ICANN76
GAC Capacity Development Workshop

DNS Abuse Mitigation

11 March 2023

Agenda

1. **Introduction to DNS Abuse** (15 min)

   Q&A

2. **SSAC Perspective on DNS Abuse** (15 min)

   Q&A

3. **DNS Abuse Survey of ccTLDs** (15 min)

   Q&A

4. **DNS Abuse Trends by ICANN org** (15 min)

   Q&A

5. **Discussion of Regional Perspective** (15 min)

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).**

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.

Outside ICANN….

…we don't talk about "DNS Abuse"

…we talk about "fraud", "crime"

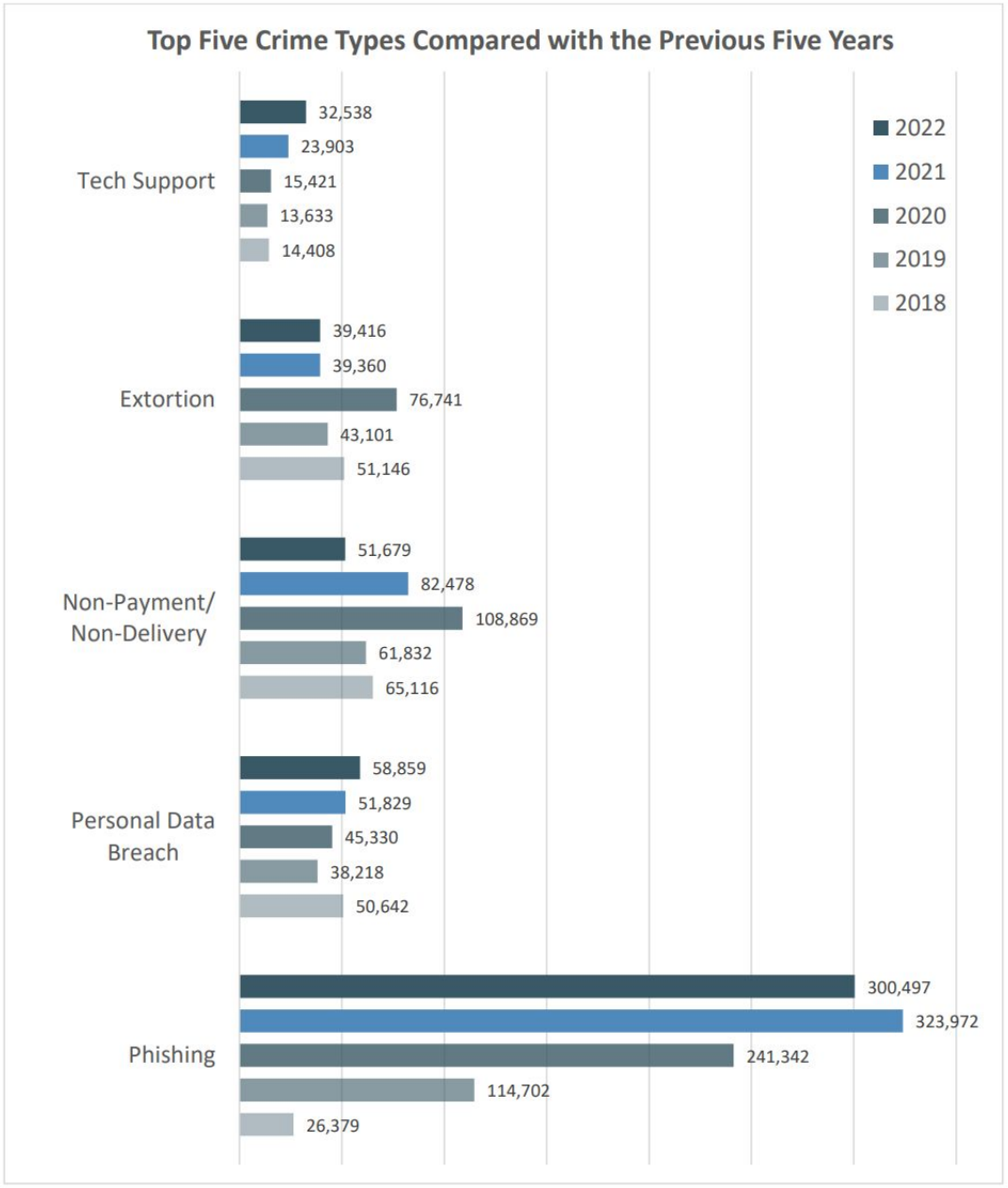
measured not by # of domains seen being used, but rather by

$ / ¥ / € loss,

# of victims

DNS Abuse's definition is a topic of debate.

ICANN | GAC
Governmental Advisory Committee



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).

Taking Action at the DNS Level

… vs at “Hosting Level”

DOMAIN NAME	TTL	TYPE	RECORD
RALNBOWBANK.COM.	14400	A	10.123.34.55

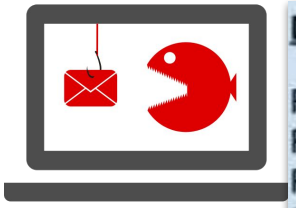
Registrar & **Registry** control this

Hosting Provider controls this

Images courtesy of Palo Alto Networks

Taking Action at the DNS Level

… vs at “Hosting Level”



DOMAIN NAME	TTL	TYPE	RECORD
RALNBOWBANK.COM.	160	A	101.14.66.2
RALNBOWBANK.COM.	160	A	222.14.10.4
RALNBOWBANK.COM.	160	A	23.124.228.102
RALNBOWBANK.COM.	160	A	101.14.66.22

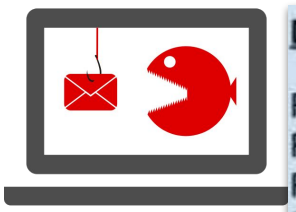
Registrar & **Registry** control this

Hosting Provider controls this

Images courtesy of Palo Alto Networks

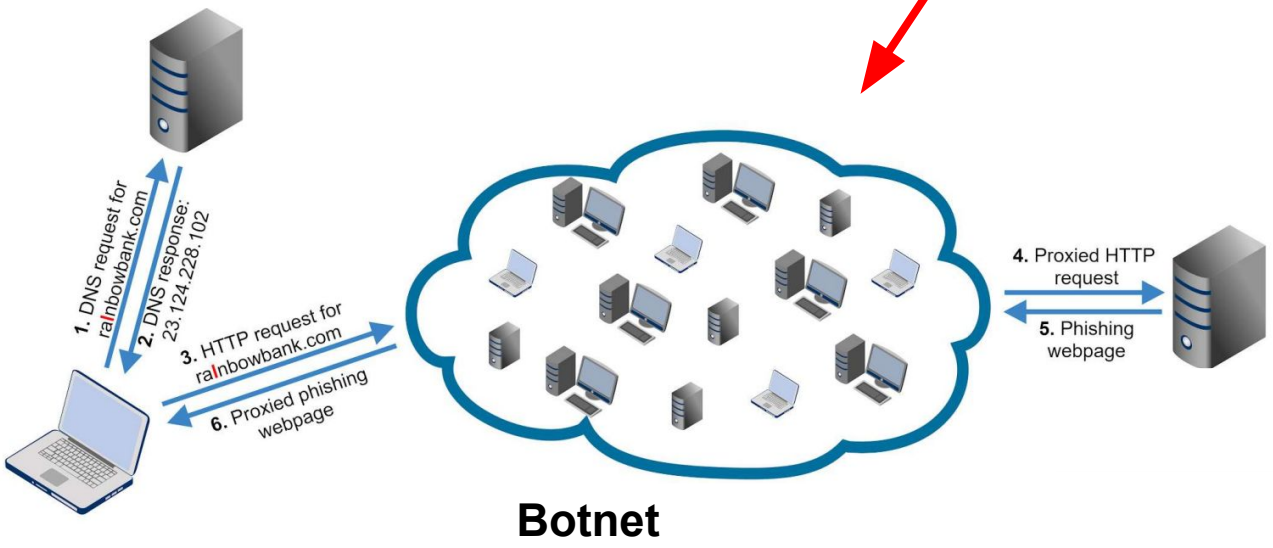
Taking Action at the DNS Level

… vs at “Hosting Level”



DOMAIN NAME	TTL	TYPE	RECORD
RALNBOWBANK.COM.	160	A	101.14.66.2
RALNBOWBANK.COM.	160	A	222.14.10.4
RALNBOWBANK.COM.	160	A	23.124.228.102
RALNBOWBANK.COM.	160	A	101.14.66.22

… + thousands of other IPs, each part of a “botnet”



Hidden
Hosting Provider…
IP = ????

Images courtesy of Palo Alto Networks

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 entities)

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