
ICANN
VIRTUAL POLICY FORUM
68

DNS Abuse and Malicious Registration During the COVID-19 Pandemic

ICANN68 Plenary Session

22 June 2020

Panelists and Agenda

Session Moderator: Bruce Tonkin

Segment 1: Developments since ICANN66 (November 2019) – What has happened? What is working well and what is not?

- Jim Galvin (Registries Stakeholder Group)
- Graeme Bunton (Registrars Stakeholder Group)
- Laureen Kapin (Governmental Advisory Committee, Public Safety Working Group)
- Peter Van Roste (Country Code Names Supporting Organization)
- Jonathan Zuck (At Large Advisory Committee)

Segment 2: What can the ICANN ecosystem (community, org, Board) do as next steps? Identify concrete incremental steps that responsible parties can easily implement that will make a tangible impact on the problem.

- Mason Cole (Commercial Stakeholders Group)
- Jeff Bedser (Security & Stability Advisory Committee)
- Brian Cimbolic (Registries Stakeholder Group)
- Graeme Bunton (Registrars Stakeholder Group)
- Laureen Kapin (Governmental Advisory Committee, Public Safety Working Group)
- David Conrad (ICANN org)

Developments since ICANN66

Segment #1

Registries Stakeholder Group

Jim Galvin

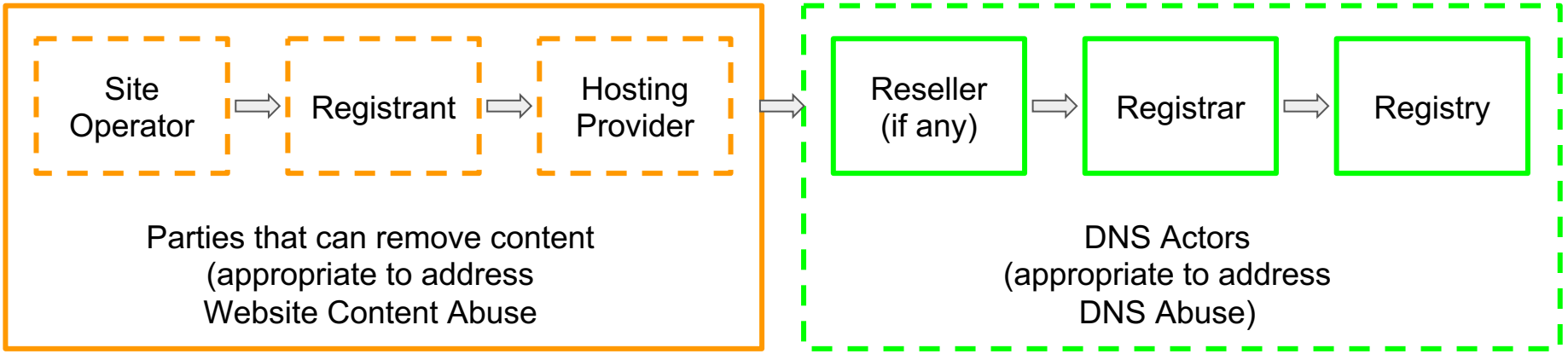
Registries and DNS Abuse

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

What is DNS Abuse?

- DNS Abuse Framework
  - http://dnsabuseframework.org/
  - Definition of DNS Abuse in the Framework officially adopted by Contracted Parties
- DNS Abuse is 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 forms of DNS Abuse).
  - Malware is malicious software
  - Botnets are collections of infected computers
  - Phishing occurs when a victim is tricked into disclosure or other inappropriate action
  - Pharming is redirecting unknowing users to fraudulent sites or services
  - Spam is unsolicited bulk email

DNS Abuse Eco System



- Registries and registrars should promptly investigate allegations of DNS Abuse and Website Content Abuse that falls within this framework
- Registries and registrars have only one blunt and disproportionate tool: take-down

Registrars Stakeholder Group

Graeme Bunton

ICANN | RrSG

Registrar Stakeholder Group

DNS Abuse Plenary

Progress since MTL/ICANN68

- Creation of the DNS Abuse Team of RrSG
  - Established working methods & priorities
  - Initially focused on external education and tools:
    - Guide to Abuse Reporting Best Practices
    - Minimum Required Information for Whois Data Requests
    - COVID-19 Statement

- COVID-19
  - Pivoted to assessing and addressing impact of COVID-19 on the DNS and DNS abuse
  - Good internal discussion and sharing of lists, approaches, tools
  - Great interaction and communication with LEA
  - Summarising data, experiences
  - Next: what worked, what didn't, what are the gaps

Governmental Advisory Committee

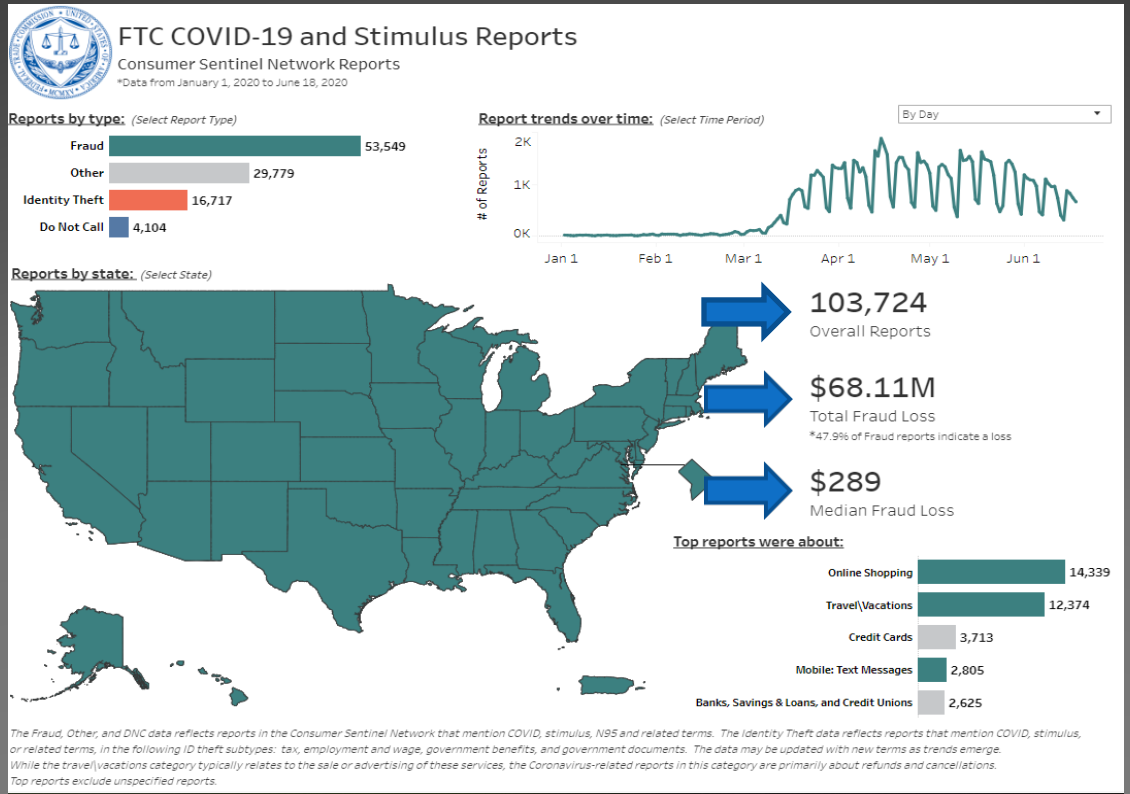
Laureen Kapin

DNS Abuse during the COVID-19 Pandemic

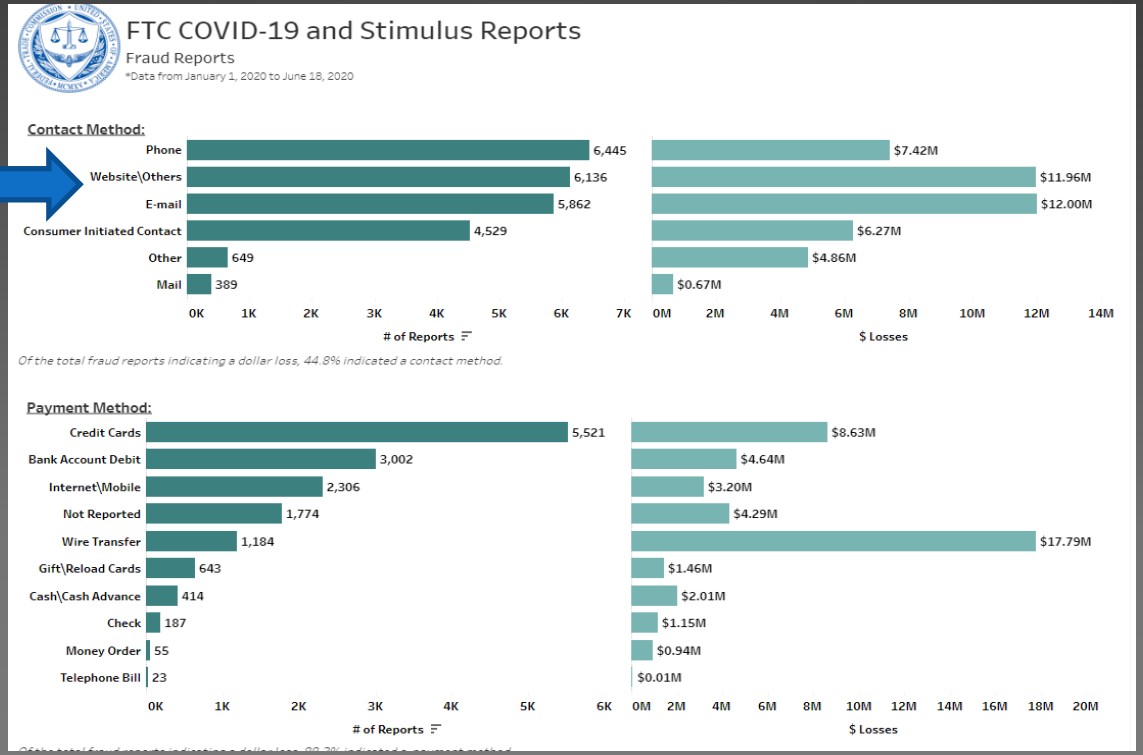
Laureen Kapin

- Counsel for International Consumer Protection
U.S. Federal Trade Commission
- Co-Chair, GAC Public Safety Working Group

COVID-19 Complaints (from FTC Consumer Sentinel Database)



COVID-19 Complaints (from FTC Consumer Sentinel Database)



Working Well: Cooperation

- LEA's working with Registrars & ICANN
- Proactive Screening & Referrals

Room for Improvement:

- Dedicated channels for LEAs to deal with DNS abuse/security threats
- Accuracy of registrant data
- Clear, enforceable contract obligations

Wish List

- Create incentives to encourage good behavior → → →
  - Verifying identity: registrant data prior to sale of domain names
    - more scrutiny for bulk registrations
- "No fly list" for registrants that repeatedly engage in abusive behavior

Country Code Names Supporting Organization

Peter Van Roste

At-Large Advisory Committee

Jonathan Zuck

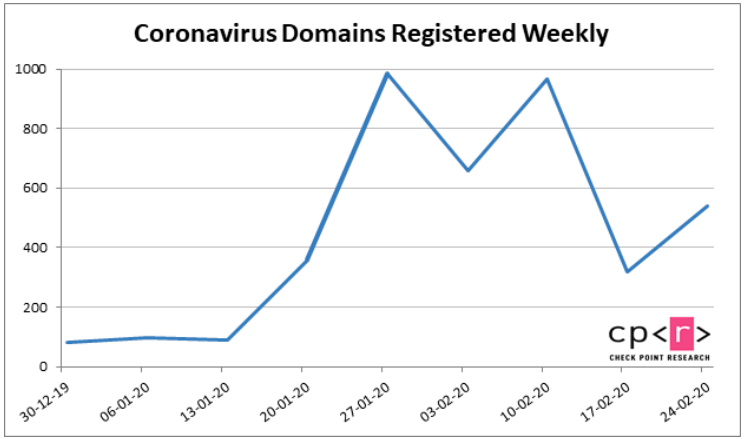
End Users Still Face Challenges

COVID DOMAINS

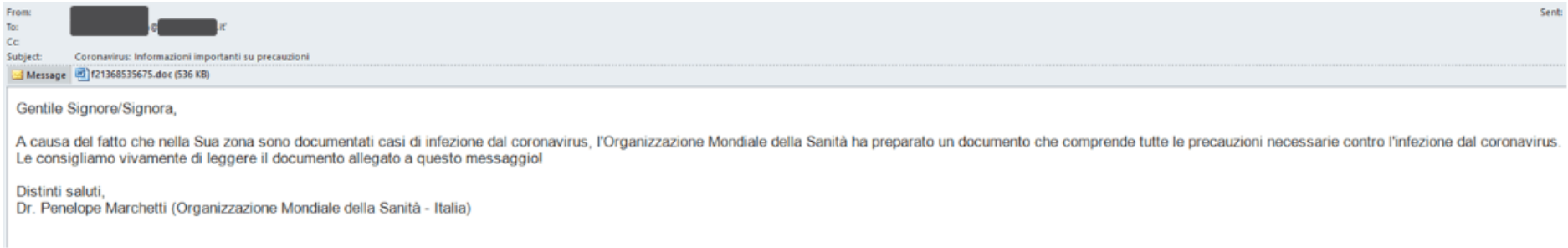
50%

***MORE* LIKELY TO BE**

MALICIOUS!



Phishing in Italy


From: [redacted]
To: [redacted]
Cc:
Subject: Coronavirus: Informazioni importanti su precauzioni
Sent:
Message f21368535675.doc (536 KB)

Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus, l'Organizzazione Mondiale della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie contro l'infezione dal coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggio!

Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

Due to the number of cases of coronavirus infection that have been documented in your area, the World Health Organization has prepared a document that includes all the necessary precautions against coronavirus infection. We strongly recommend that you read the document attached to this message.

With best regards,
Dr. Penelope Marchetti (World Health Organization – Italy

Panel Discussion

What can the ICANN ecosystem (community, Board, and org) do as next steps?

Segment #2

Commercial Stakeholder Group

Mason Cole

Facts about DNS abuse

- DNS abuse is a chronic and growing problem
- It occurs year after year, and periodically is magnified by outside events (e.g., COVID, natural disasters, civil unrest)
- The common theme: The DNS is leveraged for illicit purposes

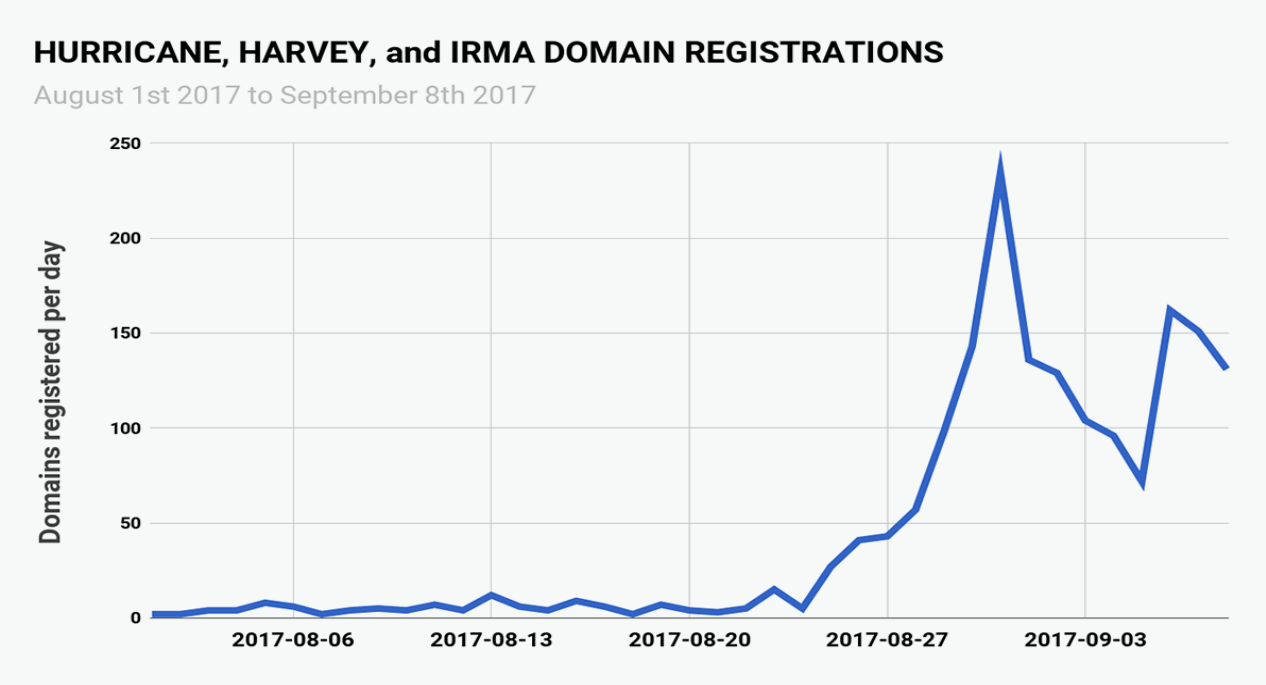
Facts about DNS abuse

- Separate from external events, DNS abuse is steadily growing

- By 2021, it is estimated that cybercrime will cost the global economy more than $6 trillion in damages, exceeding annual costs for natural disasters and the global drug trade. (Arkose Labs, 2019)

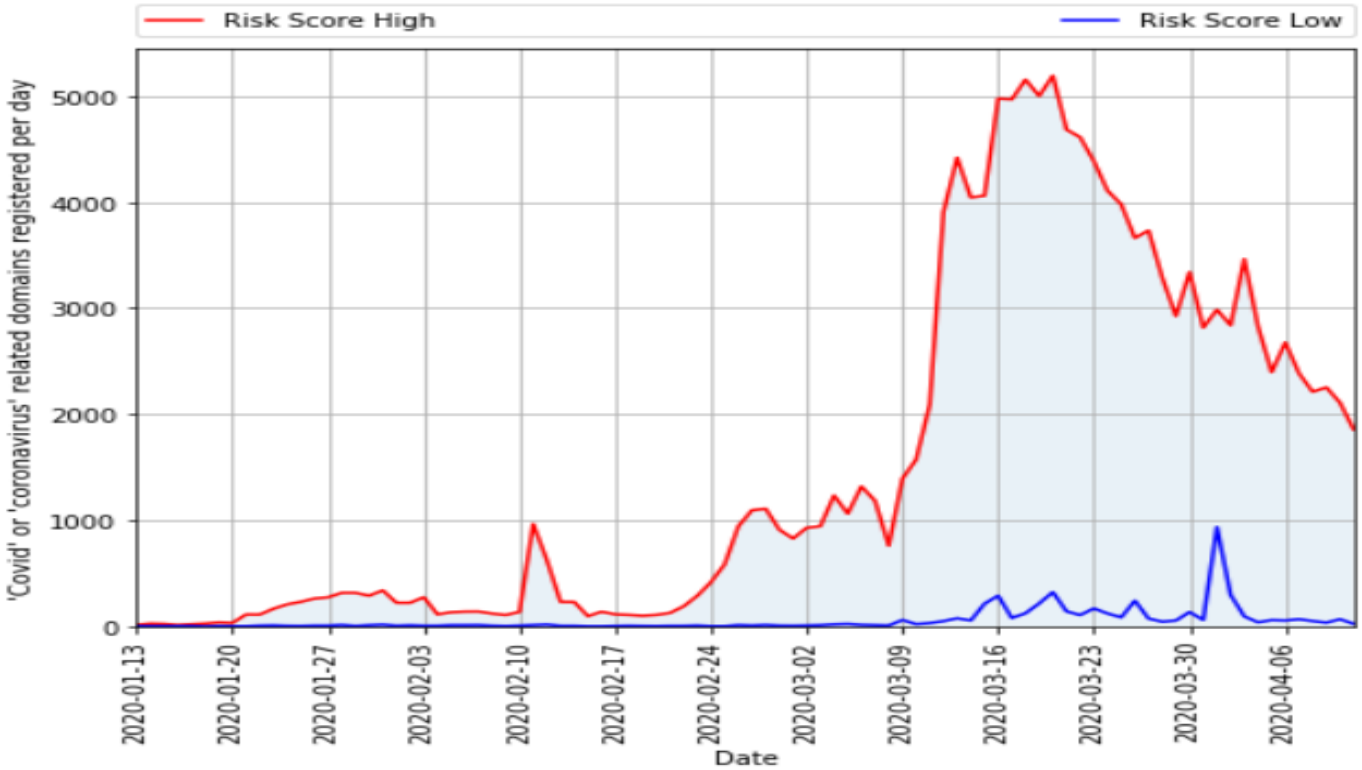
- According to the NABP (2020), abusers are leveraging the DNS for the benefit of “rogue” pharmacies:
  - most active websites have clear ties to known criminal networks or their affiliates
  - some newly created COVID-specific websites redirect users to established rogue network sites
  - many domain names, both active and inactive, are clustered on “safe haven” registrars – a practice common among sophisticated internet pharmacy cybercriminals

2017: Leveraging natural disasters



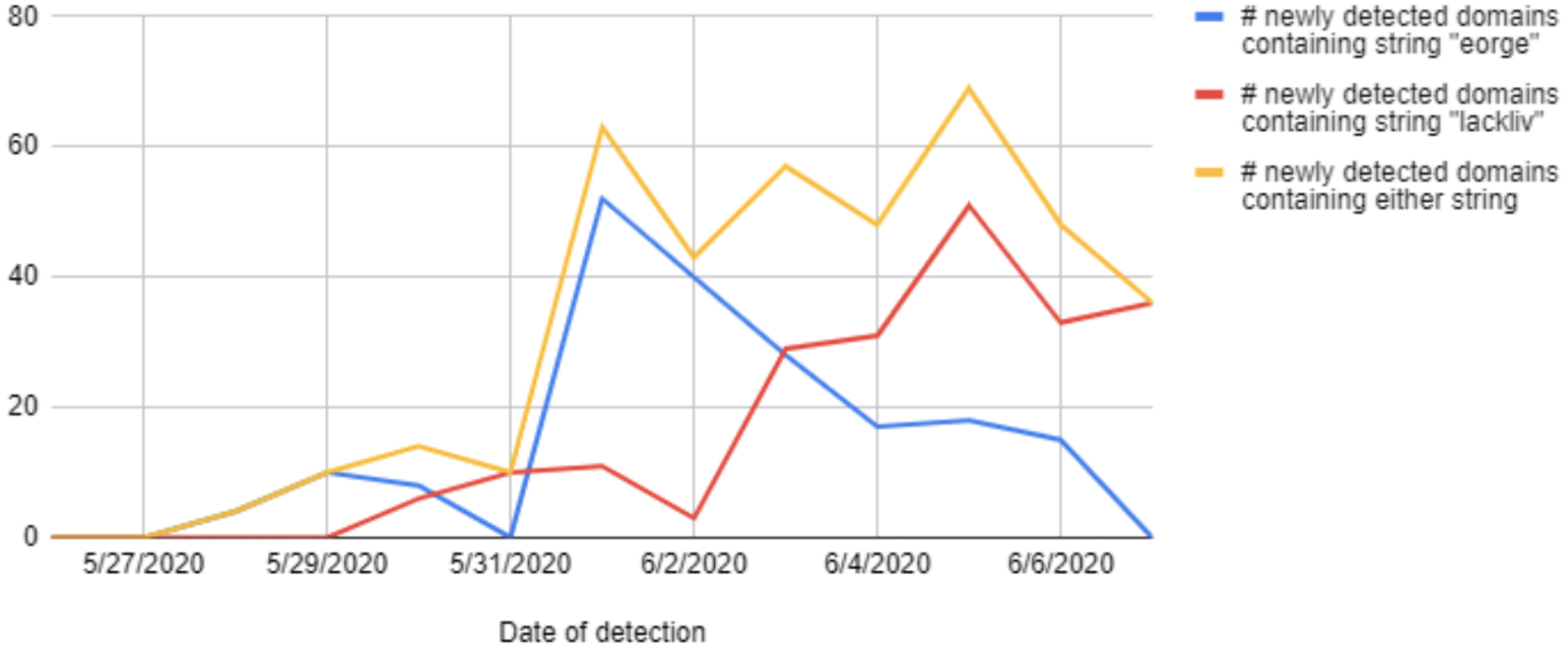
Source: Zetalytics

Trends: Leveraging COVID-19



Source: Krebs On Security

Trends: Leveraging civil unrest in the U.S.



Source: ThreatIntelligencePlatform.com

What happens during “DNS Abuse”

- COVID-19 has resulted in an increase in the efficacy of same-type cybersecurity attacks than in the past.
- People are working outside their company firewalls and on devices which aren’t managed by their company IT groups. Password spray and other brute force attacks are more practical under these circumstances.
- Due to uncertainty related to the pandemic, people are more likely to go to unfamiliar sites to get information, exposing them to criminal infrastructure more often.

Source: Microsoft

The exacerbating problem

- ICANN Org doesn’t have the tools it needs to combat the behavior via rogue registrars

- The result is a “tragedy of the commons” -- everyone is incentivized to do little because no one is held to account.

What can be done?

- Don’t address one scam at a time reactively
- Learn from past and current abuse behavior and take proactive steps to address abuse before it happens, not after everyone has been harmed
- Implement real tools for combating abuse
  - Across the board
  - Not voluntary only
- Tools can look like the response to U.S. Congress – institutionalize that process and memorialize it in contracts.
- Personal observation: Most “big players” are doing the right thing. A small group bears disproportionate responsibility. That group won’t join frameworks or come to ICANN meetings. We need tools to hold them accountable.

Security and Stability Advisory Committee

Jeff Bedser

ICANN|68
VIRTUAL POLICY FORUM

ICANN | SSAC

DNS Abuse
Work Party

- Agreement that Abuse of Consumers of the DNS is a problem…
- Framework of Effective Practices for abuse resolution
- Full DNS Eco-system Model

ICANN|68
VIRTUAL POLICY FORUM

ICANN | SSAC

DNS Abuse
Work Party

- Categorizations of Abuse
- Evidentiary Standards
- Effective Abuse Reporting Practices
- Escalation Paths
- Reasonable Timeframes
- Availability and Quality of Contact Information

Registries Stakeholder Group

Brian Cimbolic

LOOKING FORWARD

Continued dialogue between Contracted Parties and other stakeholders

Broader adoption of Framework to Address Abuse

Incentivize “good” registrations; penalize abusive registrations.

QUALITY PERFORMANCE INDEX

- Provides financial incentives for registrars with “good” registration patterns
- QPI Factors:
  - **Abuse rates** (gating mechanism)**
  - Renewal rates
  - Domain usage
  - DNSSEC enabled
  - SSL Usage
- Both a “carrot” and “stick” – Registrars that do not qualify have asked how to improve.
- Encourage other Registries to adopt – happy to share this practice, think it’s good for the DNS.

Registrars Stakeholder Group

Graeme Bunton

Governmental Advisory Committee

Laureen Kapin

ICANN org

David Conrad

What Can the ICANN organization Do?

- "Tactical"
  - New keywords in the Domain Name Security Threat Information Collection and Reporting (DNSTICR) tool.
    - Provide high confidence reports to registrars for appropriate action, track and report outcomes
    - Challenge: keyword selection -- perhaps spikes in registrations of substrings?
  - Refine the DNS Abuse Activity Reporting tool's reports
    - Explain data and its limitations better, offer more detailed data
    - Include ccTLDs and registrars
    - Focus on anomalies, offer help
  - DNS Security Facilitation Initiative
    - Provide more information and other resources to the community
    - Facilitate greater understanding of DNS ecosystem risks and mitigations
  - Proactively enforce relevant obligations
    - Compliance addresses complaints and conducts audits focused on DNS abuse using data from various sources.
- "Strategic"
  - Facilitate ongoing discussions regarding DNS Abuse
    - Clarify the roles of registrants vs. contracted parties vs. ICANN
  - Partner with anti-abuse organizations, law enforcement, etc.
    - More MoUs and other agreements to facilitate joint work/understanding
- Ultimately: whatever there is community consensus about
  - Unless the obligations are clearly written and understood, they will be unenforceable

From the latest DAAR Report

https://www.icann.org/en/system/files/files/daar-monthly-report-31may20-en.pdf

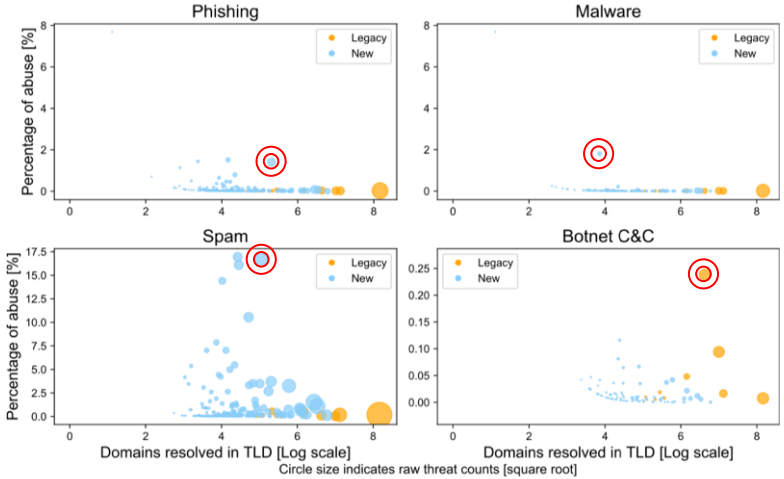


Figure 13: Percentage of abuse for domains identified as security threats vs. counts of resolved domains in gTLDs across different threat types

Understand the outliers (◎) and work with them to reduce their scores. Repeat as necessary.

Panel Discussion

Questions and Comments

ICANN 68
VIRTUAL POLICY FORUM
22–25 June 2020

Help us Improve Future Meetings

Let us know what you think of the ICANN68 Virtual Policy Forum. Visit the link below. Under “Event Details” you will find a link to a short survey.

Visit https://68.schedule.icann.org/ to access the survey.