ICANN 68
VIRTUAL POLICY FORUM

How BEST to participate?

- ADIGO Dial-in numbers: https://www.adigo.com/icann
- Zoom Dial-in numbers: https://icann.zoom.us/zoomconference

- Languages Available: English, Français, Español, 中文, العربية, Русский, Português
- Participation How-To Guide: https://68.schedule.icann.org/participation-tools
- Congress Rental Network Mobile App Download: https://urlgeni.us/ICANN68-GET-APP
  - Token: ICANN68-GAC

If you want your COMMENTS/QUESTIONS to be read out:

- Start your sentence with <QUESTION> and end it with <QUESTION>
- Start your sentence with <COMMENT> and end it with <COMMENT>

Review our Expected Standards of Behavior when participating in ICANN Meetings.

Go to:
http://go.icann.org/expected-standards

Review the ICANN Community Anti-Harassment Policy when participating in ICANN Meetings.

Go to:
http://go.icann.org/anti-harassment

Do you have a question or concern for the ICANN Ombudsman?

Email ombudsman@icann.org to set up a meeting.

ICANN

DNS Abuse

Gabriel Andrews (US FBI, Public Safety Working Group)
Laureen Kapin (US FTC, Co-Chair GAC Public Safety Working Group)

ICANN68 - GAC Session 2

22 June 2020

ICANN | GAC
Governmental Advisory Committee

Agenda

1. **Lessons Learned from the COVID-19 response**
    - ICANN Stakeholders Perspective
    - Law Enforcement/Public Authority Perspective
2. **Overview of Recent Developments related to DNS Abuse**
    - Definition of DNS Abuse
    - CCT Review Recommendations and New gTLD Rounds
    - Other updates
3. **Next Steps for the GAC**
4. **Relevant ICANN68 Sessions on DNS Abuse**

COVID-19 Response: Lessons Learned

ICANN Industry Stakeholders

- **ccTLD Managers** per Webinar for GAC Members (4-5 June 2020)
  - Proactive registration monitoring and data/identity verification, close cooperation with CERTs and Law Enforcement
  - Low criminal activity within spike of COVID-related registrations
- **gTLD Registries and Registrars** per Contracted Parties Webinar (11 June 2020)
  - Monitoring registrations and content, or blanket bans of terms by proactive parties
  - Action based discretionary means, with willing parties downstream (Rar, Resellers):
    - Industry-led voluntary Framework To Address Abuse
    - Individual Anti-Abuse Policies
  - Very Low % of abuse (~70% parked, 25% legitimate, 0.5% evil)
  - Reported challenges:
    - Volatility of content, and mobility of registration/content (TLD/Rar Hopping)
    - Difficulty in assessing harm, overaggressive blacklist, routing to correct L.E.
    - Not seen by some parties as within purview, expertise, resources or tools

COVID-19 Response: Lessons Learned

ICANN Office of the Chief Technical Officer (OCTO)

- Reported on its activities during the Contracted Parties Webinar (11 June 2020) and a Briefing of the GAC (15 June 2020)
- Expected registration spike as is usual during major events
- Developed a system to identify domain name used for pandemic-related abuse (phishing and malware per ICANN's remit) and report them to relevant parties
- Methodology
  - Matched domains with pandemic-related keywords in multiple languages using TLD zones files (all gTLDs and a few ccTLDs: .ru .se .ee .pф)
  - Looked up records in multiple threat intelligence sources to assess evidence of threat
  - Submitted report to Rar/Ry when enough could be gathered
- Results (as of 31 May)
  - Overall number of malicious domains has not increased due to the pandemic
  - 600K+ pandemic related registration, distrib. proportional to size of TLD/Registar
  - Sufficient evidence of threat and report on tens of domains

COVID-19 Response: Law Enforcement Perspective

Source Data

- Victim reporting to Law Enforcement: www.ic3.gov , FTC, FBI Field Offices
- Trusted Private Sector Partners: Microsoft, PhishLabs, ScamSurvivors

Manual Review

- Read complaints
- Ensure COVID-19 nexus + crime (fraud, malware, phishing)

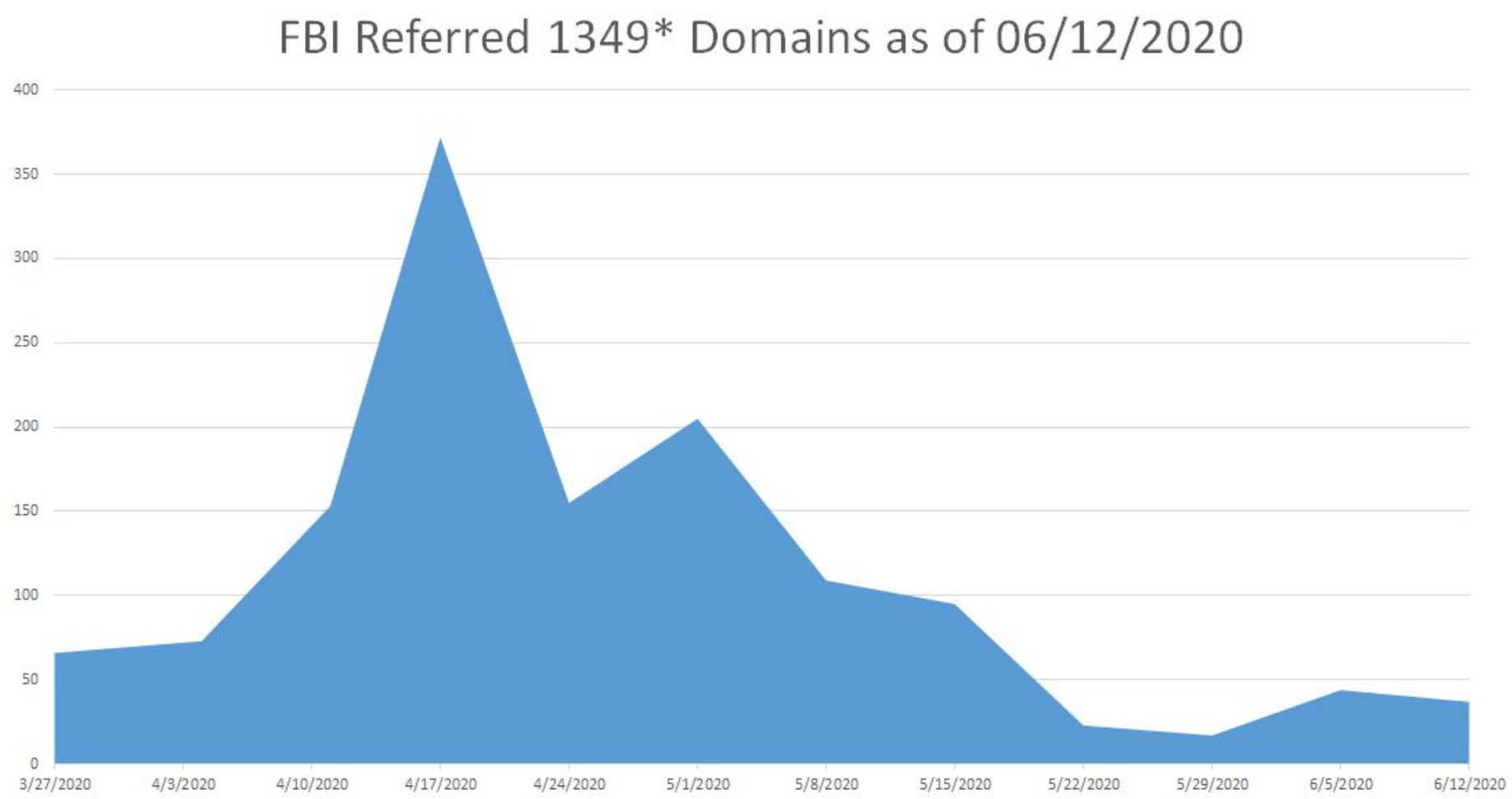
Enrichment

- RiskIQ API >> screenshots, web response codes
- IANA RDAP bootstrap >> RDAP servers by registrar >> EPP codes, registration data
- VirusTotal API >> domain redirects, # of AV engines detecting maliciousness, etc
- DomainTools API >> Risk scores for 1) malicious infrastructure, 2) Phishing, 3) Malware, 4) Spam

Referral

- Weekly
- ICANN "Fully Accredited Registrar" list: https://www.icann.org/registrar-reports/accreditation-qualified-list.html
- Preservation Letters + Memo + Domain List

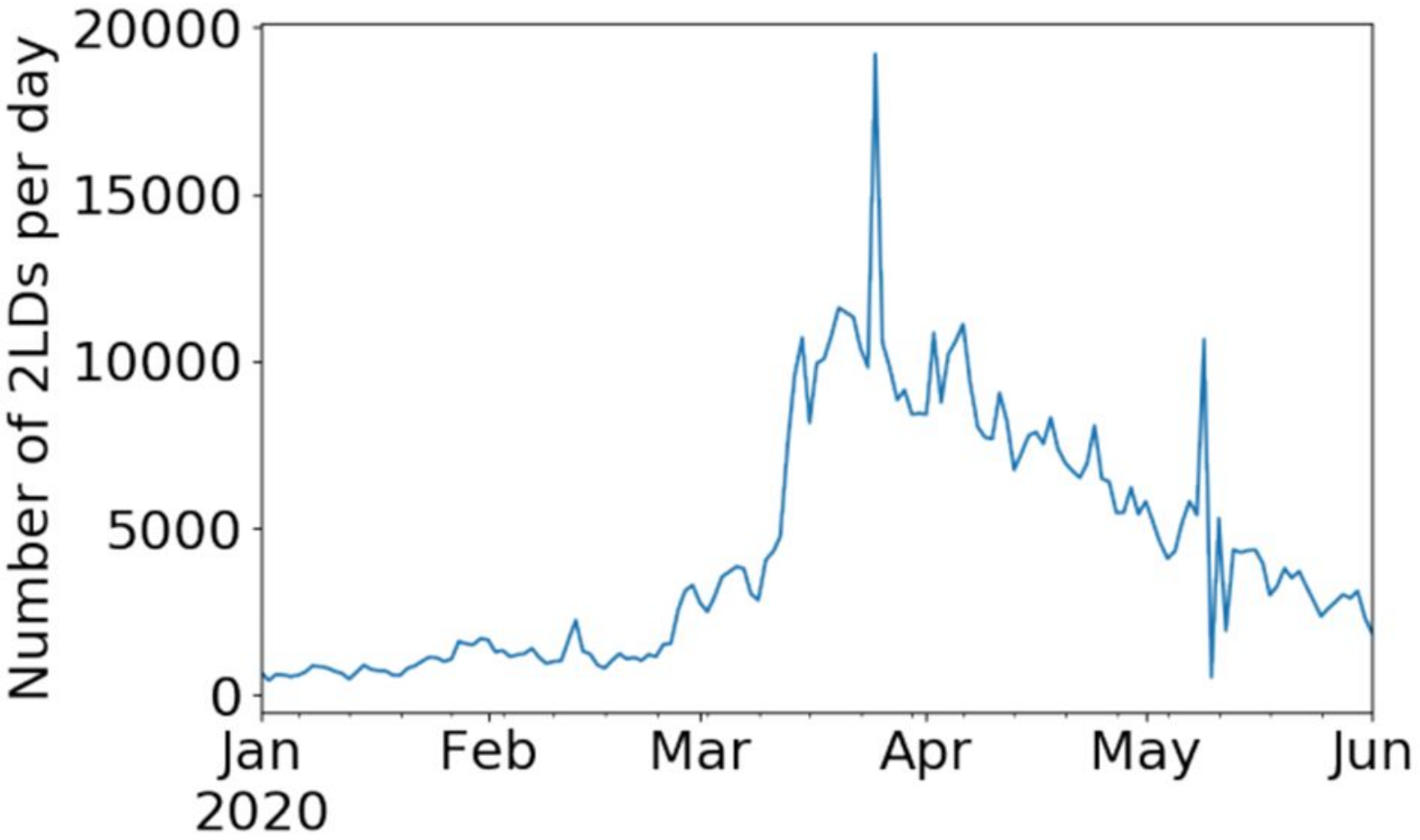
COVID-19 Response: Law Enforcement Perspective



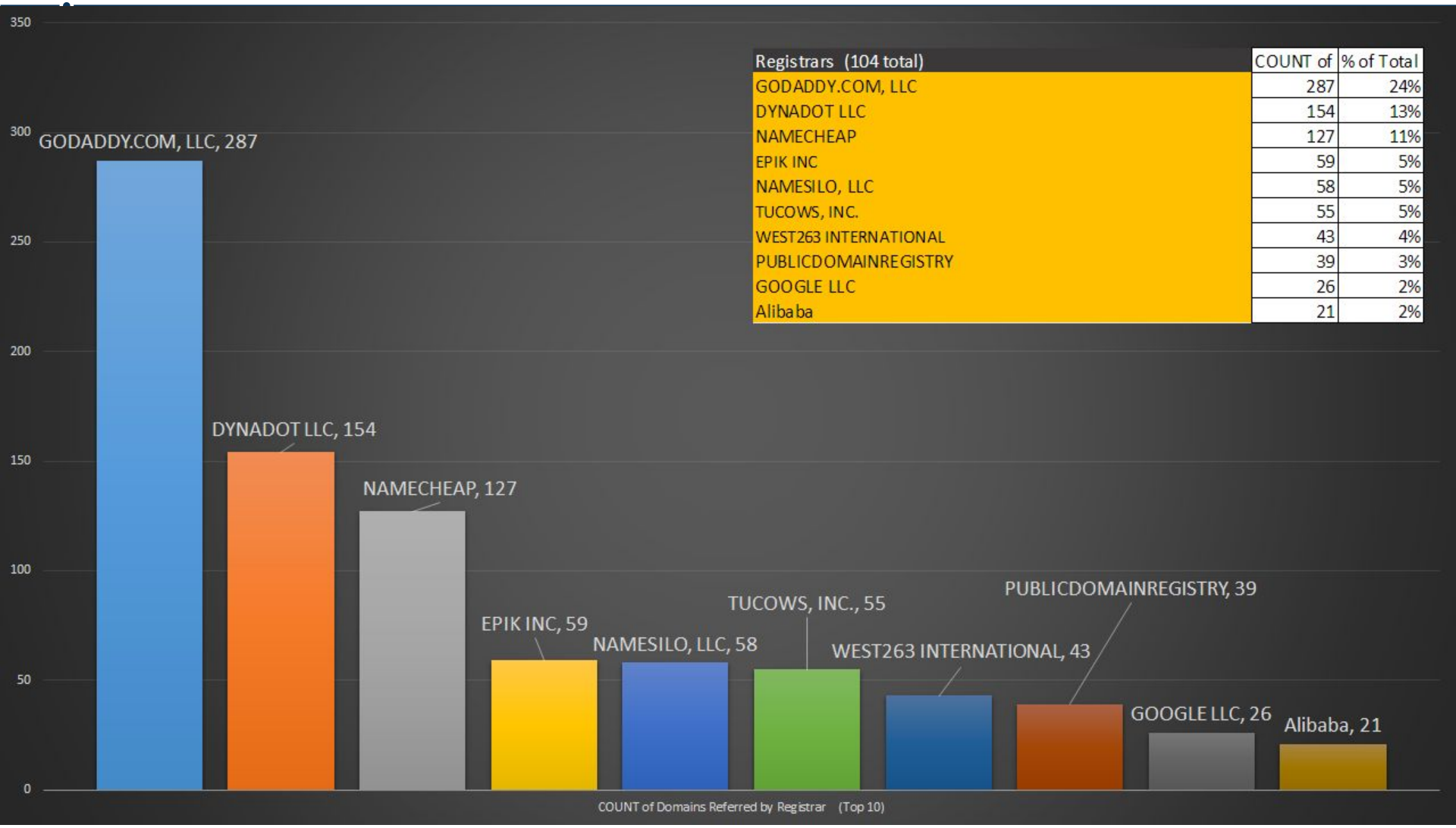
*repeat referrals infrequently occurred if domain was repeatedly reported to FBI, but was not acted upon by registrar

COVID-19 Response: Law Enforcement Perspective

Image Stolen from ICANN OCTO's Presentation:
Registrations (not use) of COVID-19 linked Domains

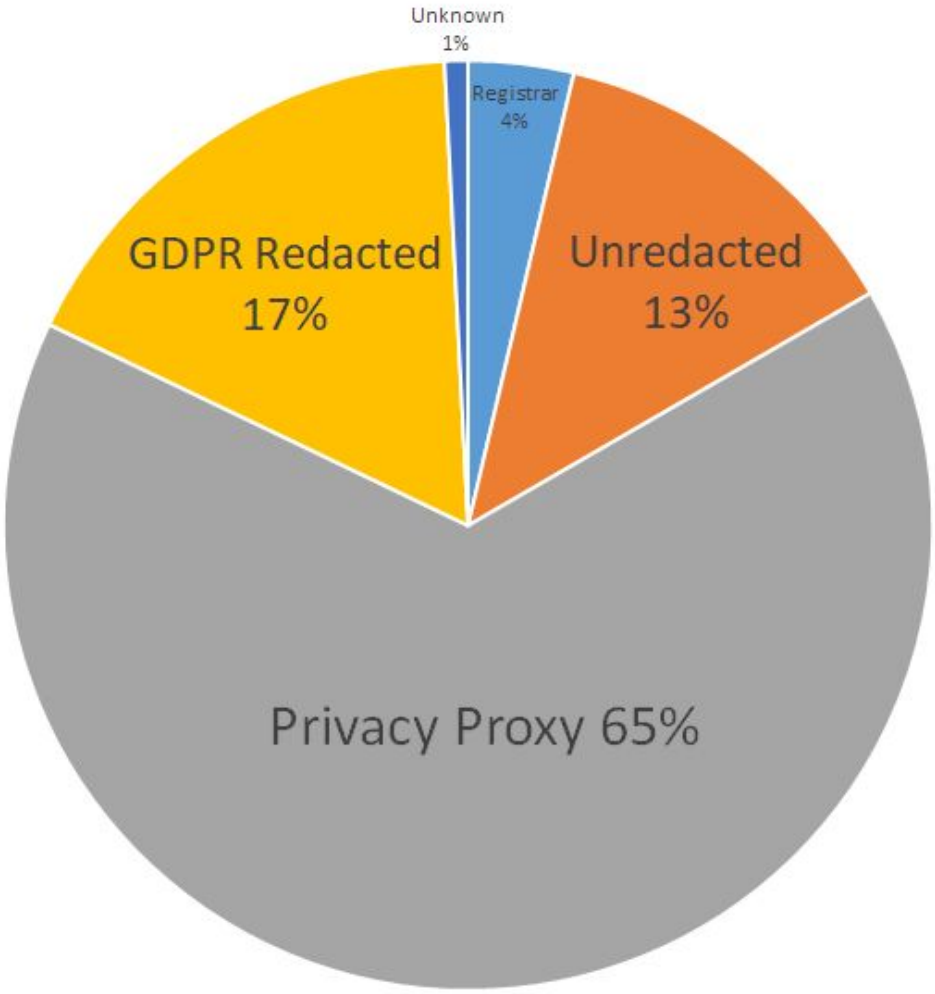


COVID-19 Response: Law Enforcement Perspective



Registrars (104 total)	COUNT of	% of Total
GODADDY.COM, LLC	287	24%
DYNADOT LLC	154	13%
NAMECHEAP	127	11%
EPIK INC	59	5%
NAMESILO, LLC	58	5%
TUCOWS, INC.	55	5%
WEST263 INTERNATIONAL	43	4%
PUBLICDOMAINREGISTRY	39	3%
GOOGLE LLC	26	2%
Alibaba	21	2%

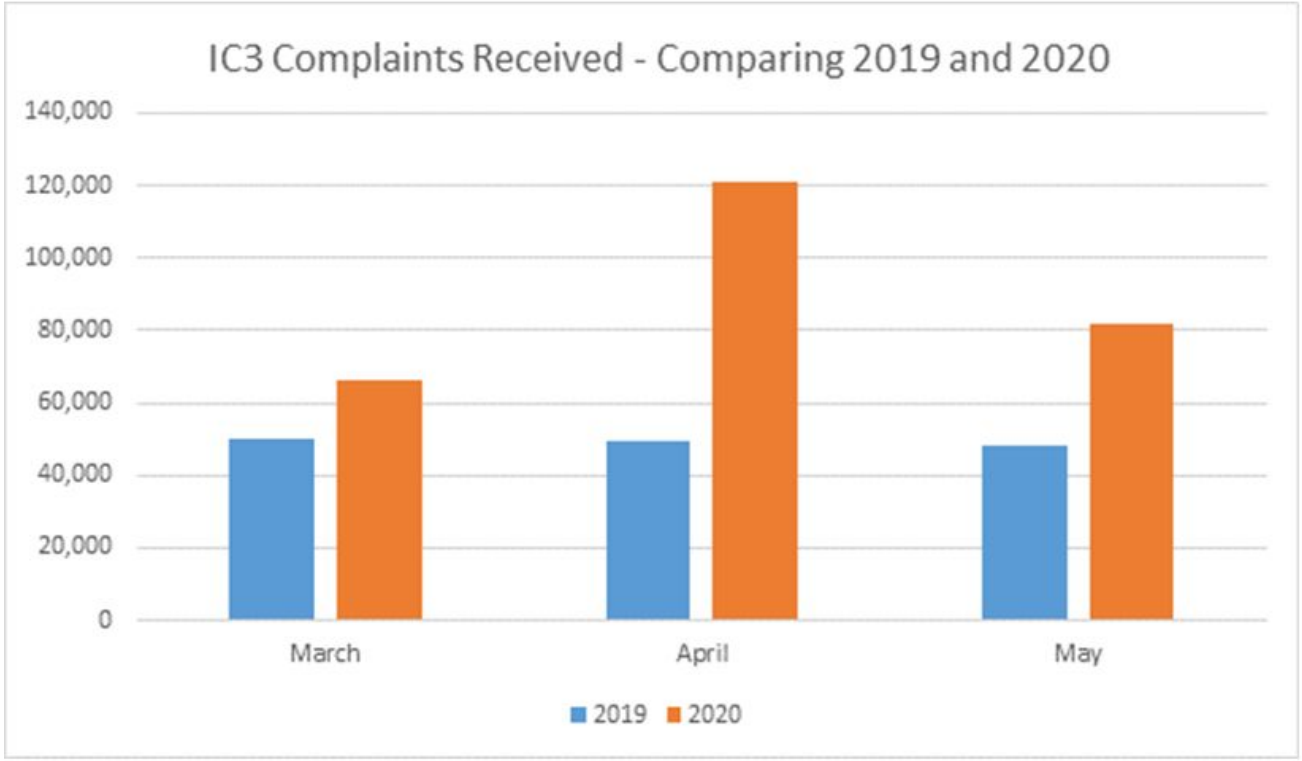
COVID-19 Response: Law Enforcement Perspective



Registrant Information Status of Referred Domains

- Privacy Proxy
- GDPR Redacted
- Unredacted
- Registrar
- Unknown

COVID-19 Response: Law Enforcement Perspective



CRIME TYPE	VICTIM COUNT	VICTIM LOSS
Mar-19	50,179	$318,464,250.34
Apr-19	49,756	$423,700,131.67
May-19	48,136	$441,550,979.47

CRIME TYPE	VICTIM COUNT	VICTIM LOSS
Mar-20	66,492	$382,180,030.30
Apr-20	120,719	$655,835,999.41
May-20	81,746	$466,805,019.37

COVID-19 Response: Next Steps

ICANN68 Cross-Community Plenary Session

- DNS Abuse and Malicious Registrations During COVID-19 (Monday 22 June at 05:00 UTC)
- Laureen Kapin (US FTC, PSWG Co-Chair) will represent the GAC on the panel of experts
- Objective
  - Review and discuss developments that have taken place since the plenary session at ICANN66, including the impact of the COVID-19 pandemic.
  - Identify next steps that the ICANN Community, Board, and Organization can take to address DNS abuse including: *concrete, incremental steps that responsible parties can easily implement that will make tangible impact on the problem*

Relevant Developments Regarding DNS Abuse

Definition of DNS Abuse

- **Contracted Parties (RySG and RrSG)** adopted a definition of DNS Abuse (17 June 2020): as "*composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other[s]*"
  - Mirrors the industry-led voluntary Framework To Address Abuse (2019)
  - Matches the definition of "DNS Security Abuse" by the CCT Review (2018)
  - Consistent with the GAC "Security Threats" per GAC Beijing Safeguard Advice (2013)
- **Should support progress on adoption of proactive anti-abuse measures** per CCT Review Rec. 14 which has been pending *"community efforts to develop a definition of 'abuse' to inform further action" (ICANN Board resolution, 1 March 2019)*
- **Will likely not address compliance enforcement challenges** related to interpretation by Contracted Parties of existing contractual provisions using such definitions (Report on audit of all New gTLD Registry Operators for Addressing DNS Security Threats, 17 September 2019)
- **Falls short of the wider notion of 'DNS Abuse' adopted by the CCT Review** as "*intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names",* and **does not include *certain forms of "Website Content Abuse"***, which the Framework To Address Abuse considers "*so egregious that the contracted party should act when provided with specific and credible notice*".

Relevant Developments Regarding DNS Abuse

CCT Review Recommendations and New gTLD Policy

- **The GNSO New gTLD Subsequent Procedures PDP WG** reported (29 April 2020) that it **is** "***not planning to make any recommendations with respect to mitigating domain name abuse*** *other than stating that any such future effort must apply to both existing and new gTLDs (and potentially ccTLDs)".*
- In the GAC Montreal Communiqué (6 November 2019), **the GAC advised the ICANN Board:** ***not to proceed with a new round of gTLDs until after the complete implementation of the recommendations*** *in the Competition, Consumer Trust and Consumer Choice Review that were identified as "prerequisites" or as "high priority".*
  [The majority of CCT-RT recommendation pertaining to DNS Abuse were identified as such]
- In its contribution to the PDP WG, per the GAC ICANN67 Communiqué and the recent GAC Consultation: ***GAC members expressed concern with this approach,*** *highlighting the importance of the CCT-RT Recommendations and the need to implement them in light of the GAC Montreal Advice*
- The GAC Leadership suggested consultation among relevant experts and expects the **GNSO Council to propose a "framing document" laying out procedural options for future work**

Relevant Developments Regarding DNS Abuse

Stability, Security, Resiliency (SSR2) Review

- The SSR2 Review Team delivered a Draft Report (24 January 2020) with a significant focus on measures to prevent and mitigate DNS Abuse.
- The GAC Comment (3 April 2020) endorsed many of the recommendations and in particular those pertaining to improving Domain Abuse Activity Reporting (DAAR) and the strengthening of compliance mechanisms.
- Final recommendations of the SSR2 RT are now expected by October 2020 (according to recent deliberations)

SSAC Working Party on DNS Abuse Issues

- It is expected that (among other things) it will:
  - discuss reliable data sources of malicious activities
  - review effective practices currently in place in the industry
  - consider new approaches and make recommendations to the ICANN Community
- A representative of the PSWG has been invited to take part
- SSAC is holding a Public Session on Tuesday 23 June 2020 at 00:30 UTC

Next Steps for the GAC

Next Opportunities for GAC Discussion during ICANN68

- GAC Preparation for Meeting with the ICANN Board — Mon. 22 June 07:00 UTC
- GAC Plenary on DNS Abuse 2/2 — Tue. 23 June 08:30 UTC
- GAC/ICANN Board Meeting — Wed. 24 June 08:30 UTC

GAC Deliberations Needed to Determine Next Steps on:

- Privacy/Proxy Services Data Disclosure (COVID-19 Lessons learned for LEA)
- Proactive Anti-Abuse Measures (Implementation of CCT Review Recommendations related to DNS Abuse)
- WHOIS Accuracy Reporting System (Implementation of CCT and RDS-WHOIS2 Review Recommendations)

Possible Questions to the ICANN Board (1/2)

Privacy/Proxy Services

- Background:
  Law Enforcement reported during ICANN68 that the majority of domains involved in pandemic-related fraud, phishing, or malware have employed **Privacy/Proxy Services** to hide the identity of the registrant.
- Question:
  What does the ICANN Board intend to do to ensure that such services can't continue to facilitate threats to the security and consumer trust in the DNS ?

Proactive Anti-Abuse Measures

- Background:
  The CCT Review recommended that ICANN negotiate contractual provisions providing financial incentives for contracted parties to adopt proactive anti-abuse measures (Rec. 14). This recommendation has been placed in pending status by the ICANN Board.
- Questions:
  - What steps, if any, have been taken by ICANN org "*to facilitate community efforts to develop a definition of 'abuse' to inform further action on this recommendation*" ?
  - Why aren't existing community-developed definitions of DNS abuse sufficient ?
  - Would ICANN (even absent a definition) consider incentivizing validation of registrant information by Registrars ?

Possible Questions to the ICANN Board (2/2)

Accuracy of gTLD Registration Data

Background:

- In 2012, **the first WHOIS Review Team** found that "*the low level of accurate WHOIS data is unacceptable*" and recommended that one of ICANN's priority should be to improve WHOIS data accuracy.
- In 2015, ICANN started identifying and reporting inaccurate gTLD WHOIS data through the **WHOIS Accuracy Reporting System (ARS).** In June 2018, as a consequence of the adoption Temporary Specification for gTLD Registration Data, **ICANN suspended operations of the ARS** limiting ICANN Compliance's ability to investigate inaccuracies.
- In September 2018, the **CCT Review recommended specific work to determine whether the ARS could proceed into its ultimate phase of identity validation.** The Board placed this recommendation in pending status until the outcome of the RDS-WHOIS2 Review.
- in September 2019, **the RDS-WHOIS2 Review estimated that 30-40% of registration data was inaccurate and recommended resuming operations of the ARS or a comparable tool** (Rec. 5.1). The ICANN Board placed this recommendations in pending status until the EPDP Phase 2 addresses the matter.
- **It is now clear that Phase 2 of the EPDP will not do so**. The GNSO Council determined that WHOIS Accuracy is not on the critical path of Phase 2, **effectively delaying any meaningful progress indefinitely.**
- **In the meantime**, pervasive gTLD registration **data inaccuracies continue to undermine the effectiveness of the gTLD registry directory service**, including in meeting the legitimate needs of law enforcement and in promoting consumer trust (ICANN Bylaws 4.6.e.ii). This situation may also jeopardize any future registration data access model when it comes to compliance with accuracy provisions in relevant data protection law.

Question:

- What does the ICANN Board intend to do, to restore ICANN's ability to address gTLD registration data inaccuracies, including but not limited to resuming the ARS identity validation phase ?

Other Relevant Sessions during ICANN68

ICANN Plenary Sessions

- DNS Abuse and Malicious Registrations During COVID-19 — Mon. 22 June 05:00 UTC | Details
- The DNS and the Internet of Things: Opportunities, Risks, and Challenges — Wed. 23 June 05:00 UTC | Details

At-Large Sessions

- DNS Abuse: COVID-19 and End-user Issues — Mon. 22 June 02:00 UTC | Details
- DNS Abuse: Setting an Acceptable Threshold — Wed. 23 June 02:00 UTC | Details

ccNSO Session

- Members Meeting - ccTLD & COVID-19 — Thu. 24 June 00:30 UTC | Details