ICANN 69

VIRTUAL ANNUAL GENERAL

Thank You to our Sponsors!

DNS Abuse: Consideration of the Issues

ICANN69 Plenary Session

Tuesday, 20 October 2020
10:30-12:00 CEST

Opening Remarks

Thomas Rickert (eco)
Moderator

Introductions

Participant	Perspective	Affiliation
Thomas Rickert	Moderator	eco
David Conrad	Overview	ICANN organization
Jeff Bedser	SSAC DNS Abuse Work Party	iThreat
Mason Cole	Commercial Stakeholder Group	Perkins Coie LLP
Chris Lewis-Evans	GAC Public Safety Working Group	National Crime Agency-UK
James Bladel	Contracted Parties House	GoDaddy

Program

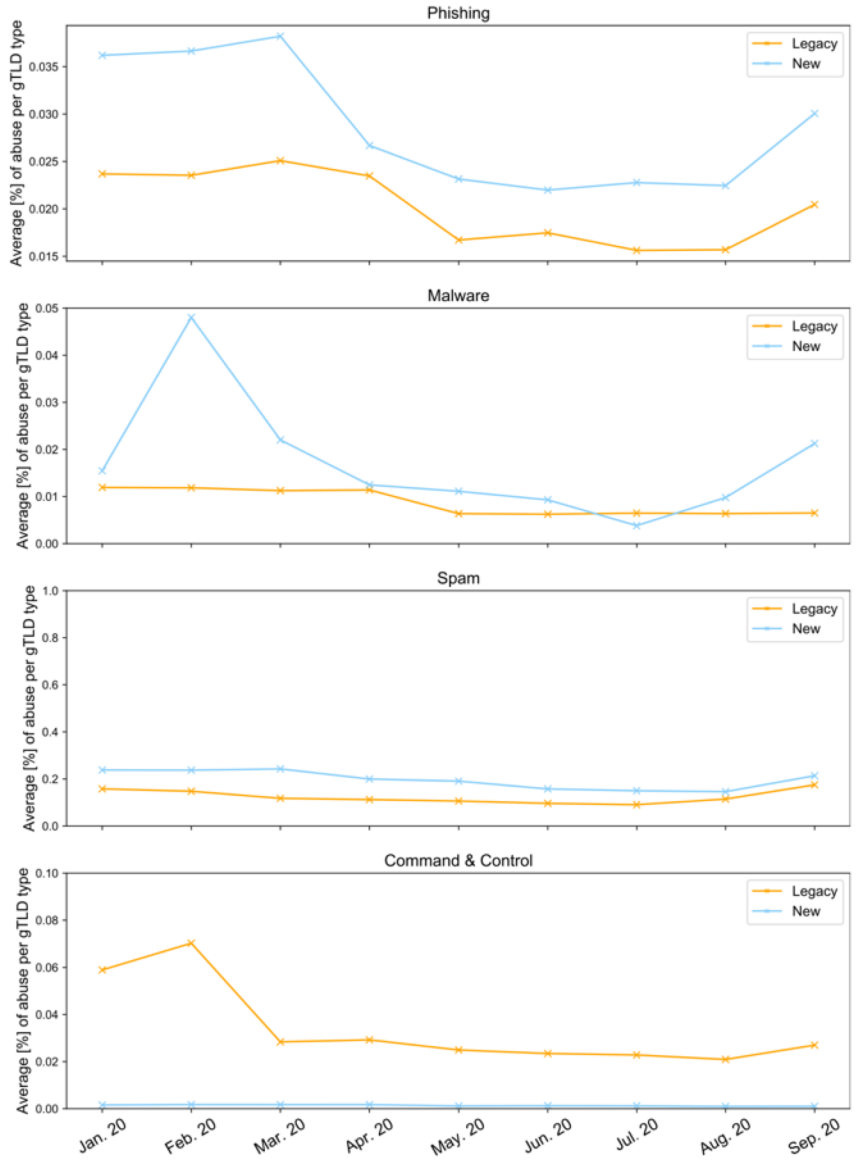
1.	Opening Remarks and Introductions	Thomas Rickert	5 minutes
2.	“Abuse Across the DNS” since ICANN66 (and before)	David Conrad	10 minutes
3.	Practical Next Steps for Tackling Abuse in the DNS	Jeff Bedser	10 minutes
4.	Commercial Stakeholder Group Perspective	Mason Cole	10 minutes
5.	Law Enforcement Perspective	Chris Lewis-Evans	10 minutes
6.	Contracted Parties House Perspective	James Bladel	10 minutes
7.	Discussion	All	30 minutes
8.	Closing Remarks	Thomas Rickert	5 minutes

“Abuse Across the DNS” since ICANN66 (and before)

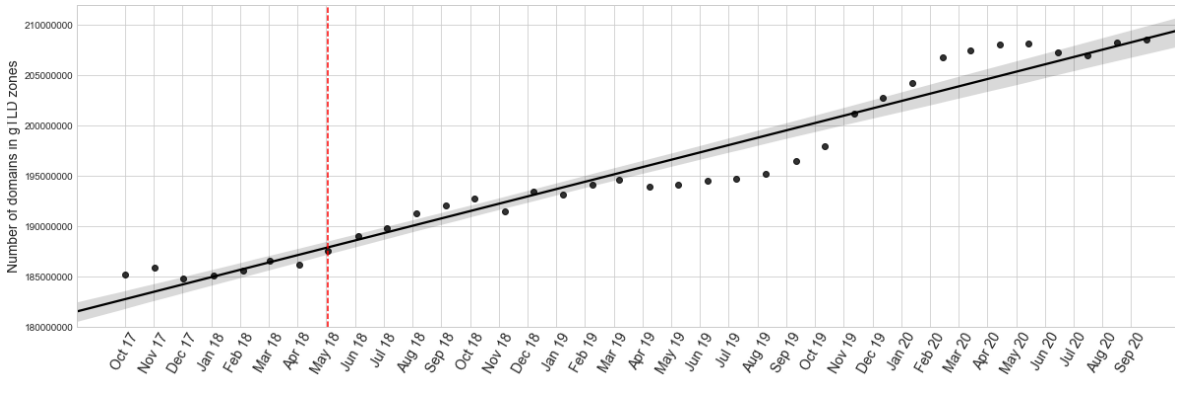
David Conrad (ICANN organization)
Overview

Domain Security Threat Landscape from Sep 2019 to Sep 2020

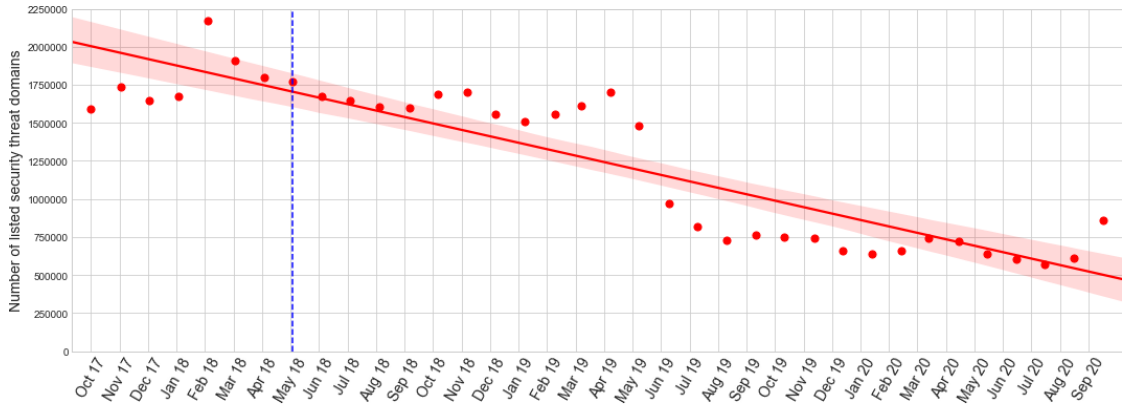
- Looking at DAAR data
  - DAAR reports only go back 6 months,
- Decreases in:
  - **Phishing**: -11,244 domains or **13.14%** less
  - **Malware**: -9,169 domains or **25.41%** less
  - **Botnet C&C**: -5,885 domains or **14.13%** less
- Increase in:
  - **Spam**: +121,551 domains or **20%** more
- Spam, as always, skews statistics:
  - Overall abusive domains: Increase of +98,486 or **12.91%**
  - Overall abuse ratio: Increase of **0.02%**
- But we keep DAAR data back to Oct 2017…



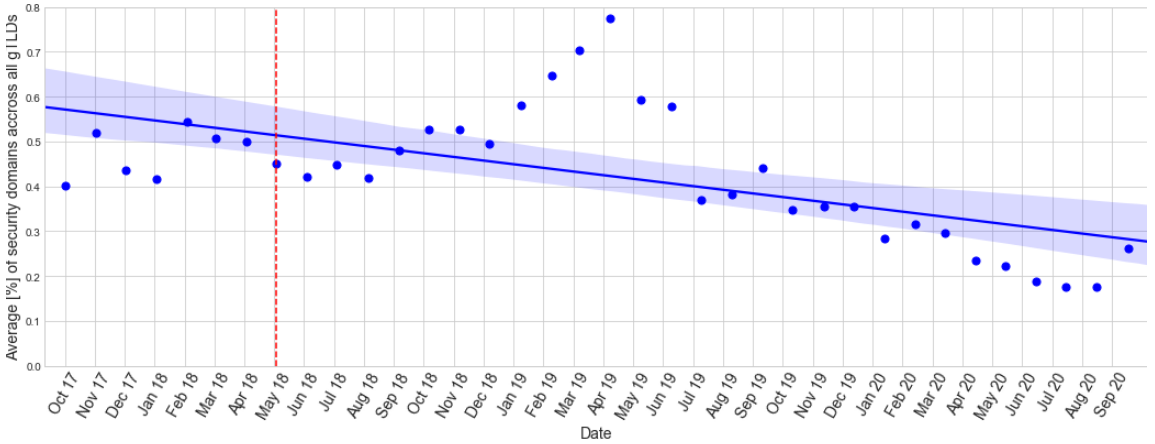
Zooming Out: Aggregated Data: Oct 2017 to Sep 2020



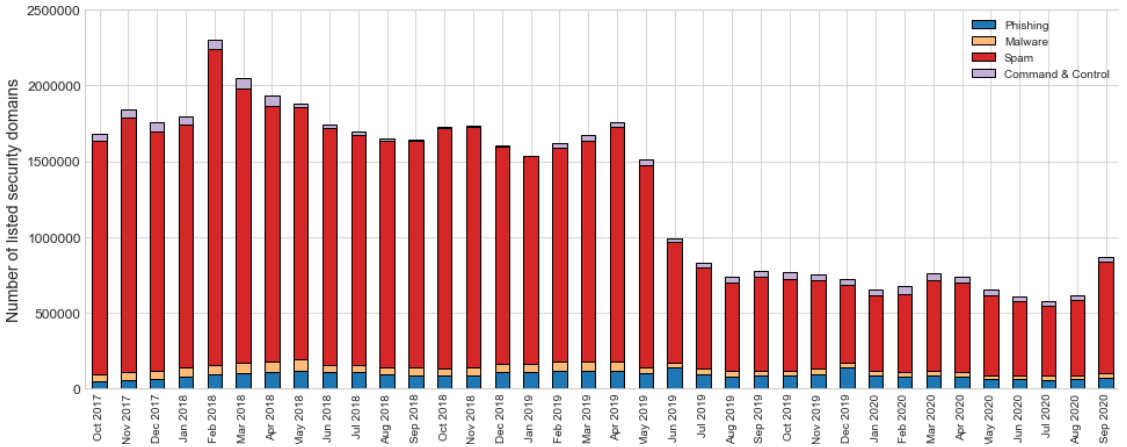
1. Number of gTLDs going up



2. Number of aggregate security threats going down

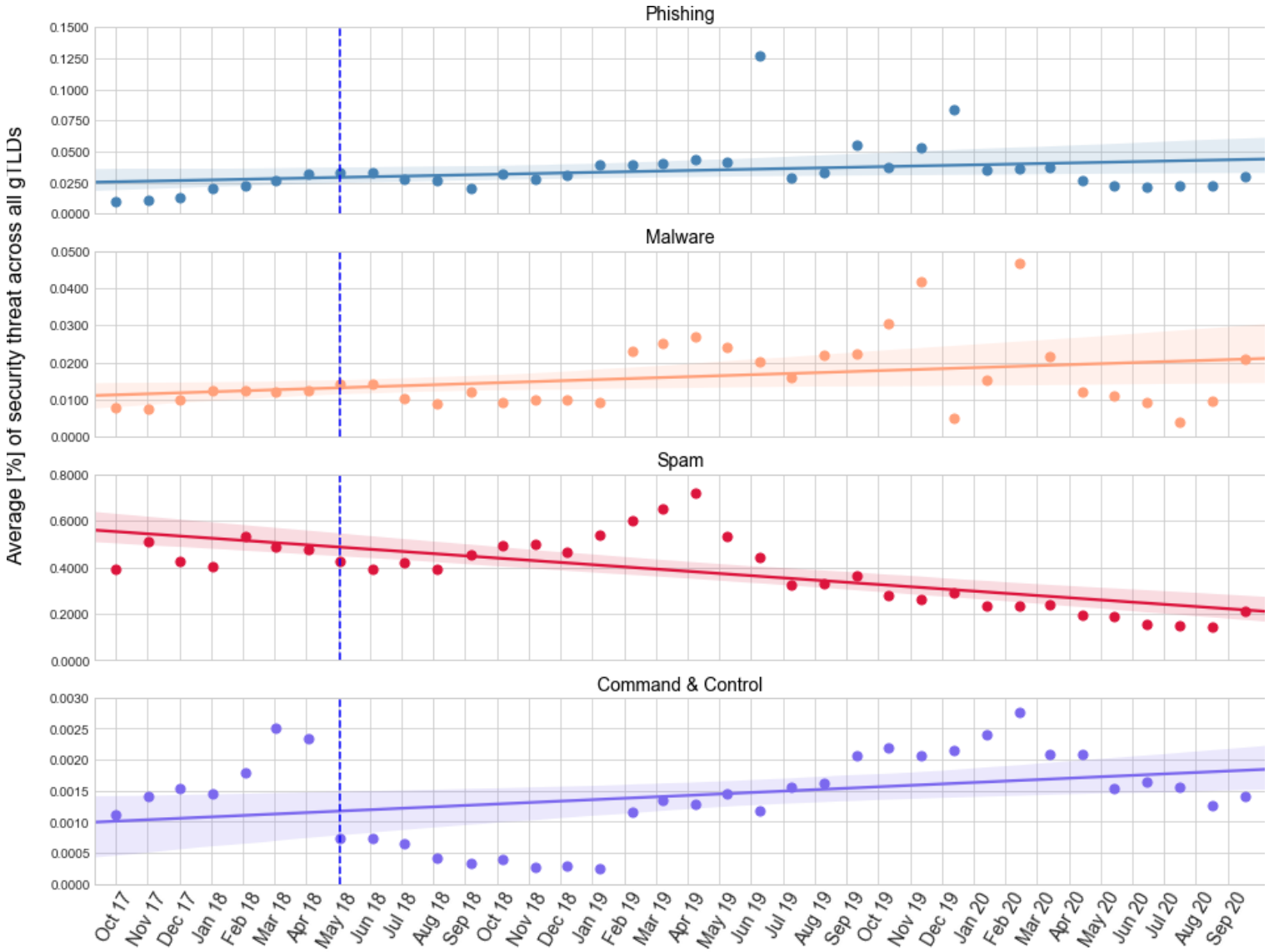


3. Normalized rate going down



4. Spam *still* domainates

Zooming Out: Individual Security Threats Oct 2017 to Sep 2020



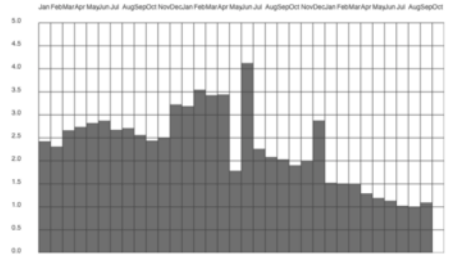
Identifier Technologies Health Indicators (ITHI)

- Started in 2018, monitors metrics associated with the “health” of the identifier ecosystem
- “Metrics M2 - Domain Name Abuse” shows trends over time (since 1/2018), abuses per 10,000 domains, and counts of gTLDs/registrars that account for 50% and 90% of reported security threats, e.g.:

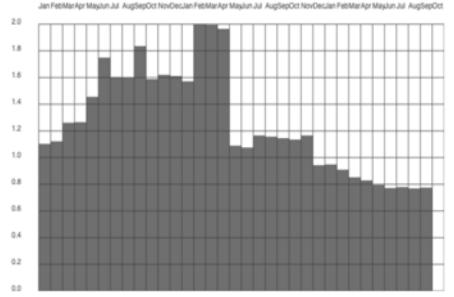
Sep 2020 Abuse Types	gTLD Registry %	# RYs for 90%	Registrar %	# RRs for 90%
Phishing	0.0357%	10	0.0110%	54
Malware	0.0129%	4	0.0078%	70
Botnet C&C	0.0172%	4	0.0029%	51
Spam	0.3525%	17	0.0894%	52

- Uses the same raw data as DAAR plus Whois data for registrars

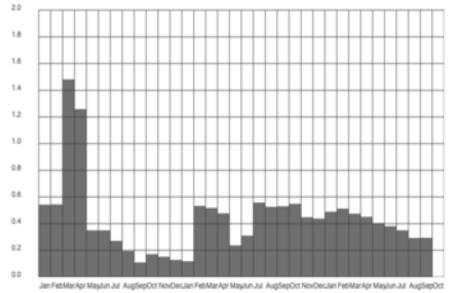
Phishing per 10,000 names from registrars



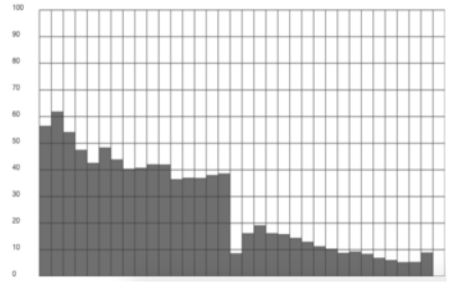
Malware distribution per 10,000 names from registrars



Botnet C&C per 10,000 names from registrars

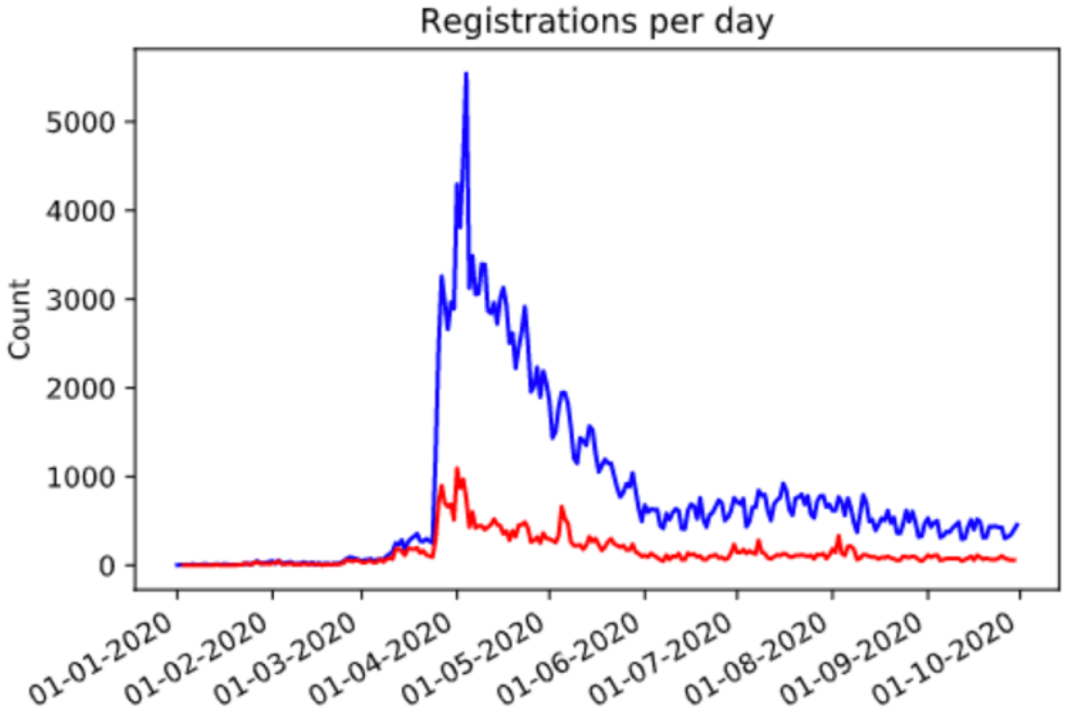


Spam per 10,000 names from registrars



Domain Name Security Threat Identification, Collection and Reporting (DNSTICR)

- Jan 2020 to Sep 2020
  - Detected 235,521 pandemic-related domains (both legit and malicious)
  - Only phishing and malware distribution
- May 2020 to Sep 2020
  - Consistent collection and analysis period
    - Detected 134,332 pandemic-related domains (both legit and malicious)
    - Of these, 8,577 (6.4%) domains had one or more reports in phishing/malware reputation lists **and** had nameservers or resolved to an IP address
    - High confidence reports: 2,329 (1.7%) domains
- Reporting of high confidence domains to registrars started in June

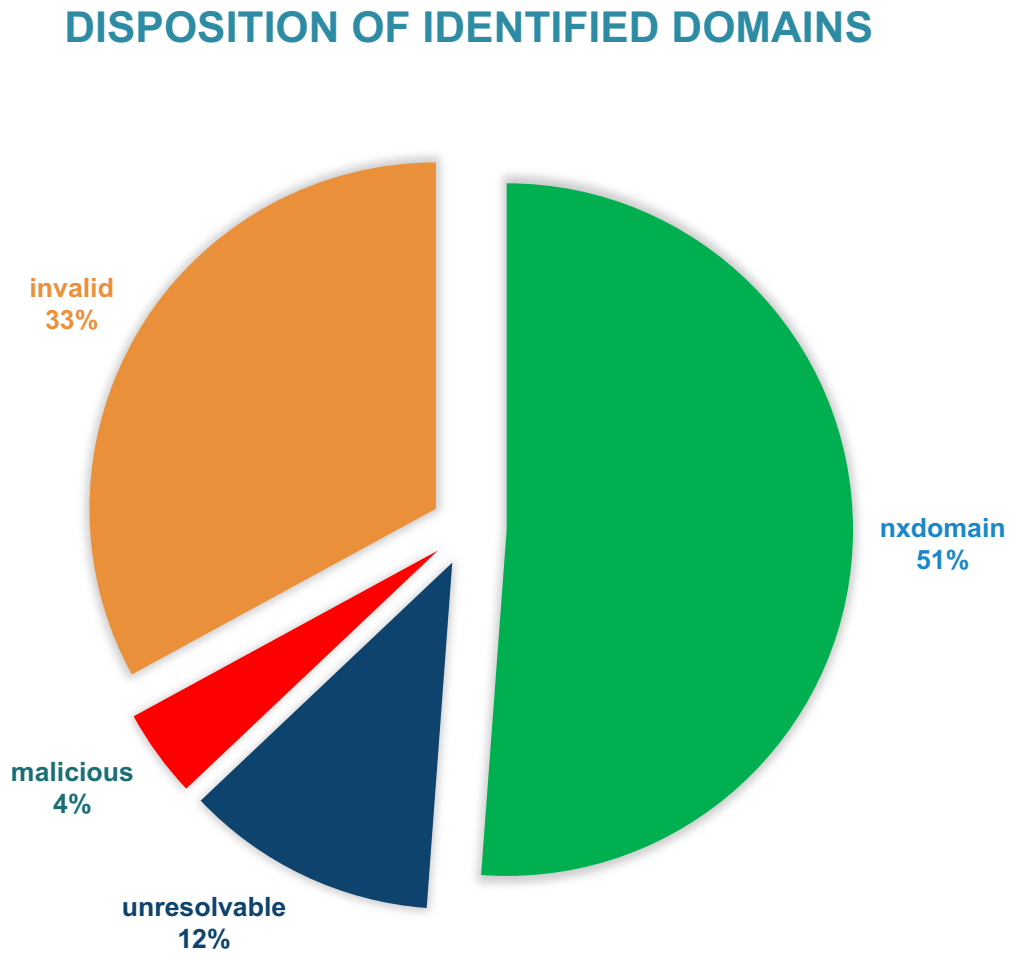


Registrations per day matching one or more of our filter terms (blue line) plus those which had one or more third-party reports (red line). Dates in DD-MM-YYYY format.

Domain Name Security Threat Identification, Collection and Reporting (DNSTICR)

- Jun 2020 - Sep 2020
  - **80,096** pandemic-related domains (both legit and malicious) seen between 1 Jun and 30 Sep
  - **170 (0.2%)** reports sent to registrars of the seen pandemic-related domains

- Of the 170 reported on, as of Oct 6:
  - 87 are NXDomain (domain does not exist)
  - 56 no longer meet reporting criteria (invalid)
  - 20 don't resolve (NS records to nameservers that don't respond)
  - 7 still appear to be malicious



Practical Next Steps for Tackling Abuse in the DNS

Jeff Bedser (iThreat)

SSAC DNS Abuse Work Party

Starting the dialog

- The internet itself is being abused to a very concerning extent, and the DNS is often used as a lever to enable this abusive outcome. DNS abuse is not the entirety of the problem, nor should one expect all abuse to stop if the DNS was longer abused.

- DNS abuse continues to victimize millions annually, and reduces the trust in the Internet, including the DNS, as a place to conduct personal, commercial, non-commercial, and other activities. This erosion of trust negatively impacts all parties in the Internet ecosystem from end-users to the service providers of that infrastructure.

- The report intends to outline a strategy to address the methodologies, practices, and cooperation necessary for reducing DNS abuse. This effort to establish best practices can only be attained with the cooperation and understanding of the majority of the entities integral to the operation of the DNS.

Key Points

- encourage standard definitions of abuse;
- determine the appropriate primary point of responsibility for abuse resolution;
- identify best practices for deployment of evidentiary standards;
- establish standardized escalation paths for abuse resolution;
- determine reasonable timeframes for action on abuse reports;
- recommend the development of “notifier programs” that will expedite and make more efficient abuse handling in certain parts of the ecosystem; and
- create a mechanism for the availability of contact information for abuse mitigation; and
- create a mechanism to ensure reasonable quality of contact information for abuse mitigation.

Commercial Stakeholder Group Perspective

Mason Cole (Perkins Coie LLP)
Business Constituency

DNS Abuse – The problem that doesn’t go away

- 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
- This is ICANN’s fourth consecutive plenary on DNS abuse

DNS Abuse – The problem that doesn't go away

According to Interisle Consulting Group (October 2020):

- During the study period (May 1 - July 31, 2020), phishing reports impacted over 99,000 unique domain names in 439 TLDs at 414 registrars. Of this total, Interisle identified 60,935 maliciously registered domain names.

- The phishing problem is bigger than reported, though the exact size is unknown. Over-redaction of Whois data is contributing to the under-detection problem.

According to SSAC

- Unchecked, DNS abuse and resultant cybercrime continues to victimize millions annually, and reduces the trust in the Internet, including the DNS, as a place to conduct personal, commercial, non-commercial and business activities. This erosion of trust negatively impacts all parties partaking in the ecosystem from end-users to the service providers enabling the infrastructure.

The statistics and where we should agree

- DNS abuse may be going up or it may be going down, depending on your source of data.
- What we can and should agree on: Abuse, when it does occur, has an impact on internet trust and needs proactive, data-driven remediation.
- Our war isn't with each other within ICANN – it's with bad actors.

Progress has been made

- Voluntary framework by registries and registrars has had a measurable impact and should be applauded.

Where progress has not been made

- Voluntary frameworks are helpful but not fully inclusive
- There remain the always referred-to 8-10 bad actor contracted parties ICANN says it knows about, where the bad guys hide

Back to Montréal

Elliot Noss of Tucows:

We need to deal with the issues that are in front of us. If compliance is able to effectively identify that there are specific elements of the contract that will help them enforce very clear bad acts that we all know are in existence, then let's talk about those. I don't believe they need those. I don't believe they need anything additional to what's in the current contracts, but let's talk about those. And let's get on with that specifically. Compliance dealing with known bad actions that we all agree should be dealt with.

Steps forward

One doesn't climb Mt. Everest in one big step. Similarly, take on DNS abuse in stages. In addition to SSAC recommendations:

- Clean up the low-hanging fruit (8-10 known bad actors) that create the biggest problems in the namespace now with the tools you have
- Argue concurrently or later over abuse definition and whether or not new tools are needed
- Consider incentives for those running "clean" registries and registrars
- ICANN: Be proactive with compliance function
- Contracted parties: Be proactive with mitigation and prevention
- Turn once-per-meeting plenary discussions into once-per-meeting progress reports to the community

Law Enforcement Perspective

Chris Lewis-Evans (National Crime Agency-UK)
GAC Public Safety Working Group

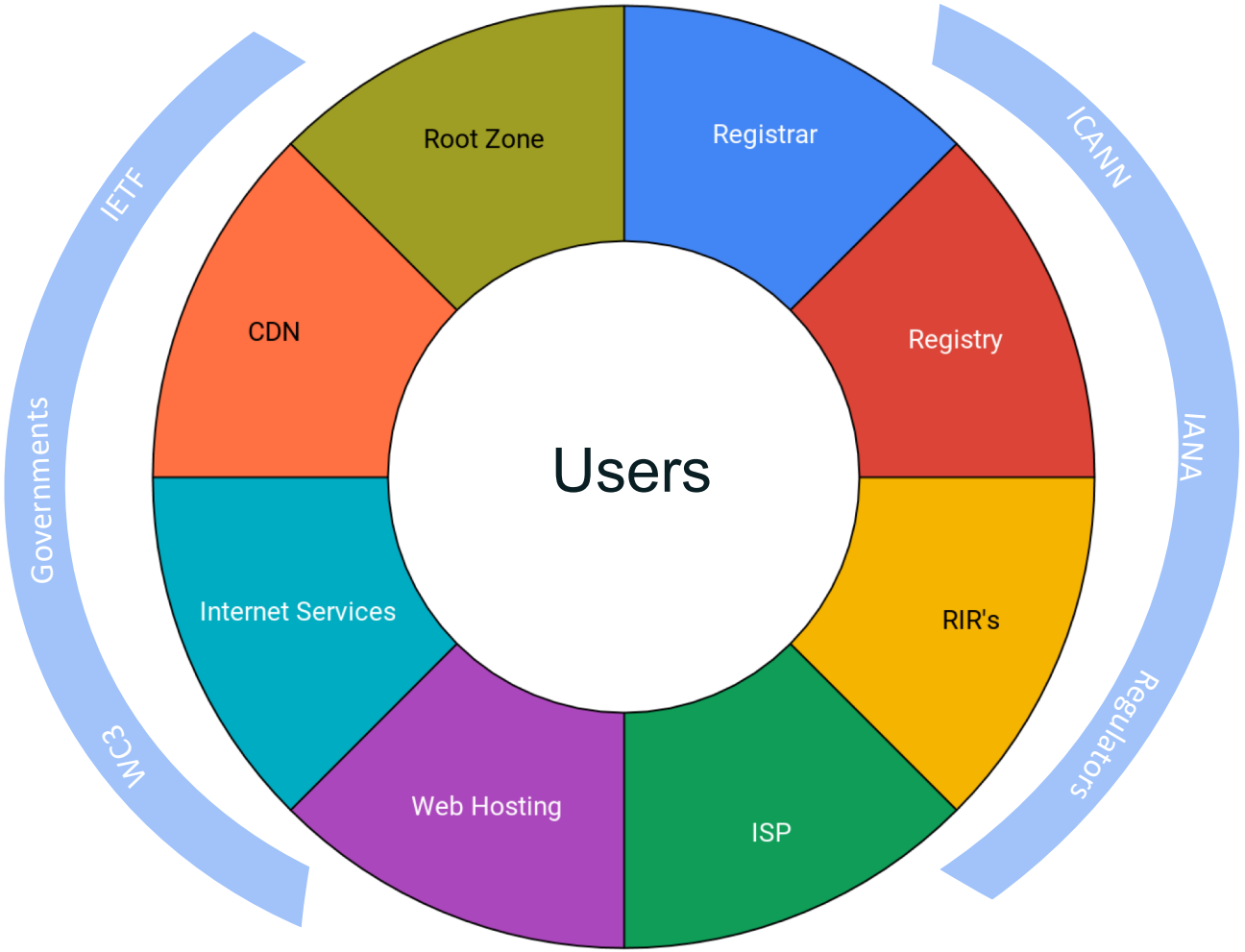
What is the issue?

- The FBI's Internet Crime Complaint Center received 467,361 complaints in 2019—an average of nearly 1,300 every day—and recorded more than $3.5 billion in losses to individual and business victims. The most frequently reported complaints were phishing and similar ploys.[1]
- 85% of reported fraud is cyber enabled.[2]
- Global ransomware reports increased by 715.08 percent.[3]
- Over 60% of cyber security incidents where personal data breaches are reported to the UK's DPA are attributed to Phishing and Malware.[4]

[1] IC3 2019 Internet Crime Report [2] Fraud and cyber crime national statistics - UK [3] Bitdefender Threat Landscape Report 2020 [4] ICO Data security incident trends

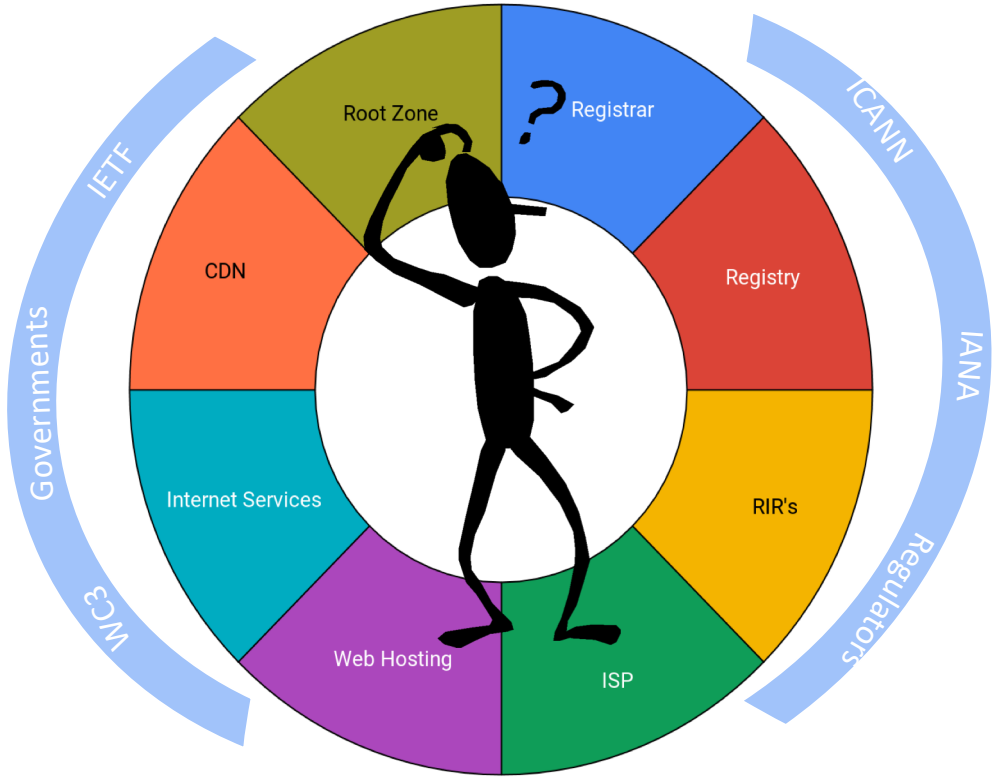
Who’s Involved

- Whole ecosystem response
- Utilise multiple mechanisms
- Common Facilitator



What can we do?

- Education on primary contact points
- Guidelines to support effective reporting
- Provide escalation pathways
- Timeliness of response
- Proactive action increase barriers
- Reactive reduction in harm caused
- Data Sharing Agreements



Contracted Parties House Perspective

James Bladel (GoDaddy)
Registrar Stakeholder Group

Introduction

- Abuse generally is an important challenge for industry, and a priority for contracted parties.
- But it's important to recognize the distinctions between "DNS abuse", and other types of abuse that are content-specific.

Limited Roles

- The mission of ICANN is to preserve the security and stability of the DNS, but its remit does not provide for content moderation.
- Likewise, the ability of a Registrar or Registry to address content abuse via the DNS is limited and often not appropriate.
  - Often referred to as the “nuclear option.”
- But outside of ICANN, industry has organized efforts to mitigate content-specific abuse.

Non-ICANN Industry Efforts

- In September 2019, 11 Registrars & Registries launched the Framework on DNS Abuse, to standardize definitions and set expectations for action.
  - Defined ”DNS abuse” as: malware, botnets, phishing, and pharming, with “spam” listed as an attack vector
  - Framework has now grown to over 50 signatories
  - Members have released a Year One update, available at http://dnsabuseframework.org
- Earlier in 2019, the Internet and Jurisdiction Policy Network published a whitepaper outlining the challenges and mitigation practices of DNS abuse.
  - Definitions aligned with The Framework, with the addition of fast-flux hosting
- Other industry alliances & coalitions target specific categories of abuse, including spam, CSAM, counter-terrorism, pharma, etc.

Current State

- In 2020, the world raced to move online in response to the COVID19 pandemic.
  - Small businesses, schools, civic, religious organizations, and even our social lives all “pivoted” to a virtual model. Even ICANN.
- Our industry played a vital role in helping modern economies weather the storm and transform.
- But we shouldn’t be surprised that criminals and opportunities followed suit.
- But the sky is not falling…

Spotlight on Phishing

- Our industry is seeing an uptick in phishing reports, aligned with the OCTO report.
- But at a more modest YoY growth (15%), nothing approaching a “surge” of abuse.
- Currently GoDaddy processes over 2000 phishing reports (not incidents) per day. The majority of these are not actionable or duplicates.

Spotlight on COVID19 scams

- COVID19-related internet scams dominated headlines
- But our data shows incidents peaked in late March or early April, coinciding with global lockdowns.
- Mostly content-focused and not necessarily novel
- Effective mitigation at the webhost (rather than Registrar/Registry/DNS) level.

Bottom line for CPH

- DNS abuse is extremely important, but we must recognize the limited role of Registrars, Registries, and ICANN.
- ICANN can help facilitate community discussions, exchange of views, research, and collection of statistics.
- But developing new policies will be difficult to scope appropriately, likely not be effective, and could distract from essential non-ICANN industry efforts.

Discussion

Thomas Rickert (eco)
Moderator

Closing Remarks

Thomas Rickert (eco)
Moderator

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann