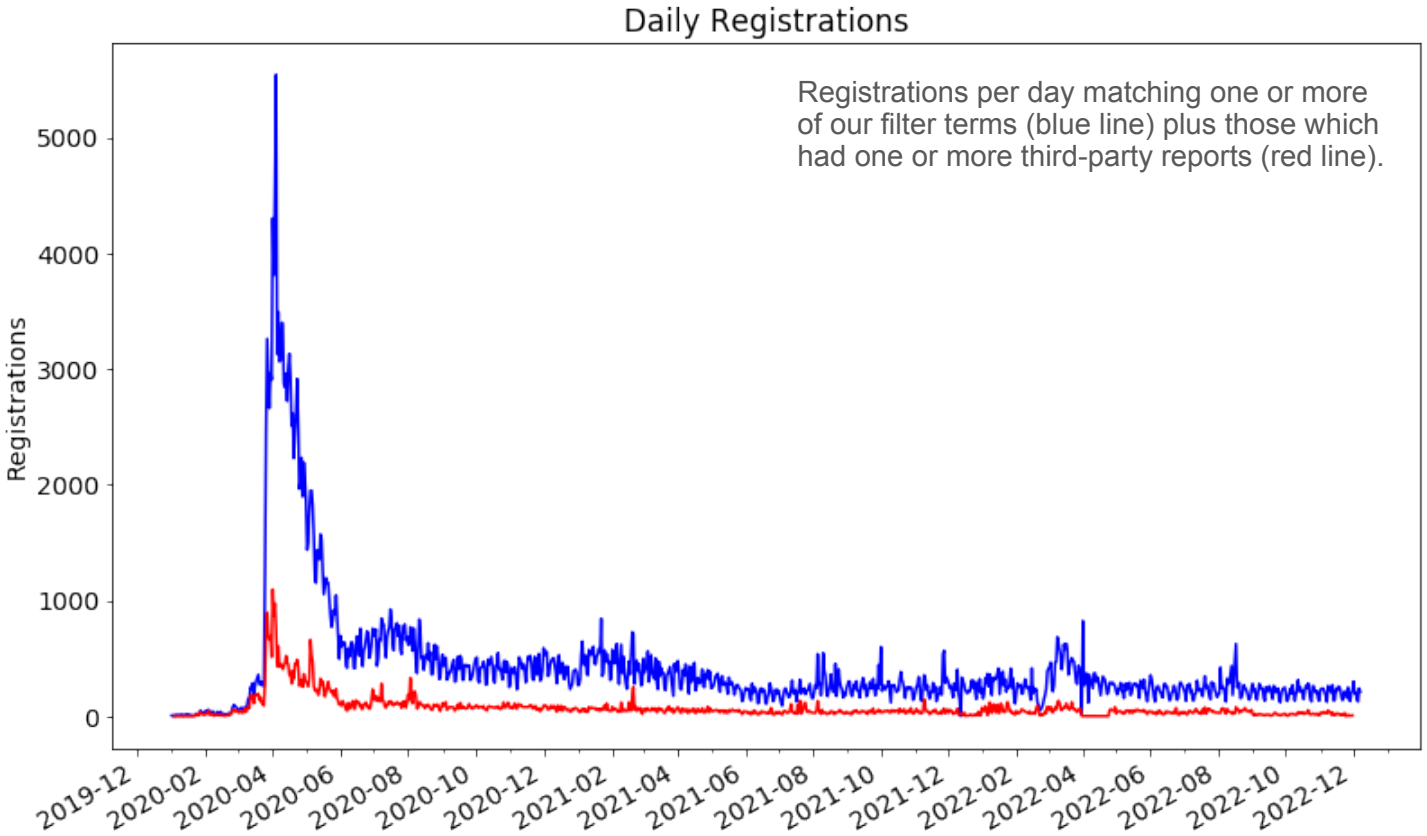


(Source: John Conwell, DomainTools)

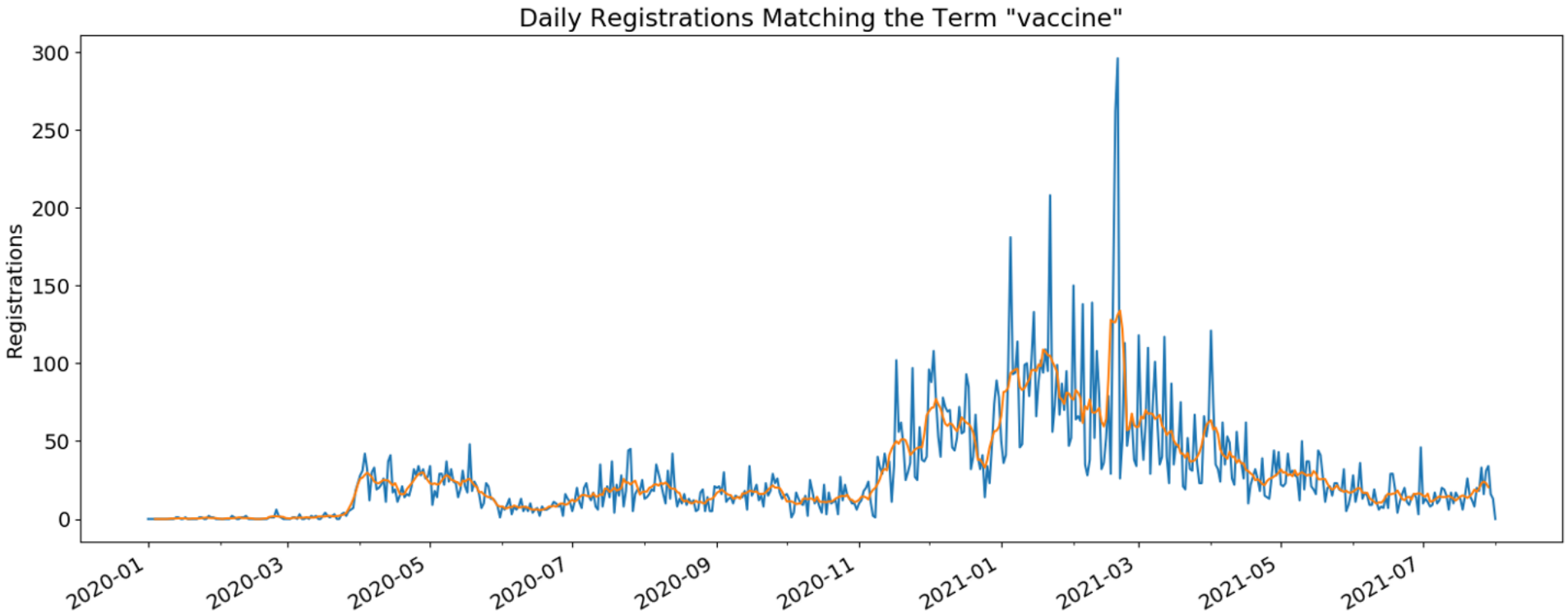
Method


Input:
zone files, *etc.*
Filter on keywords ('COVID', *etc.*)
No
Stop
Yes
Lookup in threat intelligence sources (APIs, blocklists, allowlists, *etc.*)
APIs
3rd party threat intelligence
Sufficient evidence to continue?
No
Stop
Yes
Gather other information (DNS, geolocation, *etc.*)
Submit report to registrar / registry
Yes
Sufficient evidence to report?
No
Stop

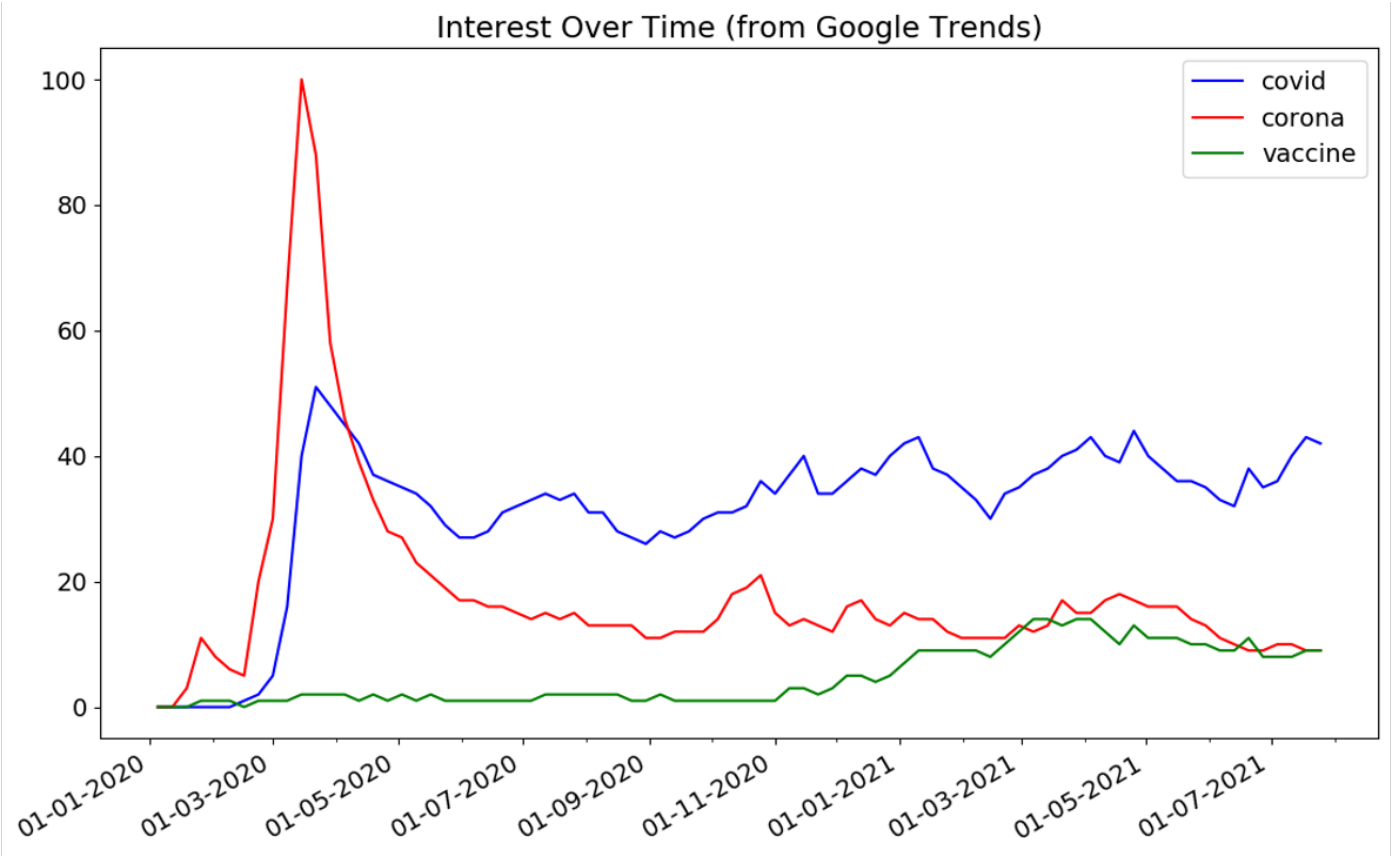
What we saw


Daily Registrations
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).
Registrations
5000
4000
3000
2000
1000
0
2019-12
2020-02
2020-04
2020-06
2020-08
2020-10
2020-12
2021-02
2021-04
2021-06
2021-08
2021-10
2021-12
2022-02
2022-04
2022-06
2022-08
2022-10
2022-12

Changing Tactics



Changing Tactics

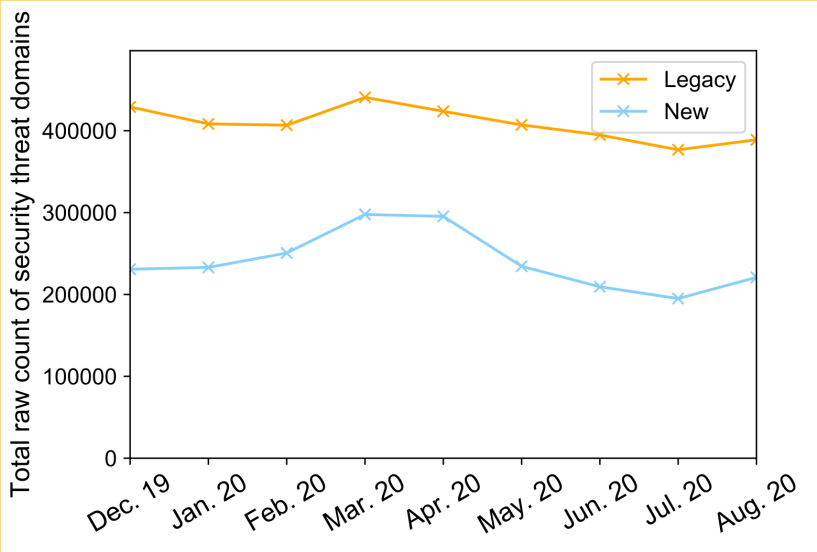


Observations

We saw *no* significant increase in overall reported abuse levels

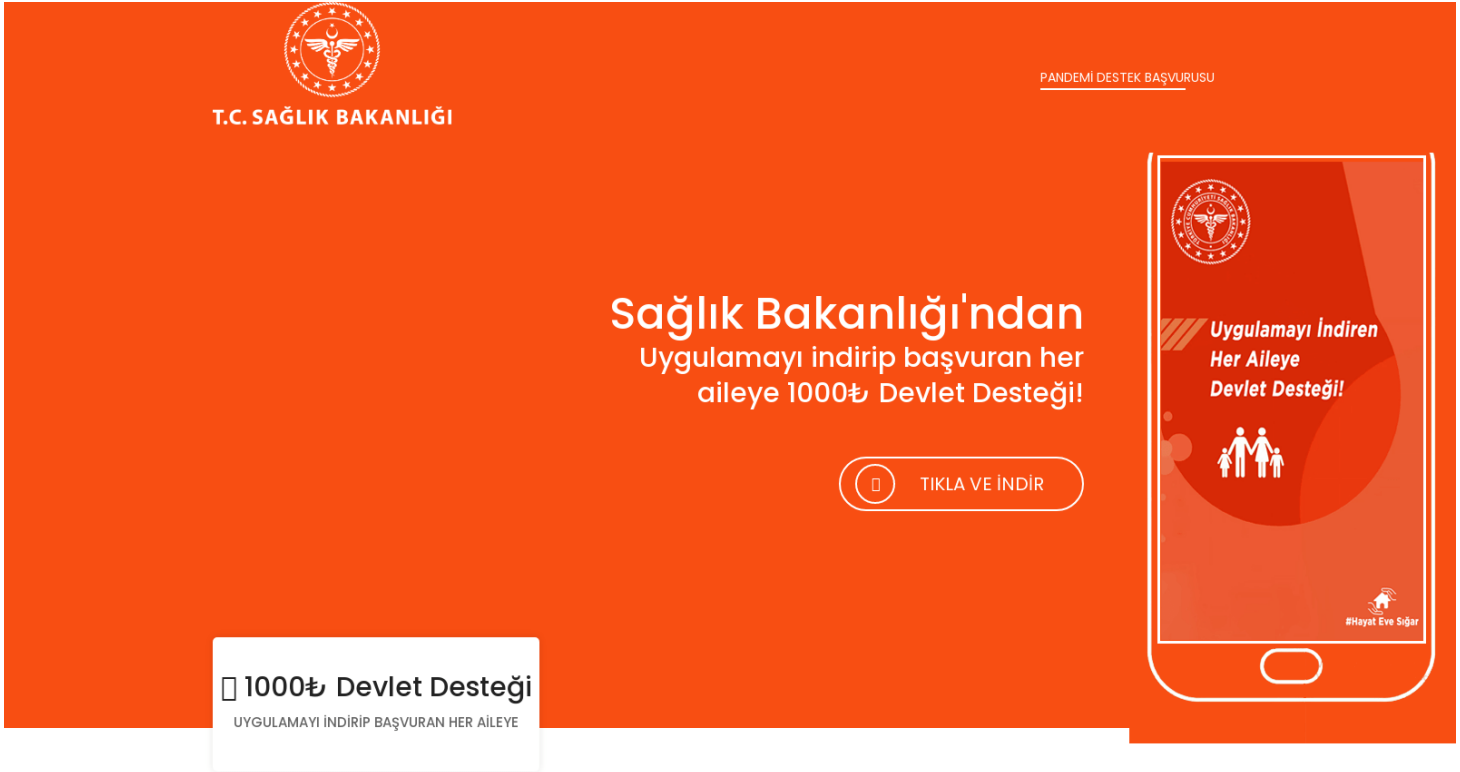
Tactics evolved, bad actors do whatever works

Majority (94%) of matching registrations had no reports of abuse



From August 2020 DAAR monthly report.

Examples


T.C. SAĞLIK BAKANLIĞI
PANDEMİ DESTEK BAŞVURUSU
Sağlık Bakanlığı'ndan
Uygulamayı indirip başvuran her aileye 1000₺ Devlet Desteği!
TIKLA VE İNDİR
Uygulamayı İndiren Her Aileye Devlet Desteği!
#Hayat Eve Sığar
1000₺ Devlet Desteği
UYGULAMAYI İNDİRİP BAŞVURAN HER AİLEYE

Examples


THE AMERICAN RESCUE PLAN
THE AMERICAN RESCUE PLAN ACT OF 2021
Frequently Asked Questions
Contact Us
APPLY NOW
$1,400
payments per person
with more than 5 million in mixed-status families eligible
$40B*
to keep families in their homes
including $100 million for housing counseling, and $10B for mortgage assistance. A relief to the 64% of Latinos worried about making their next mortgage payment.
$109B*
to fight poverty
including the 9.9 million Latino children newly eligible for the full Child Tax Credit
$54.5B*
to give people access
to the health care they need with lower-cost health coverage and funding for community health centers
$10.42B*
to help 50 million Americans
overcome hunger with more funding for WIC, SNAP, and nutrition assistance for Puerto Rico
$217.6B*
invested in education
to make sure schools reopen safely, expand internet access, and to support college students facing hardship

Examples

English | Locations | Support | Informed Delivery | Register / Sign In

USPS.COM® | Quick Tools | Mail & Ship | Track & Manage | Postal Store | Business | International | Help

USPS Tracking®

Tracking / FAQs >

Track Another Package +

Tracking Number: US9514901185421

Status :

We have issues with your shipping address

USPS Allows you to Redeliver your package to your address in case of delivery failure or any other case.
You can also track the package at any time, from shipment to delivery.

Status Not Available

Verify Address

First, we need to confirm your address is eligible for Informed Delivery.

Full name | Street Address 2 (OPT)

Street Address 1

City | Select State | ZIP Code™ (OPT)

Phone Number

Background - Meet the SSR team

Example Project - DNSTICR

Local Picture

Example Project - INFERMAL

Final Remarks

Overview of Brazil Phishing

Tracked Brands

All detected pages

Search

Search String

Countries

- All Countries
- Argentina | 1
- Brazil | 29

Industry Verticals

- All Verticals
- Banking | 11
- Consumer | 3
- E-commerce | 1
- Financial | 8
- Food | 1
- Gambling | 1
- Government | 1
- Hospitality | 1
- Retail | 2
- Transportation | 1

25 of 30 shown, 130,446 suspicious scans detected

Brand Name	Hits	Last match	Whitelist	Country	Industry
Serasa	447	2h ago	2	Brazil	Financial
Viva Sorte	1,336	2h ago	1	Brazil	Gambling
Banco Itau	62,841	2h ago	26	Brazil	Banking
Sicredi	107	9h ago	1	Brazil	Financial
MercadoLibre	2,744	14h ago	8	Brazil	Consumer
Magazine Luiza	13,471	3d ago	1	Brazil	Consumer
Banco do Brasil	9,888	4d ago	2, 1	Brazil	Banking
Banco Bradesco	4,103	5d ago	3	Brazil	Banking
Correios	703	9d ago	1	Brazil	Transportation
Realize	4,052	14d ago	1	Brazil	Financial
Hipercard	2,380	25d ago	1	Brazil	Banking
Caixa	6,748	1mo ago	1, 1	Brazil	Government
Banco Inter	2,113	1mo ago	2	Brazil	Banking
Growth Supplements	3	1mo ago	1	Brazil	Food
Pagbank	125	2mo ago	2	Brazil	Financial
Universo Online (UOL)	1,369	2mo ago	1	Brazil	Banking
Rede	44	2mo ago	1	Brazil	Financial
Omnibees	55	4mo ago	1	Brazil	Hospitality
Banco Safra Limited	275	4mo ago	2	Brazil	Banking

Data: urlscan.io (01/12/2025)

Headlines …

WhatsApp compromise leads to Astaroth deployment

Another campaign targeting WhatsApp users in Brazil spreads like a worm and employs multiple payloads for credential theft, session hijacking, and persistence

Written by Colin Cowie

NOVEMBER 20, 2025

https://news.sophos.com/en-us/2025/11/20/whatsapp-compromise-leads-to-astaroth-deployment/

GASA Global Anti-Scam Alliance (GASA) · Nov 12 · 3 min read

New Report Reveals Brazilians Face 252 Scam Encounters Annually Despite High Confidence in Spotting Fraud

The Hague, Netherlands – 12 November , 2025 – The Global Anti-Scam Alliance (GASA) will release its State of Scam Brazil Report 2025 on November 13, revealing an alarming

https://www.gasa.org/post/new-report-reveals-brazilians-face-252-scam-encounters-annually-despite-high-confidence-in-spotting

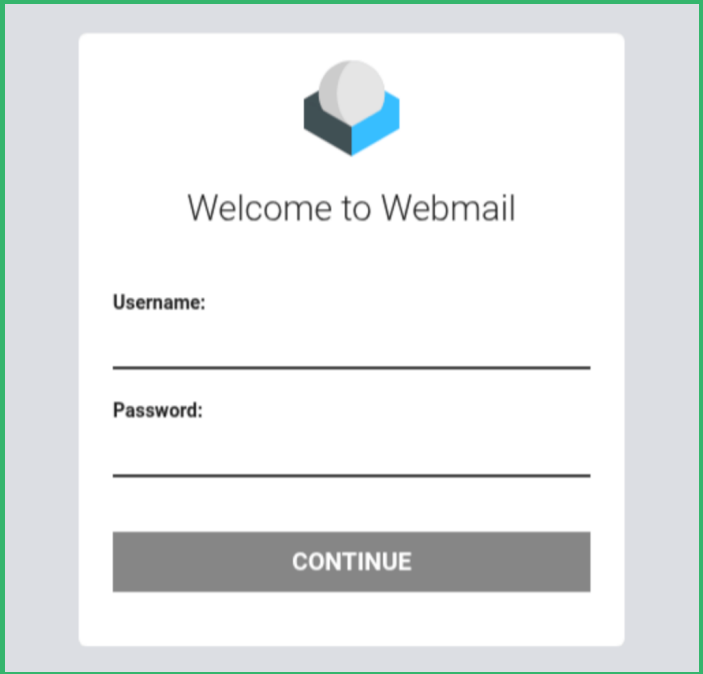
Targeted campaigns …

Social engineering page impersonating the Brazilian government's electronic tax document system (Portal da Nota Fiscal Eletrônica)

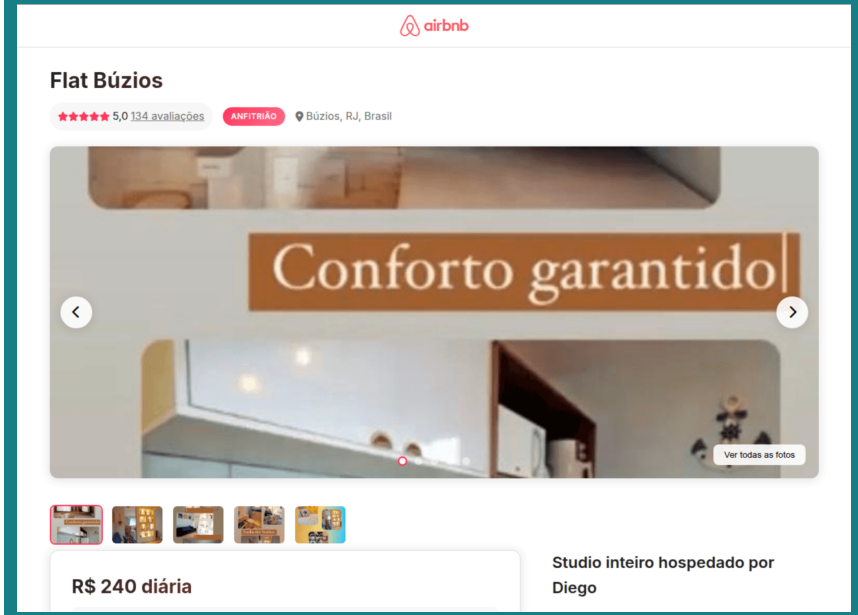
https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-targeting-brazil

https://cyble.com/blog/relaynfc-nfc-relay-malware-targeting-brazil

Use of .br …



https://alot____lote.com.br



https://www.airbnbflat___.com.br

Background - Meet the SSR team

Example Project - DNSTICR

Local Picture

Example Project - INFERMAL

Final Remarks

INFERMAL Inferential Analysis of Maliciously Registered Domains

ICANN funded project, conducted by KOR Labs / Grenoble Alpes University

KOR Labs

UGA Université Grenoble Alpes

ICANN

Exposing the Roots of DNS Abuse: A Data-Driven Analysis of Key Factors Behind Phishing Domain Registrations

Yevheniya Nosyk, Maciej Korczyński, Carlos Gañán, Sourena Maroofi, Jan Bayer, Zul Odgerel, Samaneh Tajalizadehkhoob, Andrzej Duda

CCS ’25, October 13–17, 2025, Taipei, Taiwan
https://dl.acm.org/doi/10.1145/3719027.3744869

https://www.icann.org/resources/pages/inferential-analysis-maliciously-registered-domains-infermal-2024-12-03-en

Approach

Investigate domain abuse from the *attacker's* perspective

Identify factors driving malicious (phishing) domain registrations

73 features covering three factors:

Registration attributes

Free API
Payment methods
Pricing
Discounts
Free web hosting
Free DNS
Free email

Proactive verification

Validation of contact details (phone / email address)

String-based validation

Registration restrictions (*e.g.* ID required)

Reactive security practices

Malicious domain name uptimes

Driving factors (at registrar-TLD level)

Driver	Type	Correlation to abuse counts	Increase
Retail price	Numerical	Weak Positive	1$↓ ⇒ 6.6%↑
Retail discount	Numerical	Positive	1$↓ ⇒ 49%↑
Cryptocurrency accepted	Boolean	Positive	30%
API availability	Boolean	Strong Positive	401%

Driving factors (at registrar-TLD level)

Driver	Type	Correlation to abuse counts	Increase
Free DNS	Boolean	Positive	205%
Free Web Hosting	Boolean	Positive	88%
Restrictive registration policies	Boolean	Negative	(-) 63%
Validation of phone / email address	Boolean	Negative	(-) 70%
Shorter uptimes	Numerical	Negligible	~0%

Considerations

Investigate drivers from the *attacker's* perspective

Legitimate users will also favour some factors

Consider impact of changes to both parties (bad actors adjust)

401% (API Availability)

Model looks at many factors at once. The figure doesn't exist in isolation, it holds all other factors constant. Changing other factors would change this figure.

Some variables are combined

e.g. payment methods into three:
cryptocurrency
bank transfer
digital wallets

Disclaimer

Results should be interpreted with caution and may or may not be generalized into actions by registrars or TLDs

Background - Meet the SSR team

Example Project - DNSTICR

Local Picture

Example Project - INFERMAL

Final Remarks

Final Remarks

Nothing is new

Bad actors have always changed tactics
AI won't change that
It might raise the lower end

Local picture not unusual

Metrics are key

Good metrics give valuable insight

Conversely, bad metrics can create false impressions

Thank you!

icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin.com/company/icann

instagram.com/icannorg