

Capacity Building Workshop for New GAC Members:

Introduction to “DNS Abuse” and “WHOIS” topics

GAC PSWG Speakers:

Gabriel Andrews (US Federal Bureau of Investigation)

Laureen Kapin (Federal Trade Commission)

ICANN75

September 18, 2022 (Kuala Lumpur)

ICANN | GAC

Governmental Advisory Committee

Agenda

1. **Who am I? (and what is the “PSWG”?)**
2. **What this is:**
 - **Focused on ICANN newcomers.**
 - **Friendly / casual (with breaks for questions!)**
 - **An *introduction* to the topics of “DNS Abuse” and the “WHOIS”/RDS (Registration Directory Service)**
3. **What this isn't:**
 - **New**
 - **Complete**
 - **Contentious (I hope).**

Agenda

1. Flow

- ~ 10 minutes on “DNS Abuse”
 - + 10 minutes questions and answers, discussion
- ~ 10 minutes on “WHOIS”/RDS (Registration Directory Service)
 - +10 minutes questions and answers, discussion, coffee

Agenda

Registrant

>buys



Registrar

>sells



+ ~3k others

Registry

> maintains the
"top level domain"
(after the dot)



+ dozens



DNS Abuse

It's easy to define the DNS.

- **DNS = the Domain Name System**

- Converts the **human readable** domain names ...

- ... to the **machine routable** Internet Protocol Addresses

- www.icann.org < > 192.0.43.7

Consensus on Abuse is harder.

- **DNS Abuse = ... ?**

DNS Abuse's definition is a topic of debate.

[Contracted Parties House Definition](#): (16 June 2020)

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.

[E.C. Study on DNS Abuse](#): (31 January 2022)

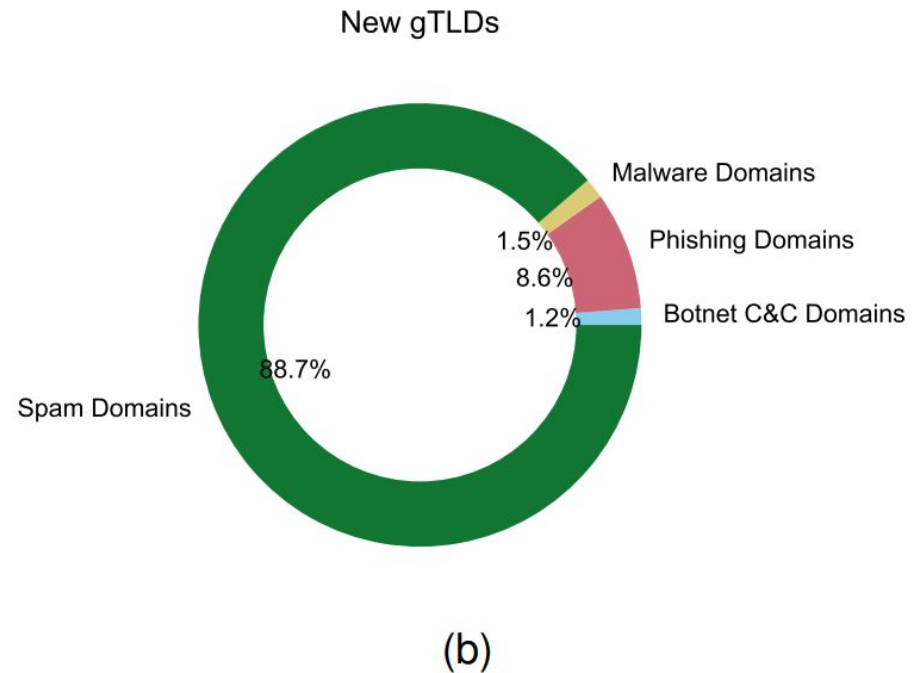
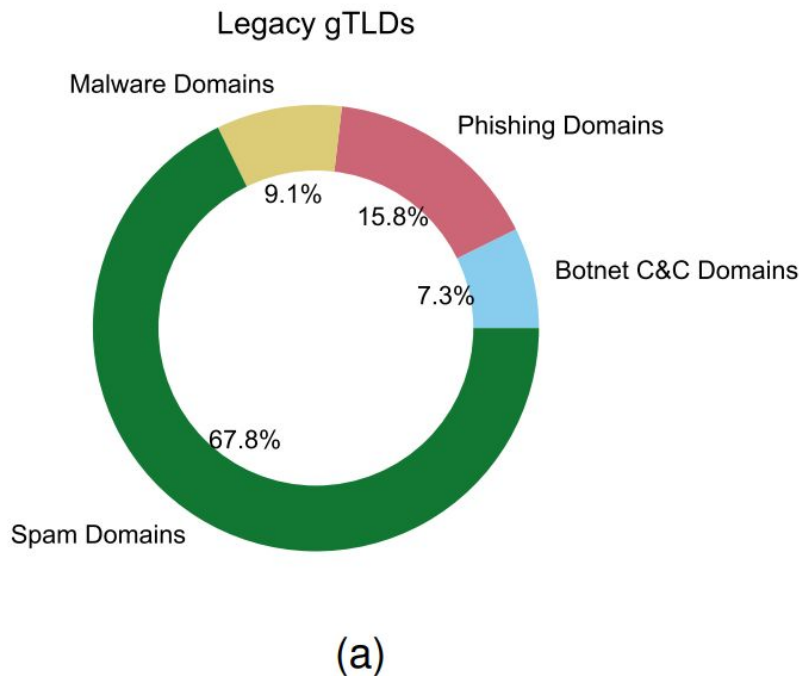
Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.

[GAC Statement on DNS Abuse](#) (18 September 2019) quotes 2016 CCT report

referring to DNS Abuse as “intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names.”

DNS Abuse's definition is a topic of debate.

ICANN's [Domain Abuse Activity Reporting](#) (DAAR) *“identifies and tracks domain names identified as **threats to the security of the domain name ecosystem, known as DNS Abuse.**”*¹



DNS Abuse's definition is a topic of debate.

Outside ICANN....

...we don't talk about "DNS Abuse"

...we talk about "fraud", "crime"

e.g., **Phishing** enables both

Ransomware

Business Email Compromise (BEC)

measured not by # of domains seen being used, but rather by

\$ / ¥ / € loss,

of victims



DNS Abuse is addressable by ICANN policy. Within limits.

ICANN policy must be developed in accordance within the “picket fence” set by the [bylaws](#).

ARTICLE 1 MISSION, COMMITMENTS AND CORE VALUES

Section 1.1. MISSION

(a) The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "Mission").

(i)...to facilitate the openness, interoperability, resilience, security and/or stability of the DNS ...

(c) ICANN shall not regulate (i.e., impose rules and restrictions on) ... content ... outside the express scope of Section 1.1(a).

DNS Abuse is addressable by ICANN policy. Within limits.

Policies addressing DNS Abuse can appear in [Consensus Policies](#) and/or contracts. E.g. ~

- ICANN [registry agreements](#) include Public Interest Commitments

(see Specification 11, 3. a)

*“Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements **a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting** or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.”*

DNS Abuse is...

... a topic you will hear a lot about within ICANN.

Here are some additional resources you may wish to know about, relevant to conversations about DNS Abuse:

ICANN's [Domain Abuse Activity Reporting \(monthly\)](#), & [Framework for Registry Operators to Respond to Security Threats](#)

[GAC Statement on DNS Abuse](#)

[Competition, Consumer Trust, and Consumer Choice Review Team](#)
2018 Final Report included DNS Abuse Topics (p88)

[DNS Abuse Framework](#)

(a commitment by prominent Rr's/Ry's to take action against abuse)

[NetBeacon](#) (www.netbeacon.org)

(receives reports of abuse, enriches them, routes to Rr/Ry/hosting parties)

[U.S. FBI Internet Crime & Complaint Center](#)

(U.S.intake for Cybercrime & Internet Fraud, publishes trends/alerts)

DNS Abuse is...

... something you're ready to talk about.

- Questions on DNS Abuse
/ Chat / Coffee

...RDS / “WHOIS” is next

WHOIS

29 OCT 69	2100	LOADED OP. PROGRAM E012 BEN BARKER BBV	CSK
	22:30	Talked to SRI Host to Host	CSK
		Left op. program running after sending a host dead message to imp.	CSK

COMPANY IMP LOG MONTH OF _____
 ADDRESS _____
 ENGINEER IN CHARGE _____
 COMPUTER SERIAL NO. _____

DATE	METER	PROBLEM & REMEDY	OPERATOR	DOWNTIME
10/13	9:30	Imp? is halted (I don't know why)	CSK	
		P = 10573 A = 0 B = 0 OP = 24200 X = 0 M = 76		
10/13	9:15P	Test started. Please don't touch.	MT	
10/14	4:40	Test in progress - will be checked tomorrow AM		
10/14	6:50pm	The above is unreadable and not signed. Please try harder.	Jon	
10/15	8:50	Sorry. Please leave amp running - test in progress	Marby	

What is WHOIS?

العربية 简体中文 [English](#) Français Русский Español

ICANN | LOOKUP

Registration data lookup tool

Enter a [domain name](#) or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

Dates

Registry Expiration: 2026-09-21 04:00:00 UTC

Updated: 2018-04-10 16:43:38 UTC

Created: 1993-09-22 04:00:00 UTC

Registrar Information

Name: CSC Corporate Domains, Inc.

IANA ID: 299

Abuse contact email: domainabuse@cscglobal.com

Abuse contact phone: tel:+1.8887802723

Technical:

Name: TBS Server Operations

Organization: Turner Broadcasting System, Inc.

Email: hostmaster@turner.com

Phone: tel:+1.4048275000

Fax: tel:+1.4048271593

Mailing Address: One CNN Center, 13N, Atlanta, GA, 30303, US

Administrative:

Name: Domain Name Manager

Organization: Turner Broadcasting System, Inc.

Email: tmgroup@turner.com

Phone: tel:+1.4048275000

Fax: tel:+1.4048271995

Mailing Address: One CNN Center, 13N, Atlanta, GA, 30303, US

Registrant:

Name: Domain Name Manager

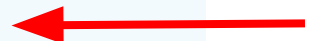
Organization: Turner Broadcasting System, Inc.

Email: tmgroup@turner.com

Phone: tel:+1.4048275000

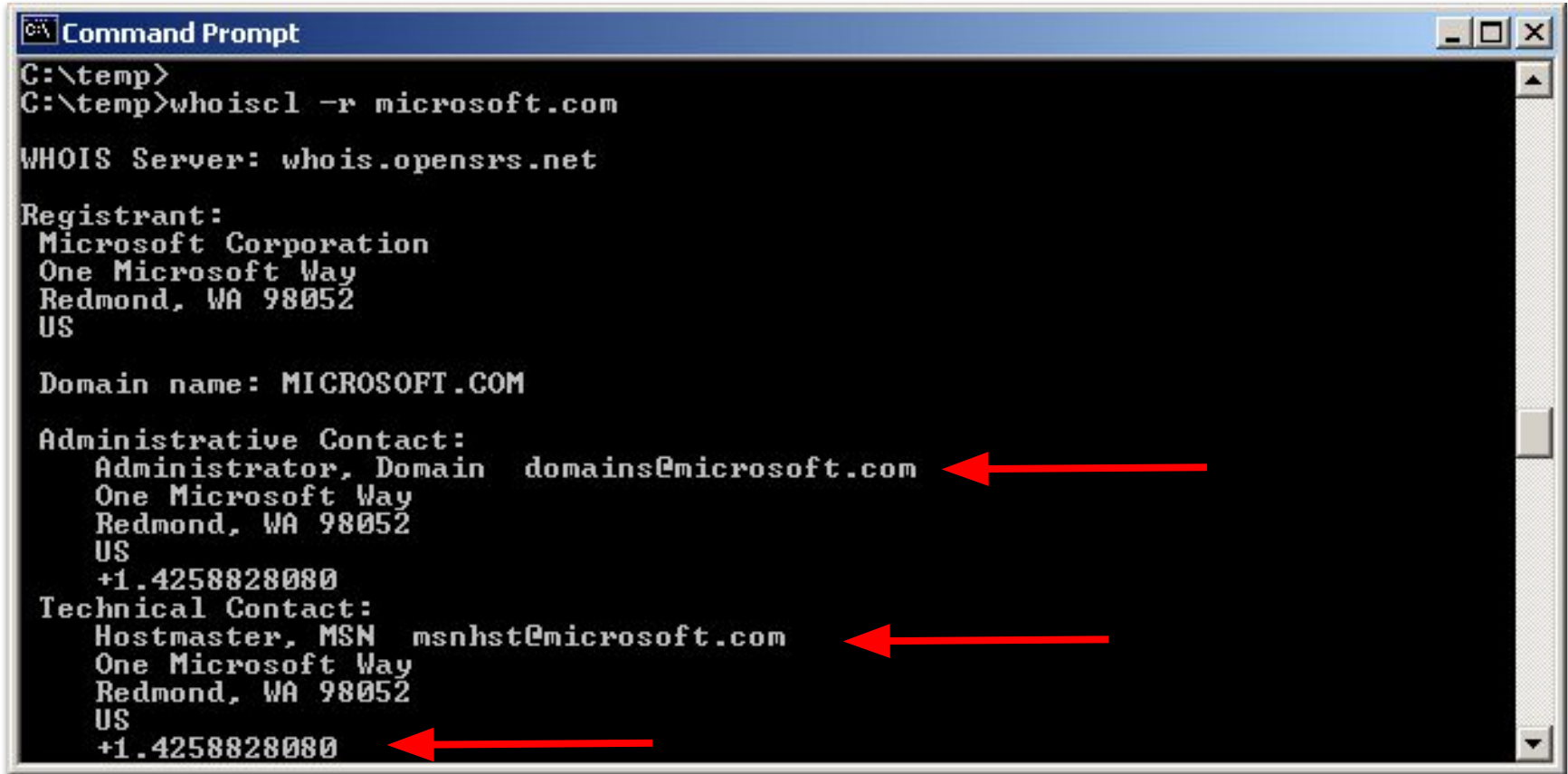
Fax: tel:+1.4048271995

Mailing Address: One CNN Center, 13N, Atlanta, GA, 30303, US



WHOIS...

What is WHOIS?



```
Command Prompt
C:\temp>
C:\temp>whoiscl -r microsoft.com

WHOIS Server: whois.opensrs.net

Registrant:
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Domain name: MICROSOFT.COM

Administrative Contact:
Administrator, Domain domains@microsoft.com
One Microsoft Way
Redmond, WA 98052
US
+1.4258828080

Technical Contact:
Hostmaster, MSN msnhst@microsoft.com
One Microsoft Way
Redmond, WA 98052
US
+1.4258828080
```


WHOIS...

... is changing.

العربية 简体中文 [English](#) Français Русский Español

ICANN | LOOKUP

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

Contact Information

Registrant:

Organization: ICANN

Mailing Address: California, US

Redacted for privacy:

some of the data in this object has been removed.

Technical:

Redacted for privacy:

some of the data in this object has been removed.

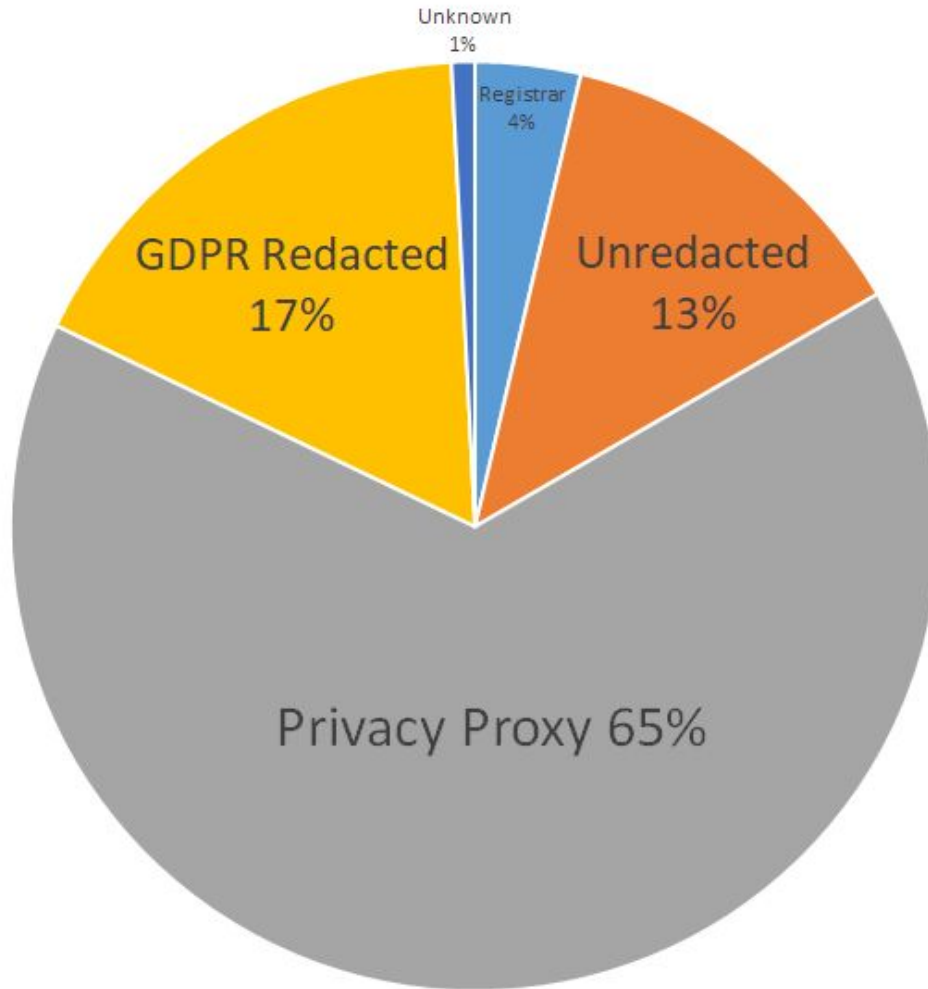
Administrative:

Redacted for privacy:

some of the data in this object has been removed.

From ICANN 68 presentation on COVID-19 Response

~1,300 domains were referred to registrars by the FBI for potential COVID-19 fraud/abuse



Registrant Information Status of Referred Domains

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

WHOIS...

... has an uncertain future.

GDPR compliant evolution of WHOIS policy is ongoing:

~~System for Standardized Access/Disclosure (SSAD)~~

≈ “WHOIS Disclosure System” (?)

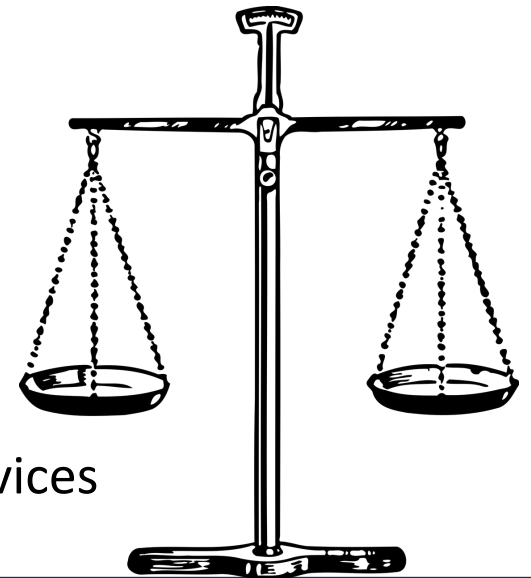
alongside conversations for

Registrant Data Accuracy

new technical protocol (RDAP)

Whois

≈ Registration Data Directory Services



WHOIS...

... has an uncertain future.

Contact Information

Registrant:

Name: Domain Name Manager

Organization: Turner Broadcasting System, Inc.

Email: tmgroup@turner.com

Phone: tel:+1.4048275000

Fax: tel:+1.4048271995

Mailing Address: One CNN Center, 13N, Atlanta, GA, 30303, US

Technical:

Name: TBS Server Operations

Organization: Turner Broadcasting System, Inc.

Email: hostmaster@turner.com

Phone: tel:+1.4048275000

Fax: tel:+1.4048271593

Mailing Address: One CNN Center, 13N, Atlanta, GA, 30303, US

Contact Information

Registrant:

Organization: ICANN

Mailing Address: California, US

Redacted for privacy:

some of the data in this object has been removed.

Technical:

Redacted for privacy:

some of the data in this object has been removed.

VS

The above is unreadable
and Not signed Please try
harder. JOU

END