

COVID-Related DNS Abuse Webinar

(Hosted by the Contracted Party House)



Agenda

- Overview
- Siôn Lloyd, ICANN SSR
- Chris Lewis-Evans, UK National Crime Agency
- Graeme Bunton, Tucows
- James Galvin, Afilias
- Brian Cimbolic, PIR
- Q&A
 - Registry/Registrar Experiences
 - Community Q&A

COVID-19, What we see

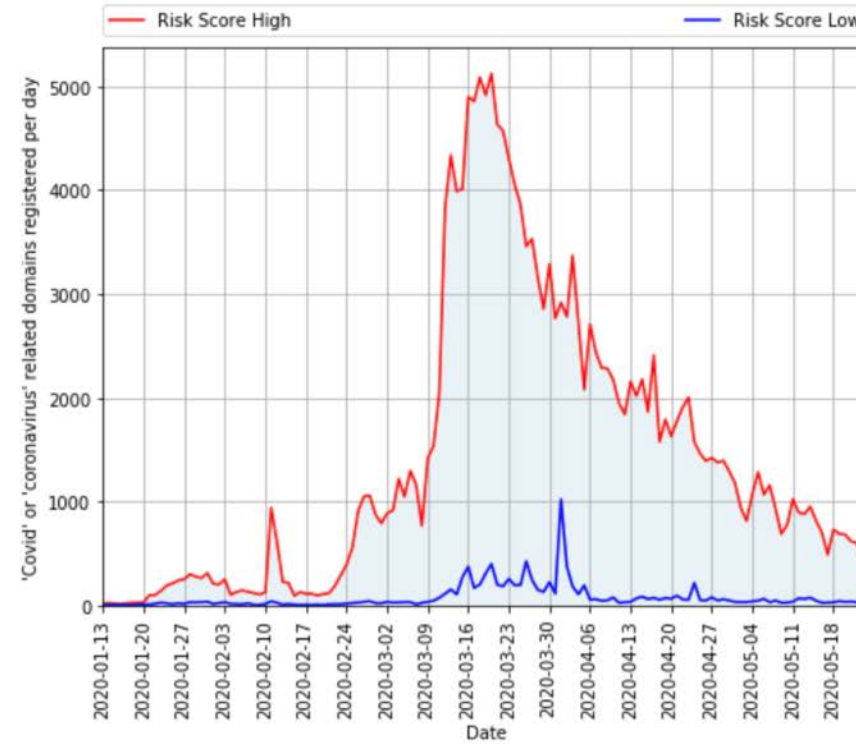
Siôn Lloyd
ICANN SSR

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

Context

TLP: White

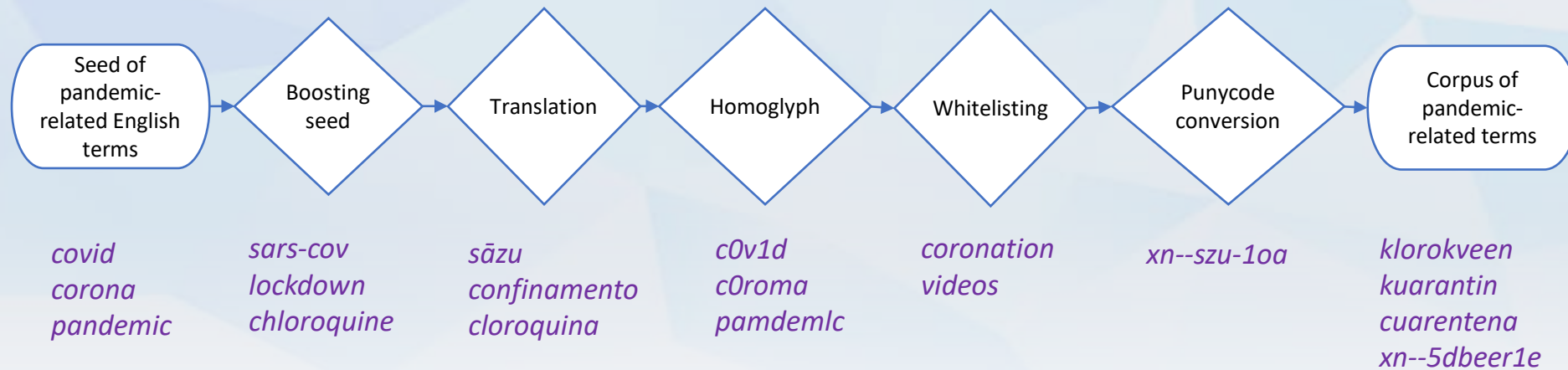
Domain trends update



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

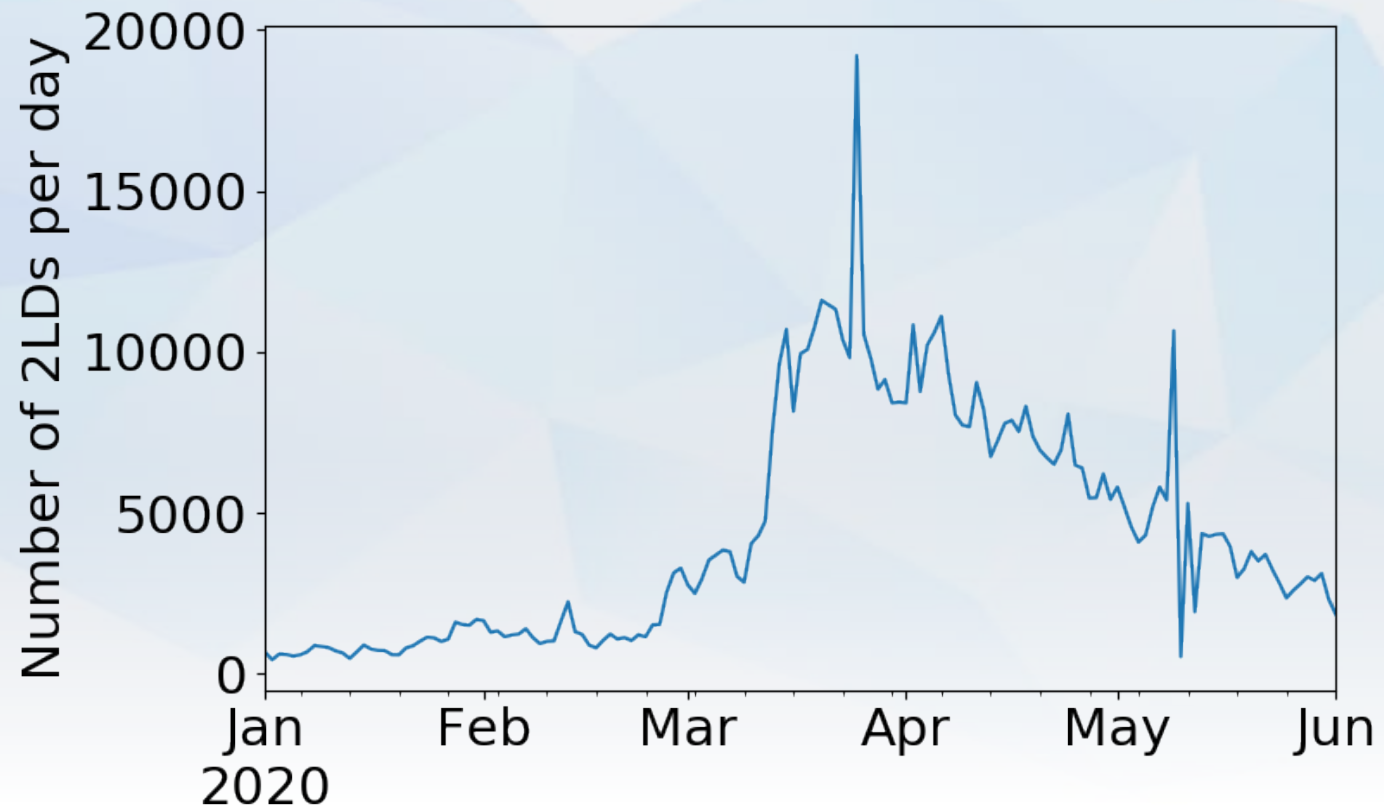
How does our identification approach work?

- Our approach for identification:
 - Pandemic-related keyword search within zone files (gTLDs + a few ccTLDs)



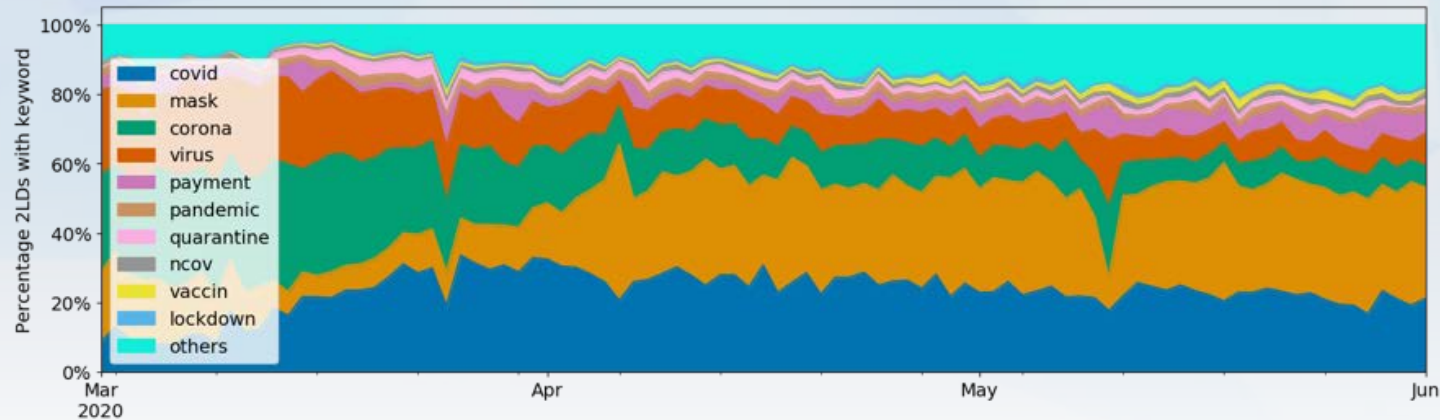
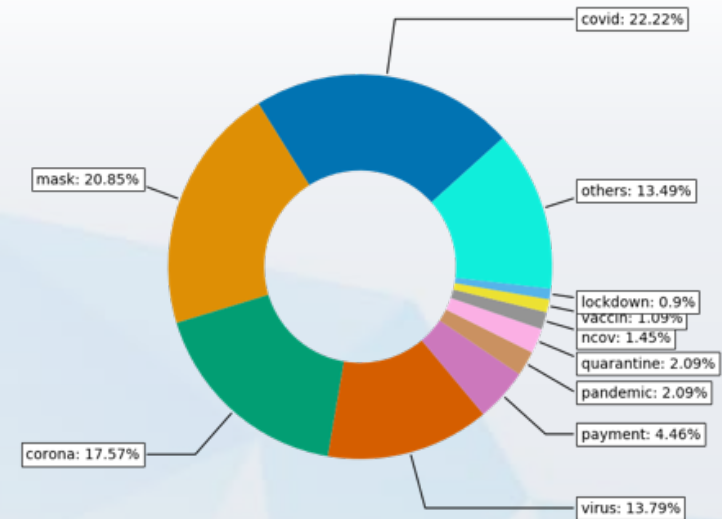
How many domains have we identified?

- 662,111 domains were identified since January 2020



What keywords do these domains contain?

- Most of the domains related to 3 keywords
 - 4 keywords account for 73% of the domains
 - Different keywords categories:
 - Disease name (covid, ncov, sars, ...)
 - Pandemic countermeasures (mask, lockdown, quarantine,...)
 - Collateral (zoom, webex, conference, ...)
 - Significant number of domains matches non-English terms



Language	%Domains
English	94,21%
German	2,13%
French	1,26%
Spanish	0,71%
Dutch	0,68%
Turkish	0,59%
Italian	0,14%
Hindi	0,11%
Malay	0,08%
Japanese	0,04%
Portuguese	0,02%
Chinese	0,02%

So far so good...

This is “data”, **not** “intelligence”

There will be benign domains, unrelated domains, defensive registrations, parked domains... along with anything malicious


What **evidence** can we find, do we trust it?

API calls – VirusTotal

The screenshot displays the VirusTotal domain analysis page. At the top, a navigation bar includes the VirusTotal logo, a search bar, and a user profile for 'Siôn Lloyd'. The main content area features a circular gauge on the left showing a score of 11 out of 82, with a 'Community Score' label below it. To the right of the gauge, a red warning icon and text state '11 engines detected this domain'. Below this, a black box represents the domain name. Further right, three metadata fields are shown: 'Registrar' (undefined), 'Creation Date' (5 days ago), and 'Last Updated' (5 days ago), accompanied by a globe icon. A tabbed interface below these fields has four tabs: 'DETECTION' (selected), 'DETAILS', 'RELATIONS', and 'COMMUNITY'. The 'DETECTION' tab displays a table of engine results.


DETECTION	DETAILS	RELATIONS	COMMUNITY	
AlienVault	⚠ Malicious		CyRadar	⚠ Malicious
Emsisoft	⚠ Phishing		ESET	⚠ Phishing
Fortinet	⚠ Phishing		G-Data	⚠ Phishing
Google Safebrowsing	⚠ Phishing		Kaspersky	⚠ Phishing
Netcraft	⚠ Malicious		Sophos AV	⚠ Malicious
Spamhaus	⚠ Phishing		ADMINUSLabs	✅ Clean
AegisLab WebGuard	✅ Clean		Antiy-AVL	✅ Clean
Artists Against 419	✅ Clean		Avira (no cloud)	✅ Clean
BADWARE.INFO	✅ Clean		Baidu-International	✅ Clean
BitDefender	✅ Clean		BlockList	✅ Clean

API calls - AlienVaultOTX



DashboardBrowse ▾Scan EndpointsCreate PulseSubmit SampleAPI Integration

SEARCHSIGNINLOYD ⚙️ ?



CCTC Top Indicators

MODIFIED 18 MINUTES AGO by Joshua_saxe | Public | TLP: Green

GROUPS: COVID19 Cyber Threat Coalition Vetted, CYBSEC-TIA, Public Library Threat Intelligence

SUBSCRIBE (40) ▾

ADD TO GROUP ▾





DOWNLOAD ▾

EMBED

CLONE

SUGGEST EDIT

Report Spam



Indicators of Compromise (66067)

Related Pulses (2215)


Comments (0)

History (0)

URL (42989)

Domain (8060)











Hostname (15018)



TYPES OF INDICATORS

Show 10 ▾ entries

Search:

TYPE	INDICATOR	TITLE	ADDED ▾	ACTIVE	RELATED PULSES	
domain	tempattidurpasien.com		Jun 3, 2020, 2:17:16 PM		0	 
URL	https://t.co/GppF0yYNAN		Jun 3, 2020, 2:17:16 PM		1	 
URL	https://movemycouch.com/404.shtml		Jun 3, 2020, 2:17:16 PM		0	 
URL	http://www.meduchet.com/crm/21138163051d1d676653c26.71326395install...		Jun 3, 2020, 2:17:16 PM		0	 
URL	https://secure.runescape.com-un.ru/m=weblogin/loginform194,533,474,814...		Jun 3, 2020, 2:17:16 PM		0	 

© COPYRIGHT 2020 ALIENVAULT, INC. | LEGAL | STATUS | DO NOT SELL MY PERSONAL INFORMATION

API calls - phishtank

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

Signed in: [slonlloyd](#) | [My Account](#) | [Sign Out](#)


PhishTank® Out of the Net, into the Tank.

[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

Submission #6604832 is currently ONLINE


Submitted May 31st 2020 9:02 PM by [N1Antifraude](#) (Current time: Jun 1st 2020 11:17 AM UTC)

https: [REDACTED]

 **Verified: Is a phish** [Next unverified phish >](#)
As verified by [paulch](#) [NotBuyingIt](#) [Vasily1](#) [emidaniel](#) [Romantic kiss](#) [PhishKiller73](#)

Is a phish **100%**
Is NOT a phish 0%

[Screenshot of site](#) [View site in frame](#) [View technical details](#) [View site in new window](#) [Something wrong with this submission?](#)



API calls – google safe browsing



The site ahead contains malware

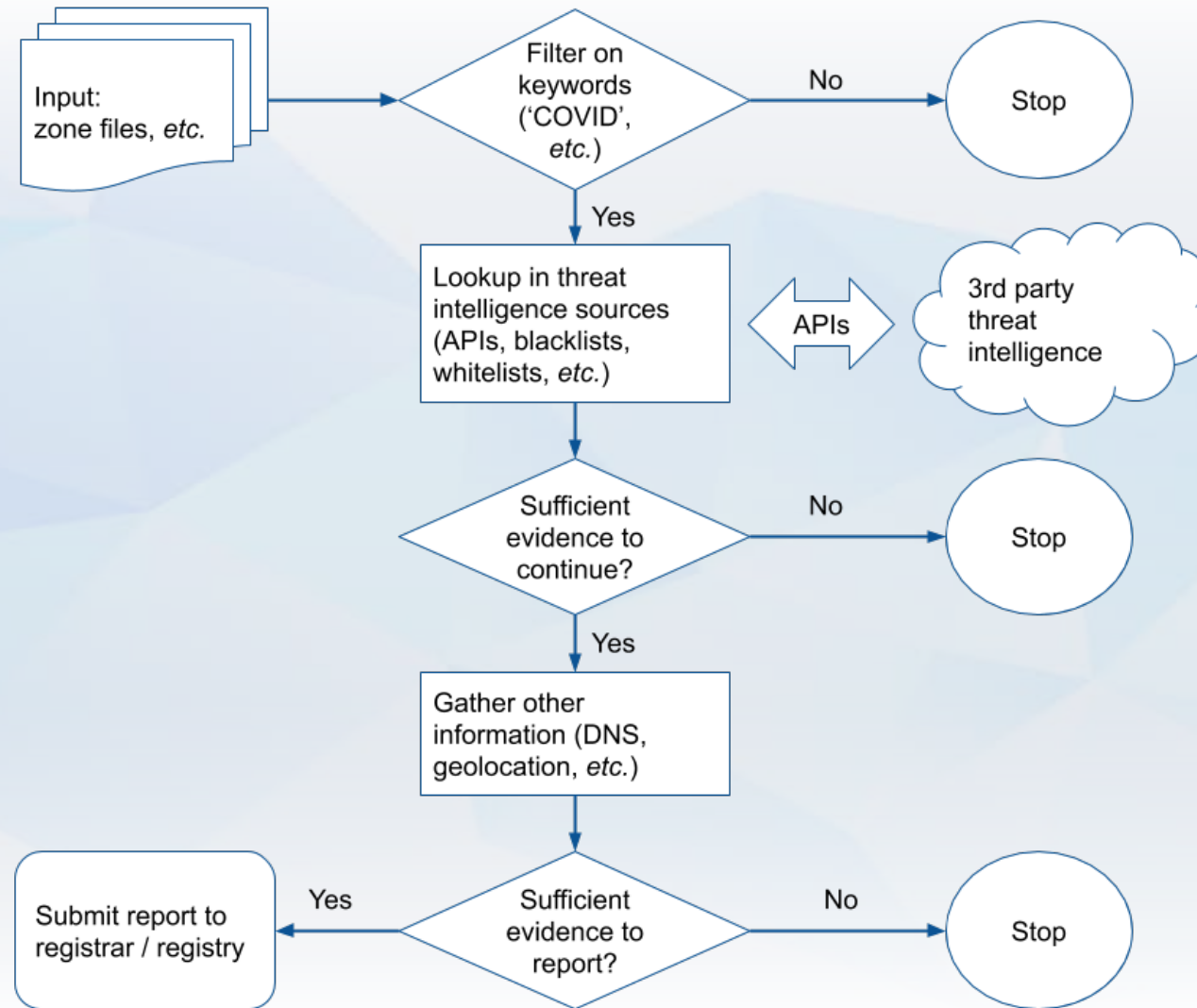
Attackers currently on **malware.testing.google.test** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

☐ Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

[Back to safety](#)

Reporting Data Flow



Roughly an order of magnitude lost at each gate:

- Thousands of registrations per day
- Some reports on hundreds
- Sufficient evidence on tens

Conclusion

Conclusion

Sure, there is bad stuff out there

BUT; it is not anywhere near as bad as some figures would suggest

OFFICIAL



National Cyber Crime Unit COVID-19 Domains

Chris Lewis-Evans – Lead Cyber Protect

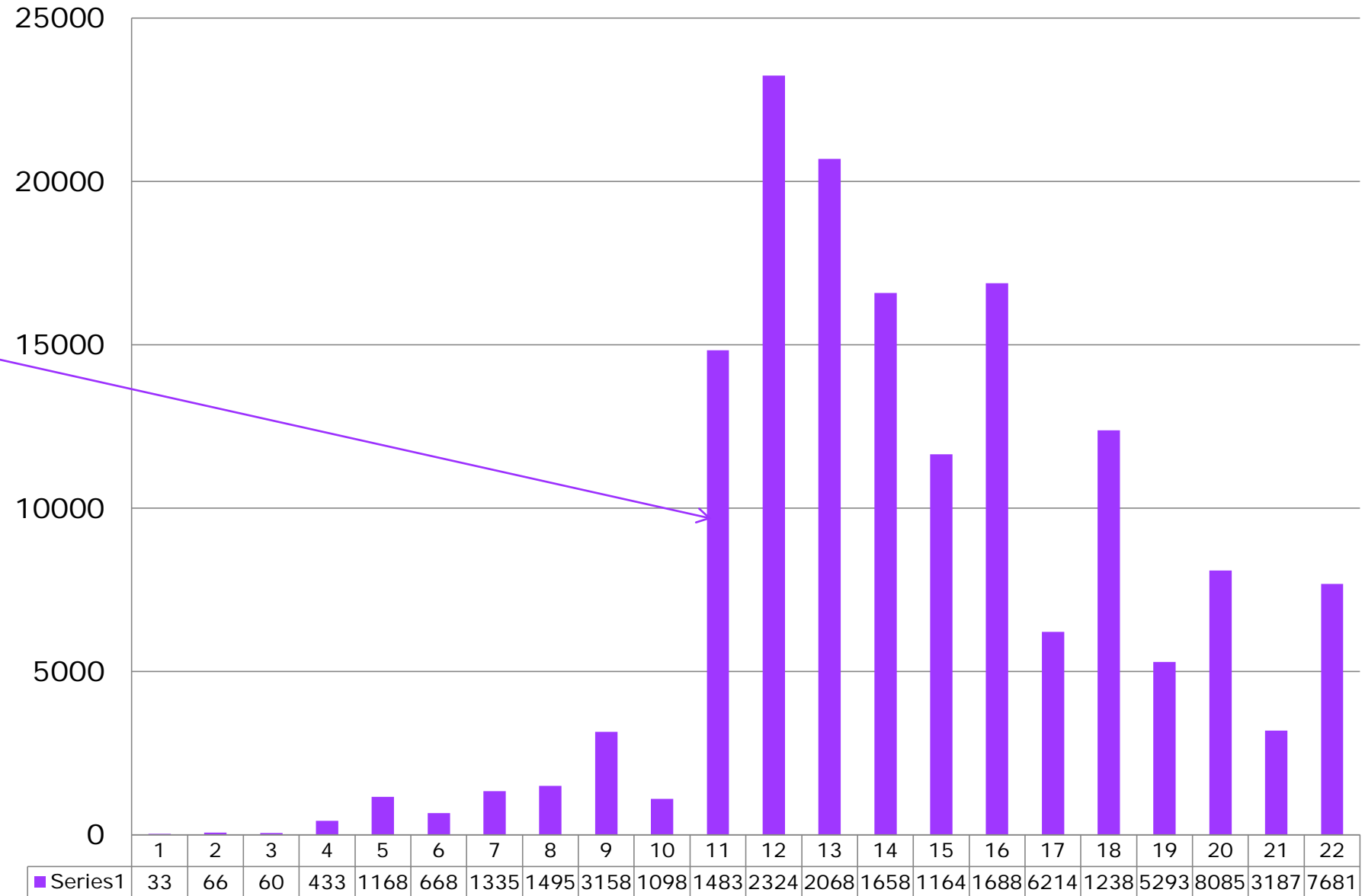
Initial encounters

- Receiving high numbers of reported domains
- Receiving repetitive notifications
- Majority of domains parked
- Cross Governmental response
 - Healthcare Regulatory Bodies
 - Trading Standards
 - Tax and welfare bodies

Co-vid related Domains registered per Week

source: holdintegrity.com

Week 11 first full country
enters lockdown



Activity

- Interaction with ccTLD around enhanced validation
- Information sharing with a number of rr/ry's
- Validating Maliciousness across all identified domains
- Providing evidential packages for suspension
- Over 2000 reports of COVID related scams

Outcomes and Work in Progress

- Provided single point of contact for UK
- Received Co-vid contact points
- No new criminal groups, tools or vulnerabilities
- Educational material to prevent and protect the public
- Need for better information sharing mechanism
- Arrests and disruptions

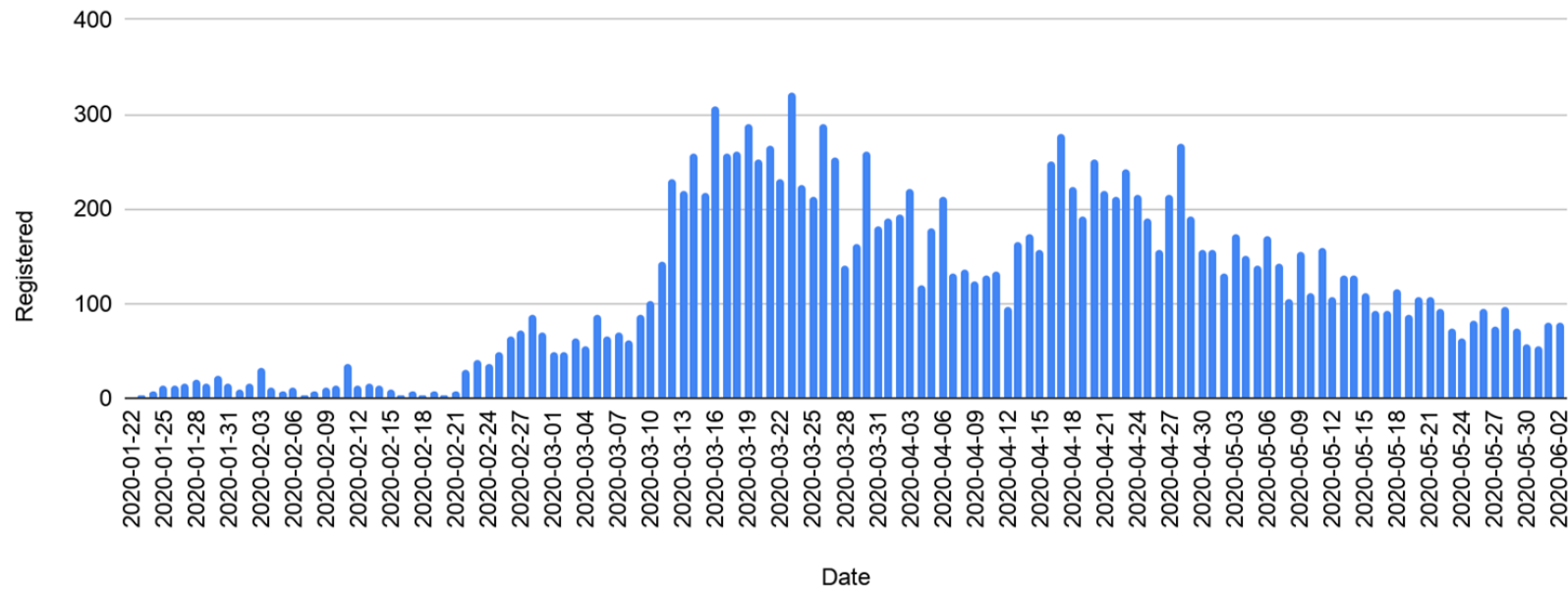
The background is a solid blue color. Scattered around the central text are several large, 3D, blue letters. These letters include 'O', 'C', 'U', 'S', and 'K'. They are positioned at various angles and depths, creating a sense of three-dimensionality. The central text 'tucos' is white and has a slight shadow, making it stand out from the blue background and the other 3D letters.

tucos

COVID-19 and Domain Registration

Daily COVID-19 Registrations

COVID-19 Registrations by Day



First COVID-19
related domain
registered on
2020-01-22

“Oh shit” on
2020-03-15

Manual Review for Harm Process

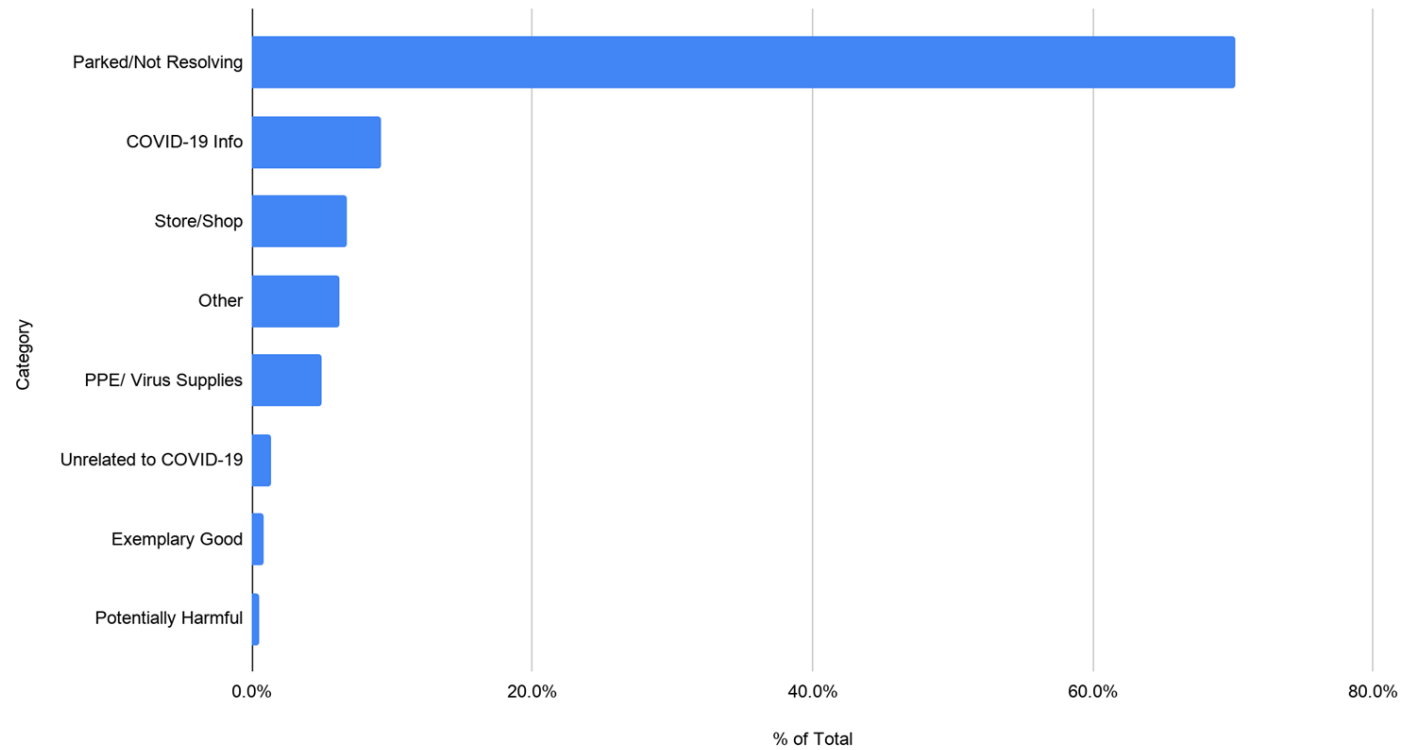
- Realization that this is an *exceptional* circumstance
- Run COVID-19 related keyword search on new registrations (%covid%,%corona%, ...)
- Load daily keyword matches in to Google Sheet
- Review and categorize
- Compliance team investigates potential harm
- Harm: Leaning on DNS Abuse Framework - threats to human safety foremost, more broadly anything our team found concerning

Manual Review Results

Category	% of Total
Parked/Not Resolving	70.1%
COVID-19 Info	9.2%
Store/Shop	6.7%
Other	6.3%
PPE/ Virus Supplies	5.0%
Unrelated to COVID-19	1.3%
Exemplary Good	0.9%
Potentially Harmful	0.5%



% of Total vs. Category



The Good

- <https://sacoronavirus.co.za/> - Official South African COVID-19 site
- <https://spreadartnotviruses.com/> - COVID-19 Art Project
- <https://covidsurvey.ca/> - York University Study

The Bad

- Personal information gathering
 - Anonymous exposure notification
 - Fake tests & fake cures
 - Unclear boundaries: vitamin C
 - Questionable products
 - COVID-19 resistant tents
 - PPE opportunists
-
- No examples of coordinated mis- or dis-information

Resellers

- Worked with larger resellers to share information
- Resellers have more tools and customer relationships to leverage
- Some implemented blanket bans on COVID-19 related terms

The Difficulty of Manual Review

- DNS Abuse was well covered
- Content abuse is difficult because:
 - Requires tooling Registrars don't necessarily have
 - Content changes constantly
 - Lack of authorities available to review potential harm
 - Harm is difficult to identify in practice
 - Totally outside the realm of our expertise and purview



Thank you

gbunton@tucows.com

tucows.com

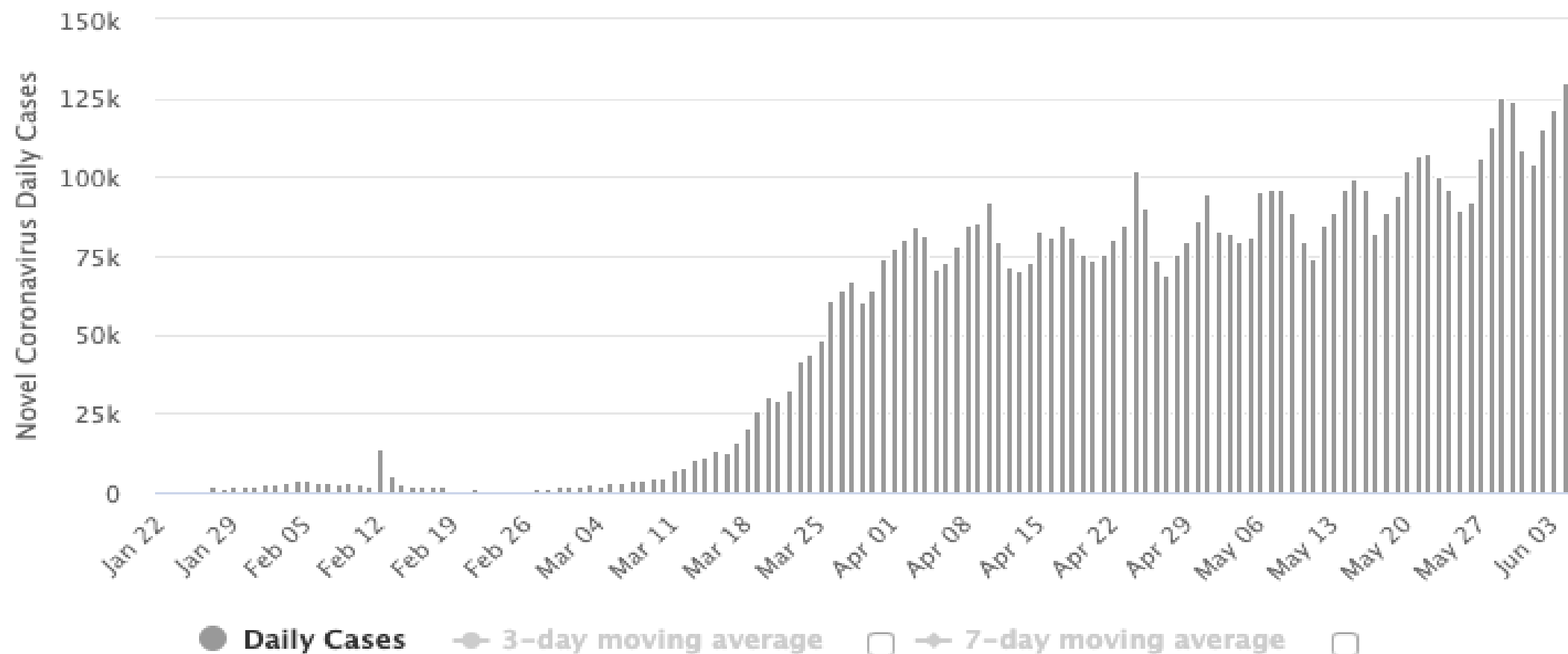


Afilias Anti-Abuse vs COVID-19

James M. Galvin, Ph.D.
Afilias, Inc.

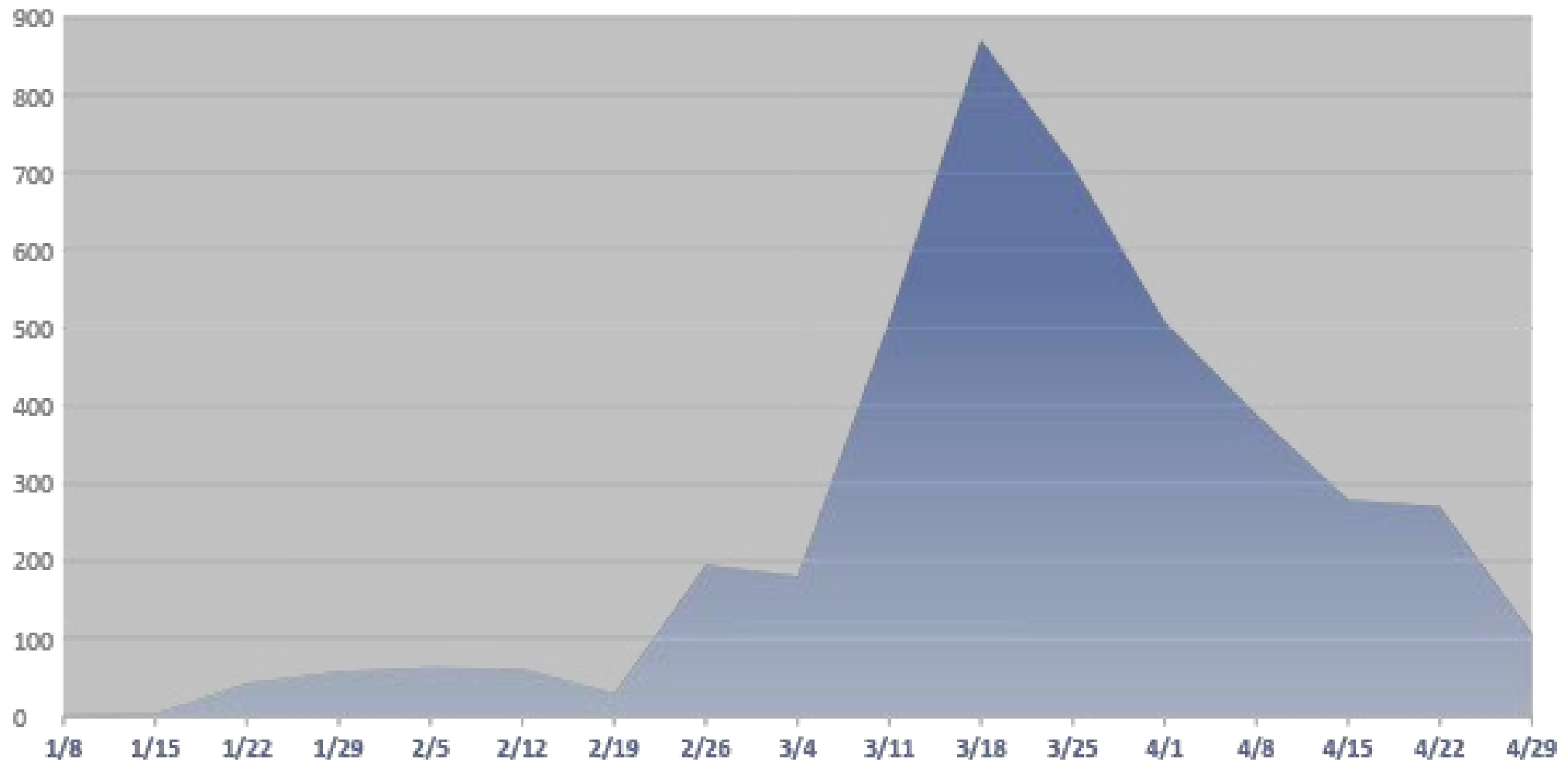
Daily New Cases

Cases per Day
Data as of 0:00 GMT+0



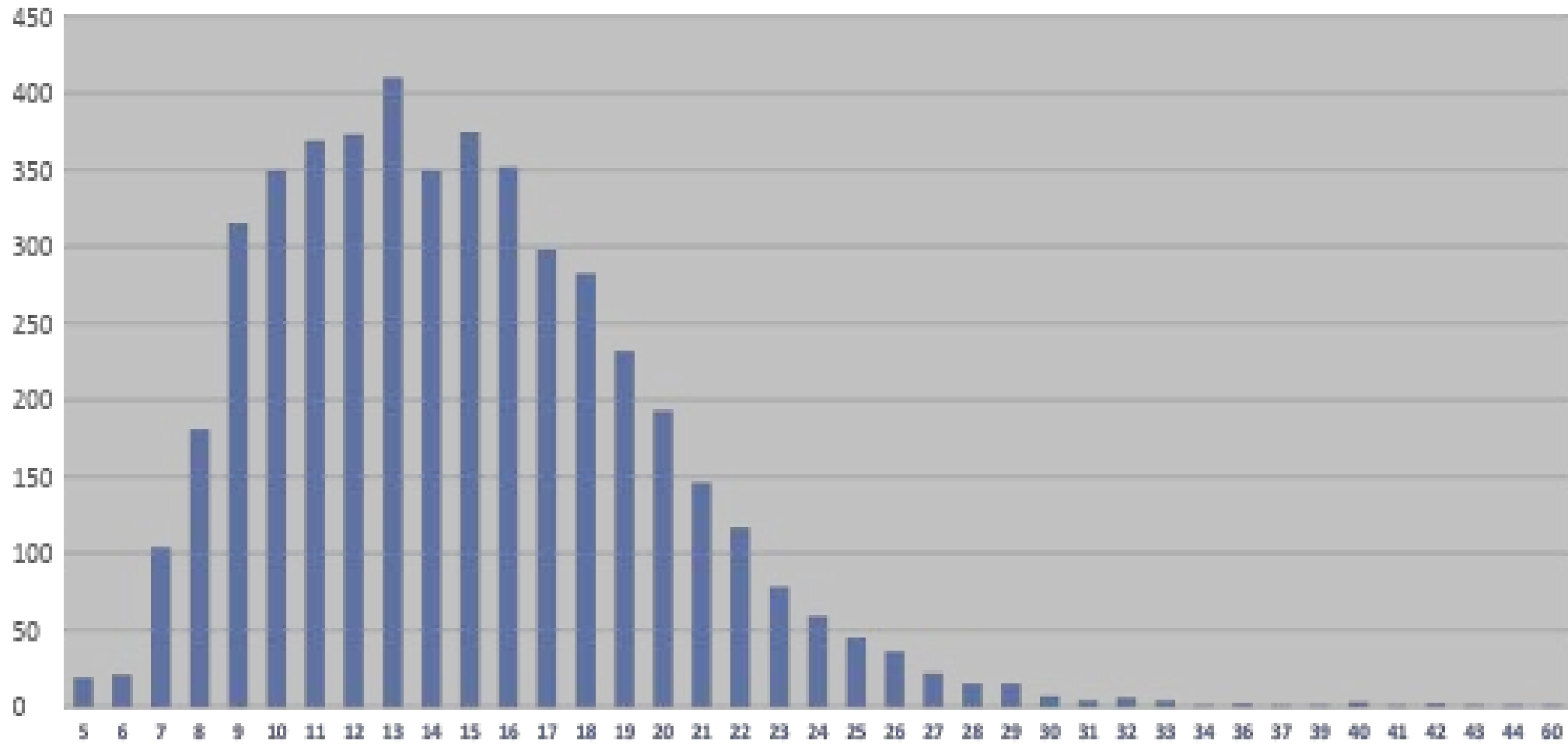
Source: **Worldometer** - www.worldometers.info 

Weekly COVID Related Registrations: Afilias TLDs



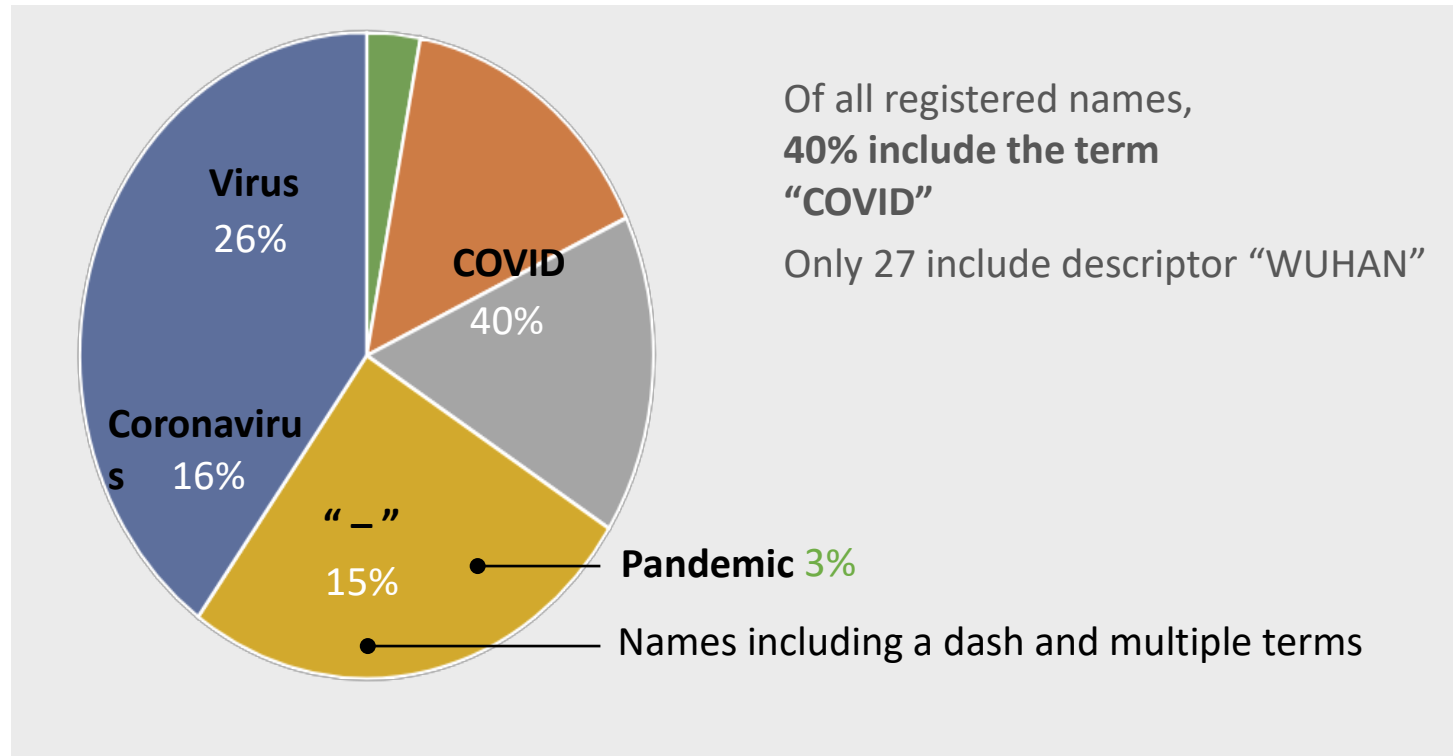
Based on 4,792 registrations with COVID-related names registered across 25 Afilias TLDs

COVID Names Peak at 13 Characters



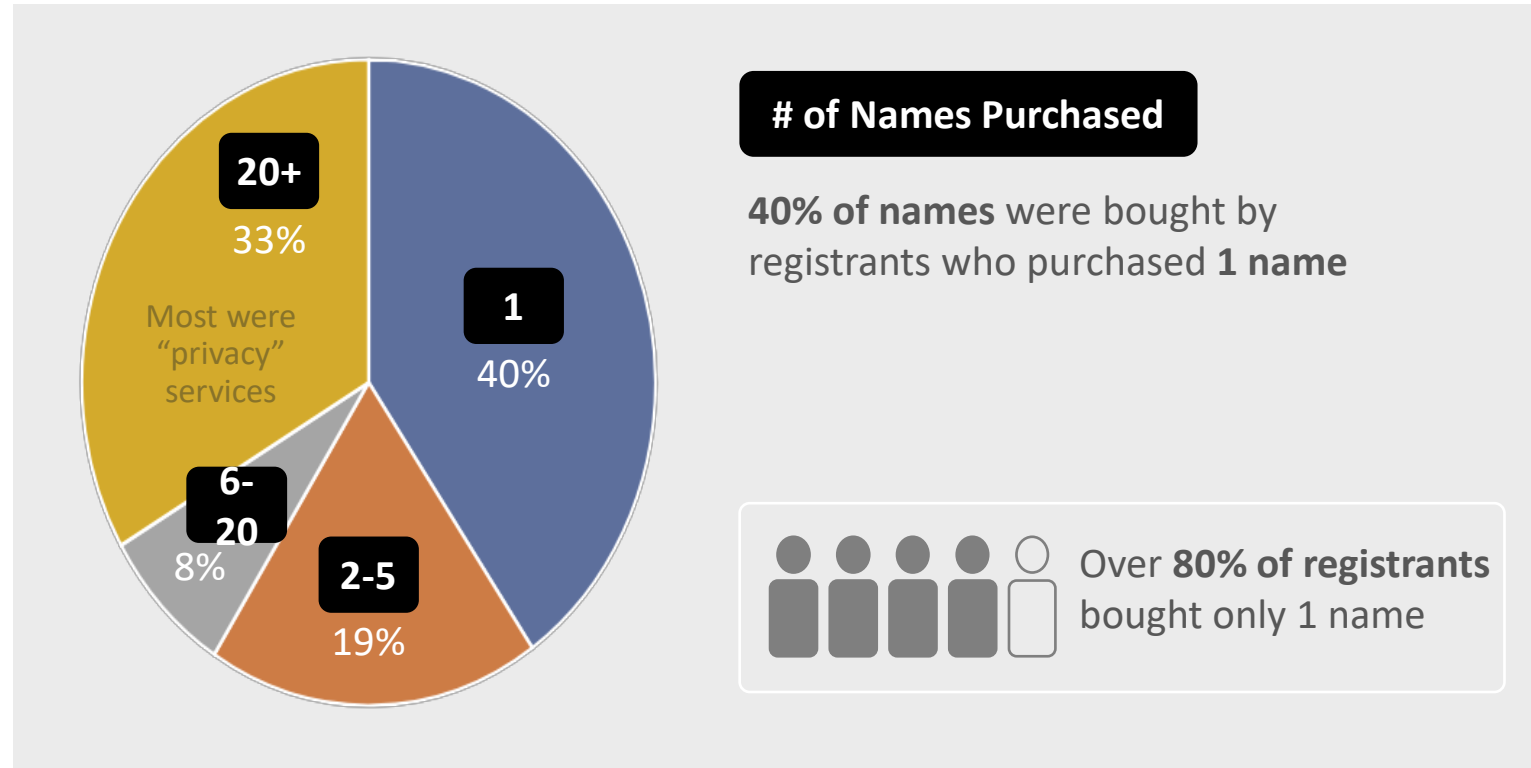
Based on 4,792 registrations with COVID-related names registered across 25 Afilias TLDs

“COVID” AND “VIRUS” Are Best Descriptors



Based on 4,792 registrations with COVID-related names registered across 25 Afiliat TLDs

COVID Registrants Bought Single Names

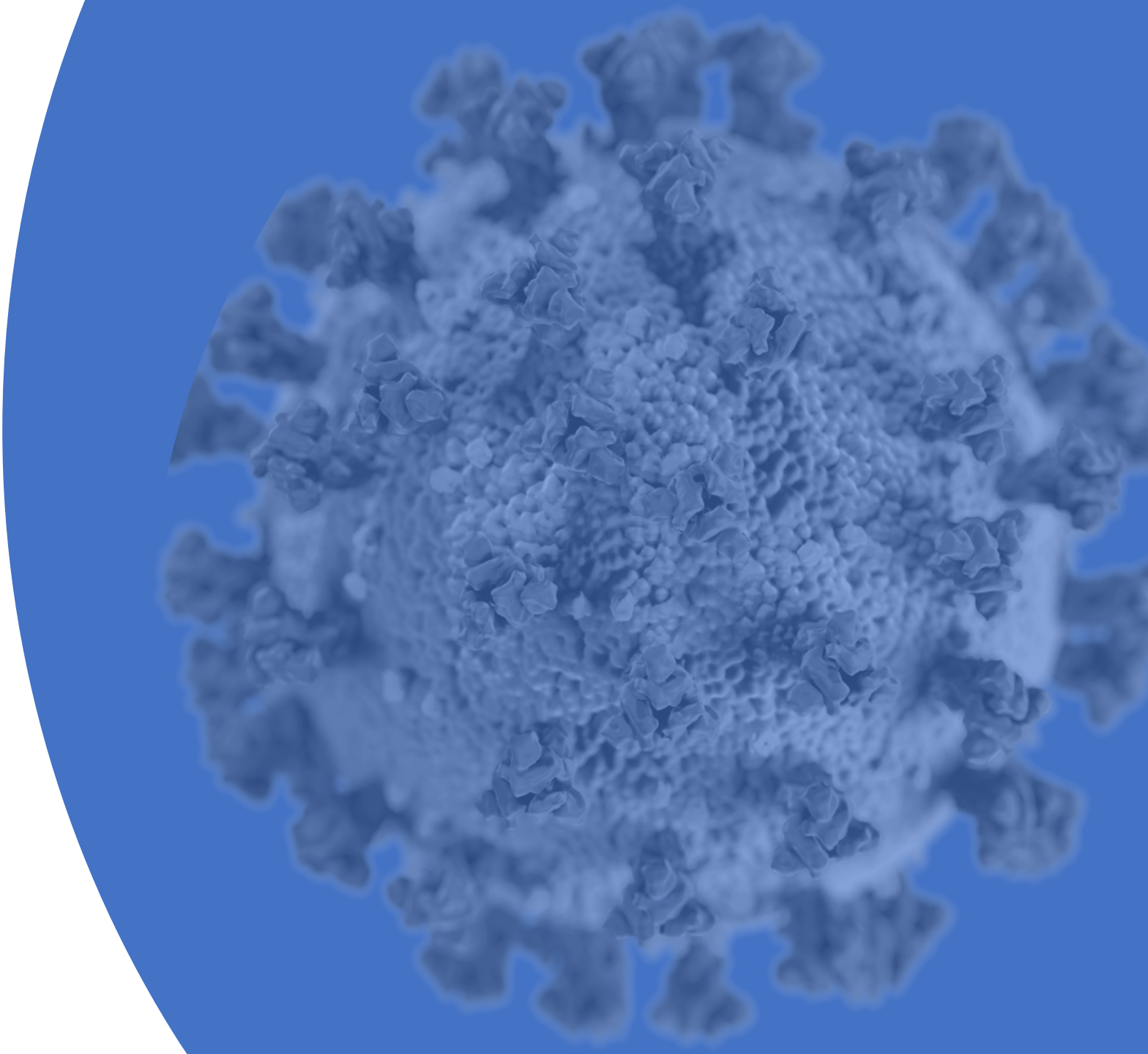


Based on 4,792 registrations with COVID-related names registered across 25 Afiliis TLDs



COVID Domains

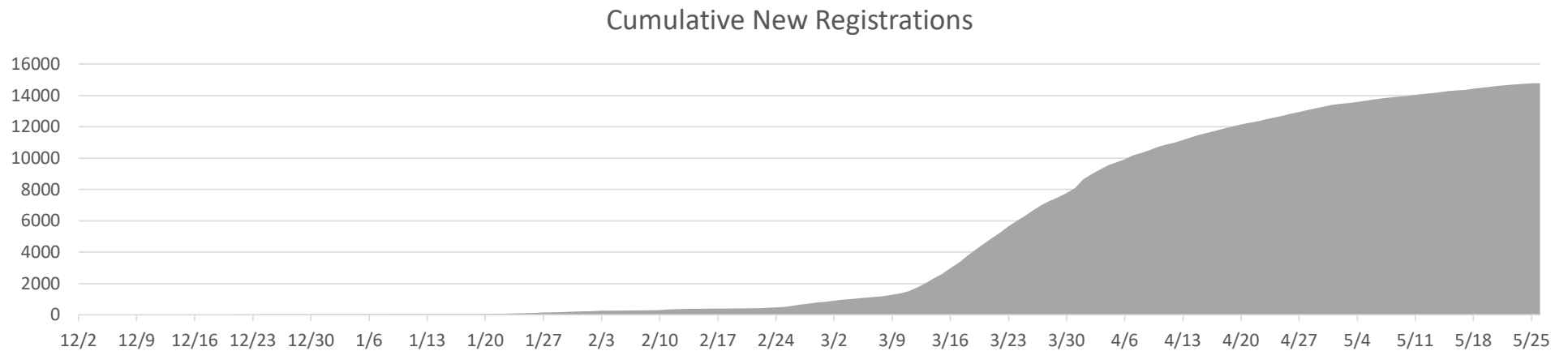
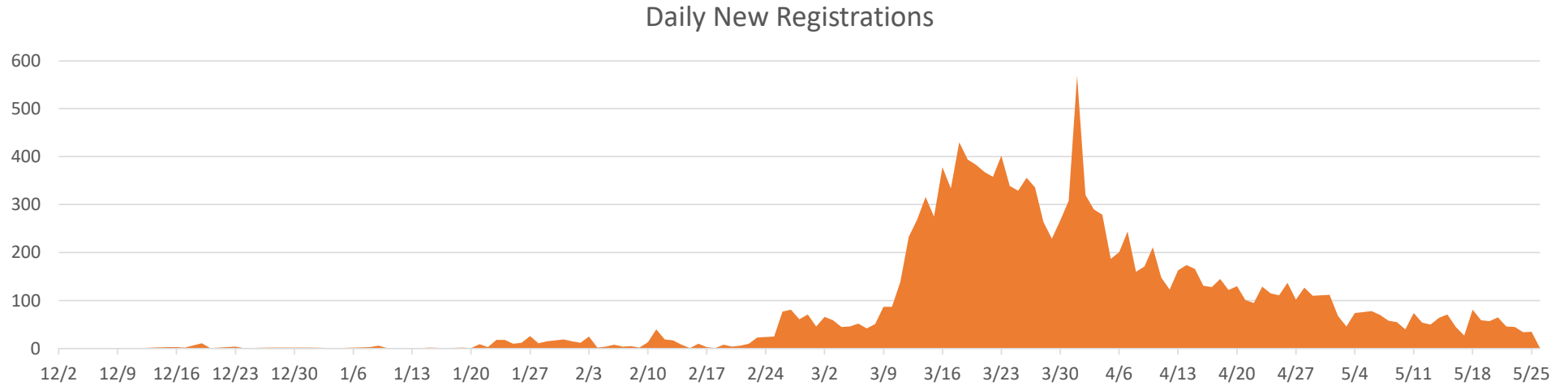
Brian Cimbolic, General Counsel,
PIR



Monitoring Begins

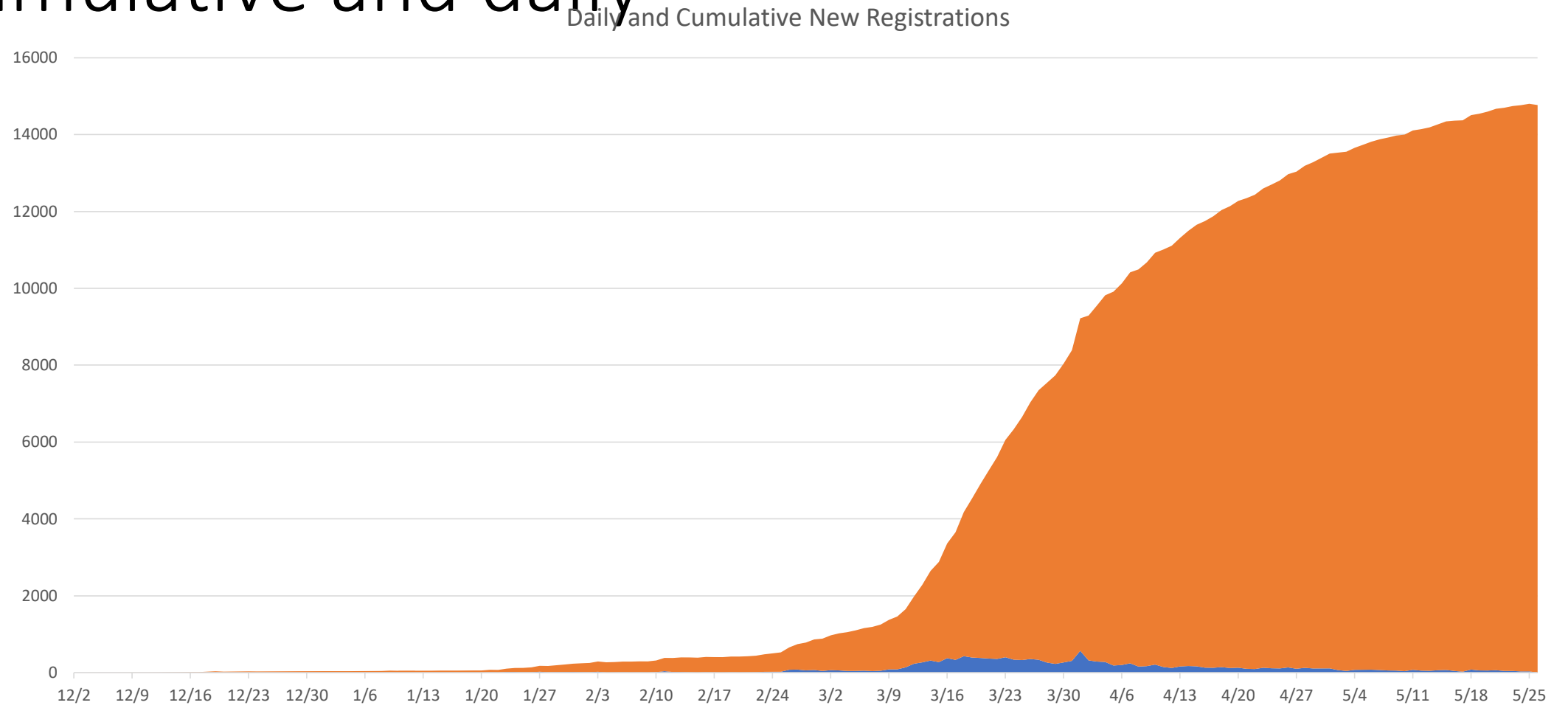
- Early March, spike in registrations related to COVID became clear.
- Concern regarding abuse/phishing related to these names.
- Also concerned regarding things like fake “cures” and “vaccines.”
- Began screening certain keywords in registration.
- Act on limited instances of domains pursuant to our Anti-Abuse Policy. Informed by:
 - Framework to Address Abuse
 - Anti-Abuse Principles

14.7k ORG COVID-related DOMAIN names



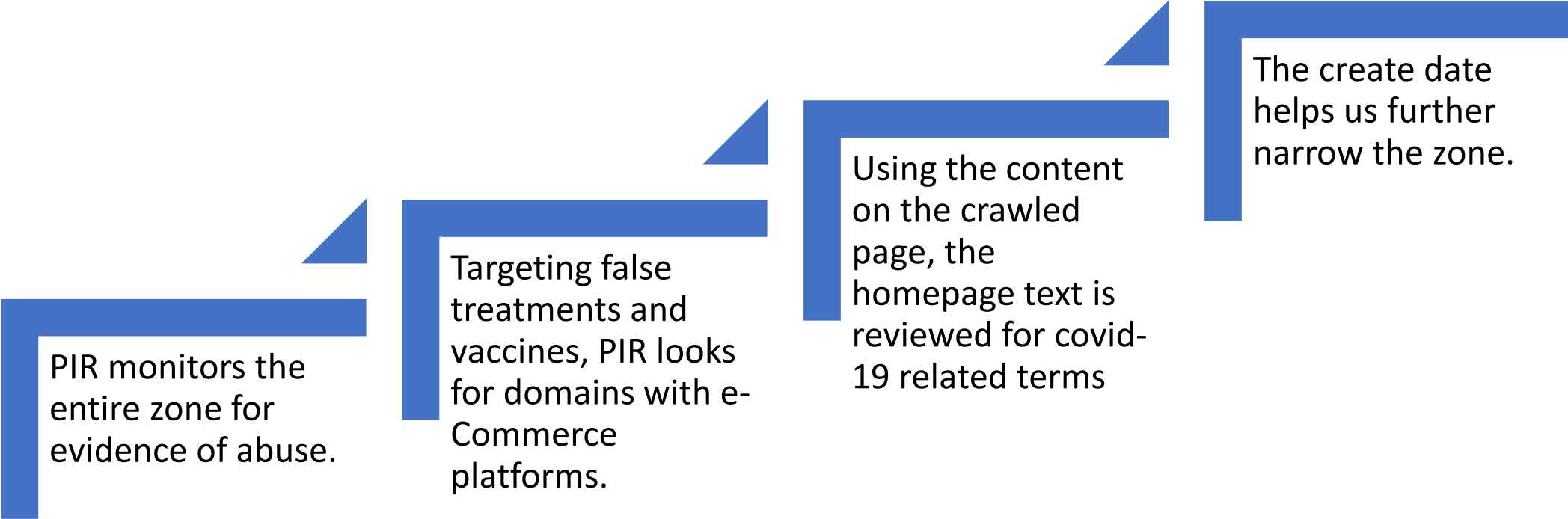
Public Interest Registry

Cumulative and daily



Public Interest Registry

.ORG ABUSE MONITORING



PIR monitors the entire zone for evidence of abuse.

Targeting false treatments and vaccines, PIR looks for domains with e-Commerce platforms.

Using the content on the crawled page, the homepage text is reviewed for covid-19 related terms

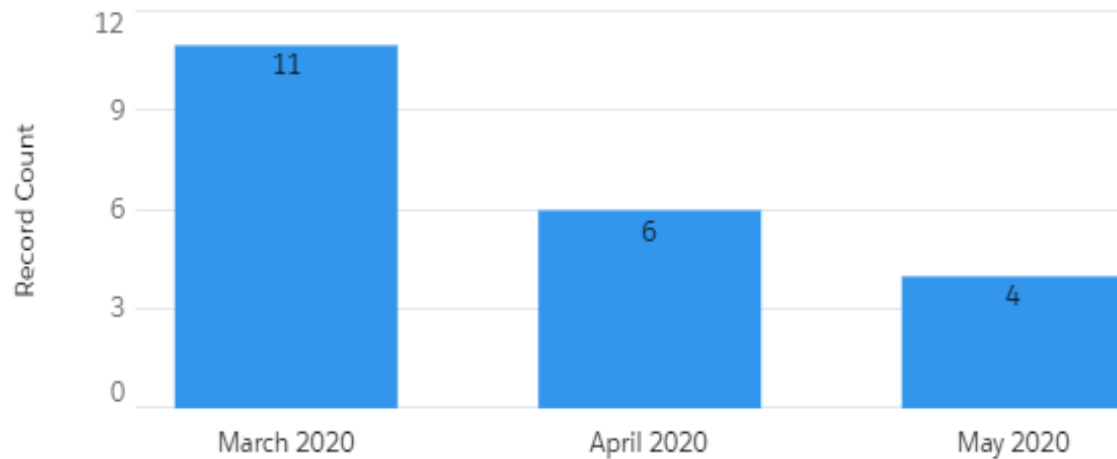
The create date helps us further narrow the zone.

Covid-19 Domain Abuse Tracker

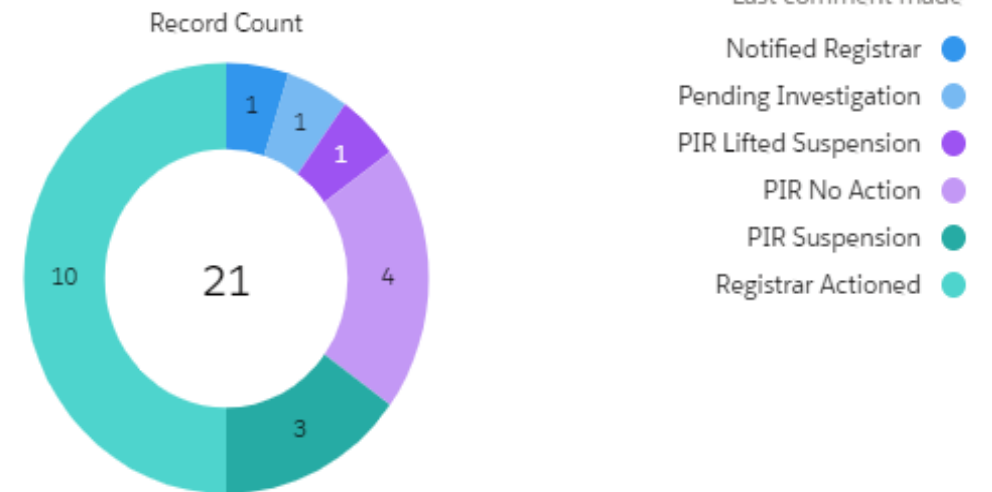
Potentially abusive COVID-19 Names identified and Investigated - Total: 21

COVID-19 Action

Abuse - COVID



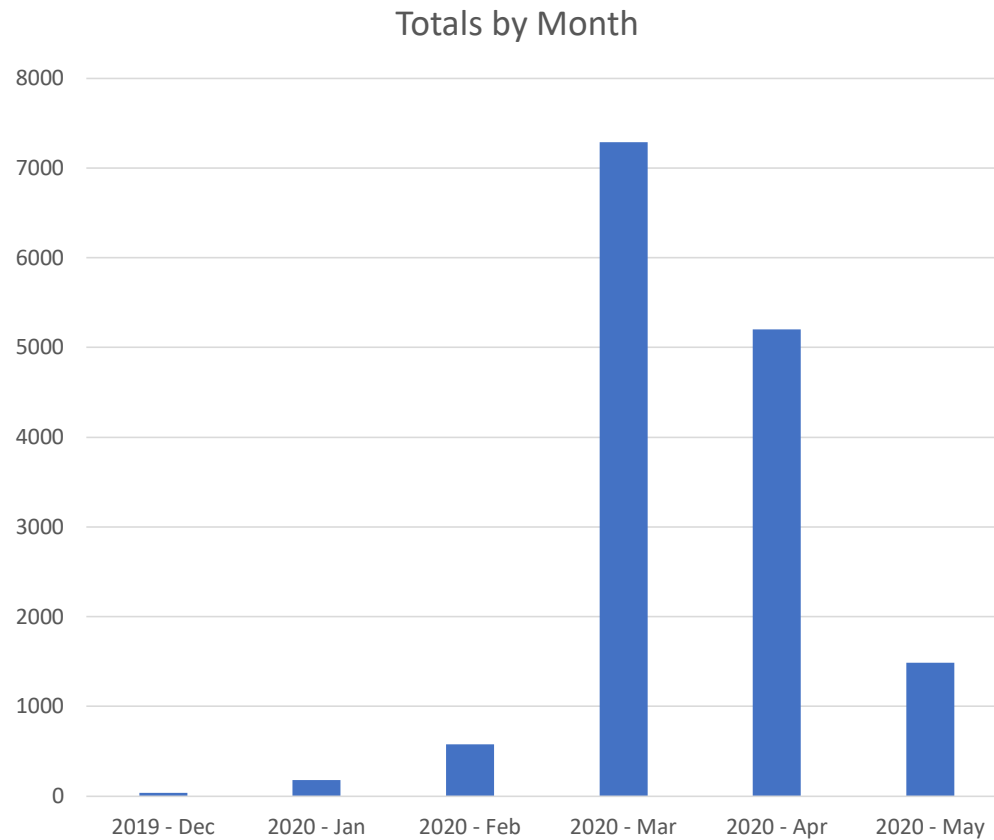
Abuse - COVID Action 2020



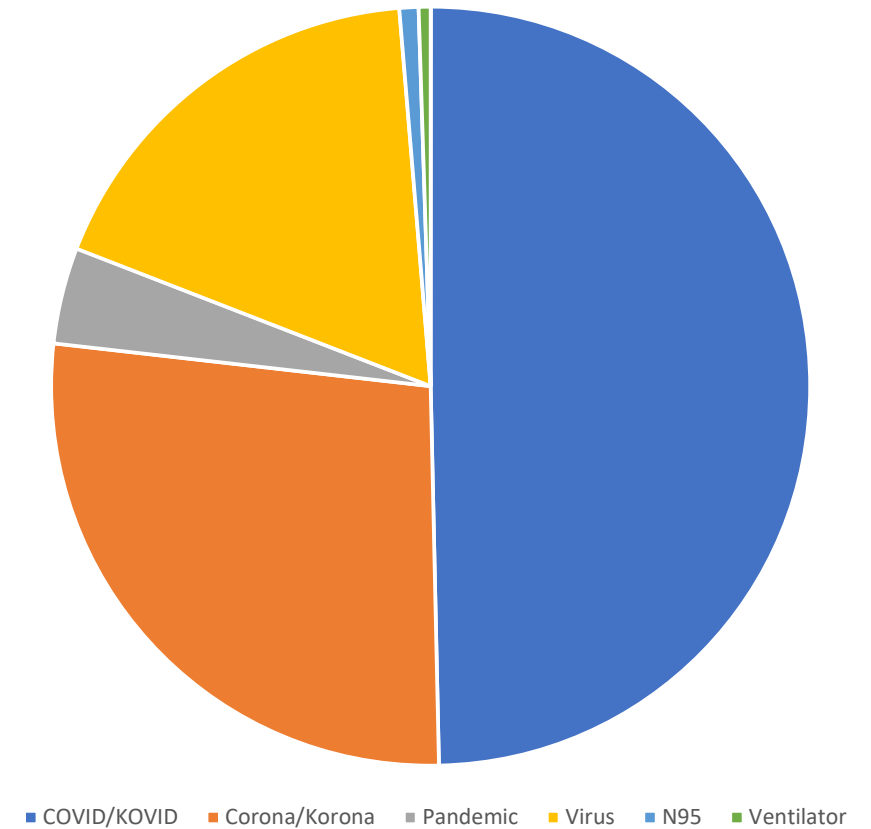
* Registrar Actioned – Registrar actioned the domain name by Suspending, Parking the Site or Deleting the domain name
PIR No Action – Domain Investigated and found to be Legitimate – No Further action taken by PIR

Registration Trends

Monthly New Creates



Common Keywords



Trends Observed

- Keywords: corona, korona, covid, kovid, virus, pandemic.
 - Small number of n95, ventilator included in grand total

- Additional terms have about 50-200 domains related to them.
 - Flatten the curve and social distancing, PPE, test kits, stimulus, Fauci, Cuomo
- Some of the domains ultimately flagged for abuse did not have any direct keywords whatsoever:
 - 6 of the 21 do not have COVID Related domain names (ex. give4cdcf.org, gatesfonudation[.]org)