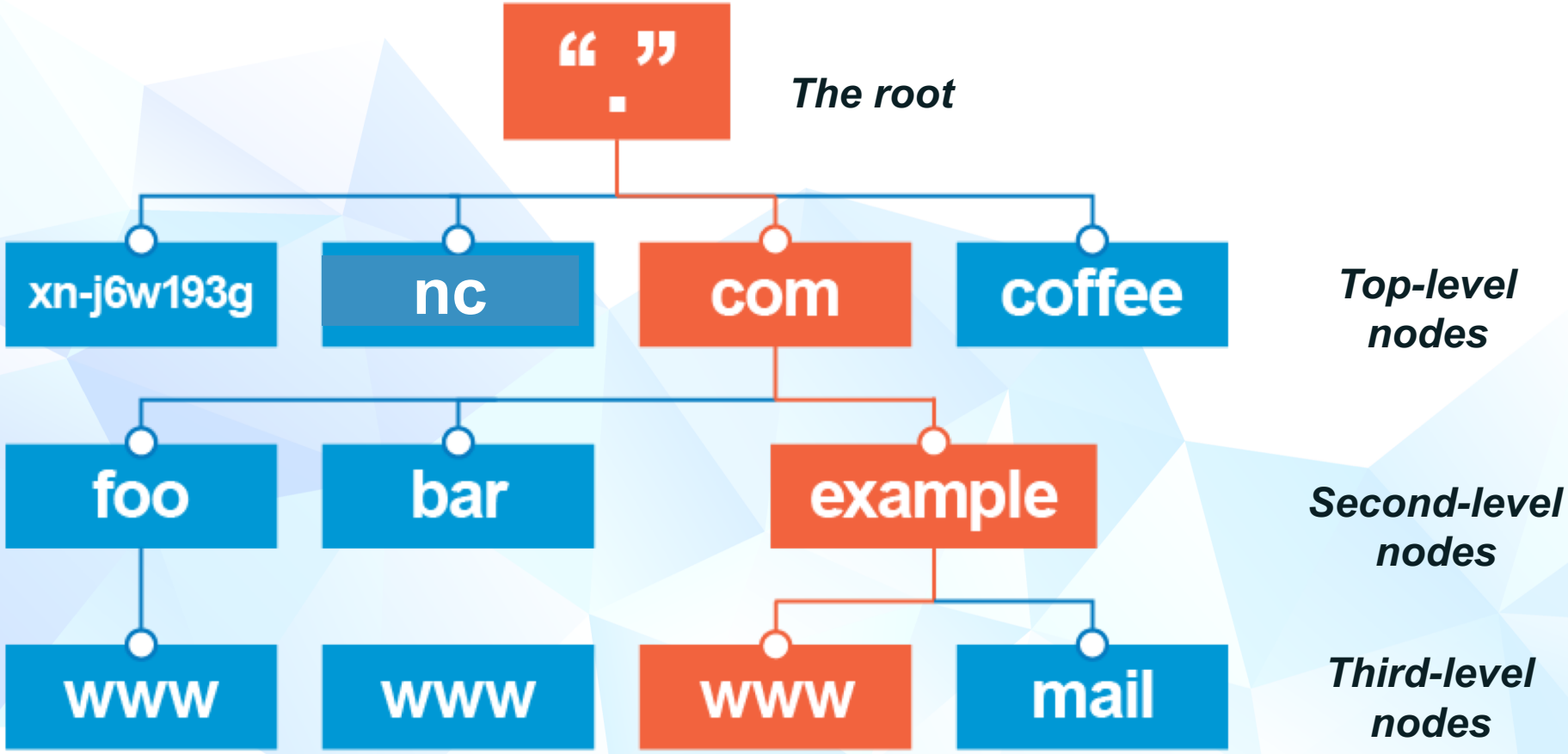
DNS Abuse Handling

FIRST TC – Noumea – New Caledonia

Champika Wijayatunga
Regional Security, Stability and Resiliency Engagement Manager – Asia Pacific

10 September 2018

The Domain Name System (DNS)



The DNS Ecosystem relationships

Ensuring the Security, Stability and Resiliency (SSR) of the DNS Ecosystem

- Engage actively with security, operations, and public safety communities to gather and process intelligence data that indicate (imminent) threats to DNS or domain registration service operations (the "DNS ecosystem").
- Facilitate or participate with these same communities in threat preparedness activities to protect against or mitigate threats to DNS ecosystem.
- Perform studies or analyze data to better understand the health and well-being of the DNS ecosystem.
- Coordinate DNS vulnerability disclosure reporting
- Lend subject matter expertise to build capability among ccTLD and public safety communities in subjects relevant to the DNS ecosystem, including DNSSEC, abuse or misuse of DNS infrastructures or operations.

Who?, What?, When?, Where?, How?

- Who is the target of your action?
  - Registrant
  - Hosting operator (Web, Mail, DNS…)
  - Network (ISP)
  - Registrar (or reseller),
  - Registry Operator
- What is the goal of the action?
- When will you act? In synchrony with others?
- Where in the world are the people, content, networks, or systems that you're targeting?
  - Many investigations involve parties or criminal assets in several jurisdictions
- How will you take action?
  - Court order, acceptable use, compliance violation

What should WHOIS display?

- Is the domain name to be transferred to a different sponsoring registrar?
- Are you transferring the registration? To whom? Have you investigated fee waivers?
- What name server is hosting name resolution?
- What status should the registry set for the domain?
  - E.g., prevent transfer, update, or delete?

Registration Directory Services (RDS)/WHOIS

- Registration Directory Services (RDS) is a publicly available and distributed directory containing information about registered domains such as icann.org
  - Each registrar and registry operator maintains its own database of registration data and provides access to this data via its own directory service

- RDS has evolved to serve the need of many different stakeholders, such as registrants, law enforcement agents, intellectual property and trademark owners, businesses and individuals

- The stable operation of the Internet relies on the basic concept that you cannot run a hierarchical and decentralized system like the Internet (a network of networks) if you cannot find the people who operate it to warn of problems and coordinate responses to operational issues

- In addition, the WHOIS system helps serve the public interest as it contributes to the security and stability of the Internet by providing contact information to support issues related to consumer protection, investigation of cybercrime, DNS abuse and intellectual property; as well as to address appropriate law enforcement needs.

Changes to WHOIS since 25 May 2018

What has not changed?

- Registration Data for all of the applicable fields will continue to be collected, transferred, and retained as before.
- Registrars and registry operators are required to continue to escrow Registration Data.
- Existing rules and procedures for rights protection mechanisms and the trademark clearinghouse remain in place.

VS

What has changed?

- Access to Registration Data will be tiered/layered. Personal data will be redacted for Registration Data processed in the EU. Third-party with legitimate interest may gain access to non-public Registration Data by contacting the relevant registrar/registry operator.
- Registrars will provide an anonymized email address or web form to contact registrants, admin and tech contacts.
- All other information for tech and admin contacts will be redacted.

WHOIS Before and After 25 May 2018

WHOIS record field	Before 25 May	Current WHOIS
Domain Name	Display	Display
Registry Domain ID	Display	Display
Registrar WHOIS Server	Display	Display
Registrar URL	Display	Display
Updated Date	Display	Display
Creation Date	Display	Display
Registry Expiry Data	Display	Display
Registrar Registration Expiration Date	Display	Display
Registrar	Display	Display
Registrar IANA ID	Display	Display
Registrar Abuse Contact Email	Display	Display
Registrar Abuse Contact Phone	Display	Display

WHOIS Before and After

WHOIS record field	Before 25 May	Current WHOIS
Reseller	Display	Display
Domain Status	Display	Display
Domain Status	Display	Display
Domain Status	Display	Display
Registry Registrant ID	Display	Do not display
Registrant Name	Display	Do not display
Registrant Organization	Display	Display
Registrant Street	Display	Do not display
Registrant City	Display	Do not display
Registrant State/Province	Display	Display
Registrant Postal Code	Display	Do not display
Registrant Country	Display	Display
Registrant Phone	Display	Do not display
Registrant Phone Ext	Display	Do not display

WHOIS Before and After

WHOIS record field	Before 25 May	Current WHOIS
Registrant Fax	Display	Display
Registrant Fax Ext	Display	Display
Registrant Email	Display	Anonymized email or web form
Registry Admin ID	Display	Display
Admin Name	Display	Display
Admin Organization	Display	Display
Admin Street	Display	Display
Admin City	Display	Display
Admin State/Province	Display	Display
Registrant Fax	Display	Display
Registrant Fax Ext	Display	Display
Registrant Email	Display	Display
Registry Admin ID	Display	Display
Admin Name	Display	Display

WHOIS Before and After

WHOIS record field	Before 25 May	Current WHOIS
Admin Organization	Display	Do not display
Admin Street	Display	Do not display
Admin City	Display	Do not display
Admin State/Province	Display	Do not display
Admin Postal Code	Display	Do not display
Admin Country	Display	Do not display
Admin Phone	Display	Do not display
Admin Phone Ext	Display	Do not display
Admin Fax	Display	Do not display
Admin Fax Ext	Display	Do not display
Admin Email	Display	Anonymized email or web form
Registry Tech ID	Display	Do not display
Tech Name	Display	Do not display
Tech Organization	Display	Do not display

WHOIS Before and After

WHOIS record field	Before 25 May	Current WHOIS
Tech Street	Display	Do not display
Tech City	Display	Do not display
Tech State/Province	Display	Do not display
Tech Postal Code	Display	Do not display
Tech Country	Display	Do not display
Tech Phone	Display	Do not display
Tech Phone Ext	Display	Do not display
Tech Fax	Display	Do not display
Tech Fax Ext	Display	Do not display
Tech Email	Display	Anonymized email or web form

WHOIS Before and After

WHOIS record field	Before 25 May	Current WHOIS
Name Server	Display	Display
Name Server	Display	Display
DNSSEC	Display	Display
DNSSEC	Display	Display
URL of ICANN Whois Inaccuracy Complaint Form	Display	Display
>>> Last update of WHOIS database	Display	Display

Next steps: Developing a Unified Access Model

Developing a Unified Access Model

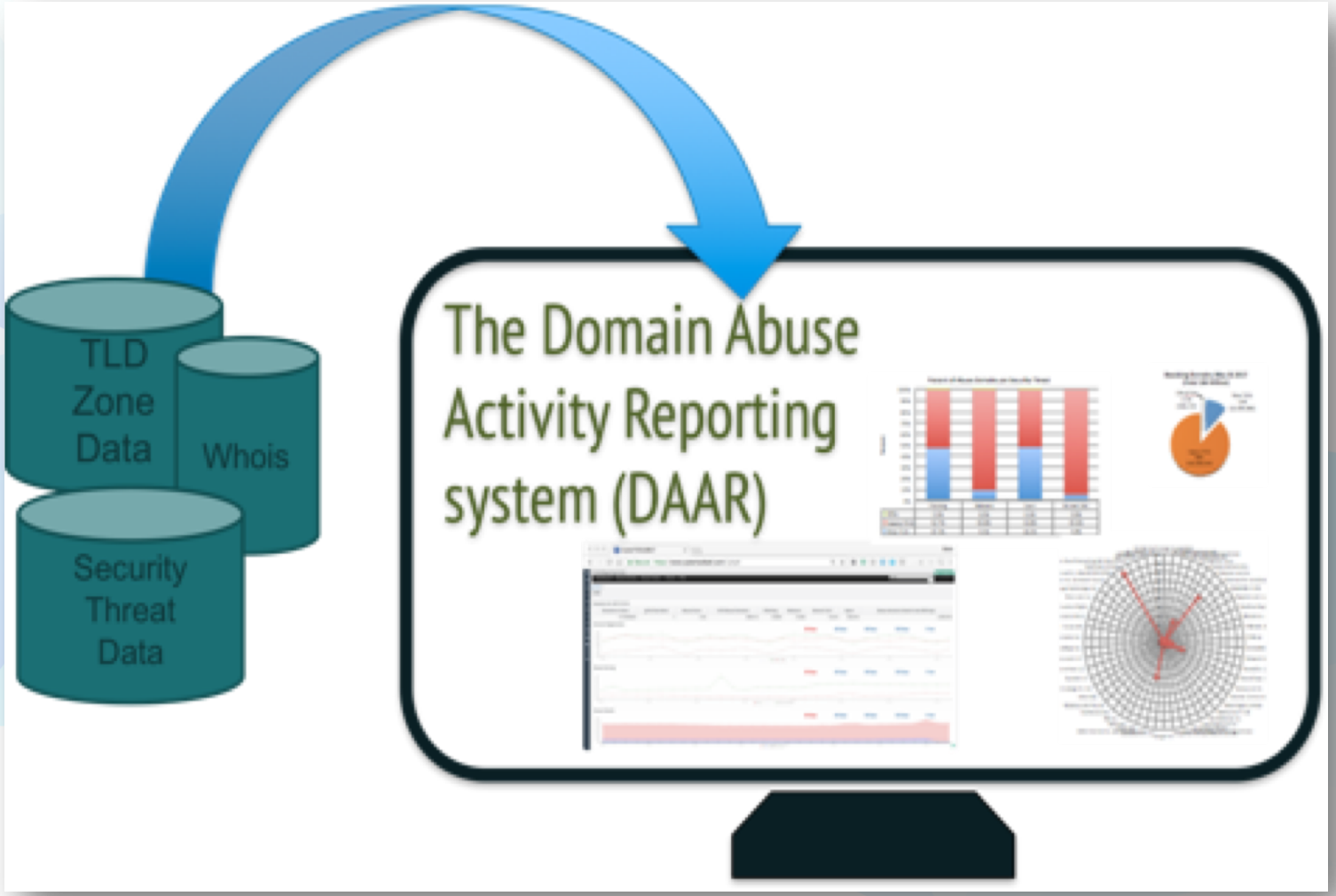
- **18 June 2018:** ICANN published "Framework Elements for a Unified Access Model for Continued Access to Full WHOIS Data" for community feedback. Goal is to develop a model in line with the GDPR to provide legal certainty for all parties
  - Elements included for community discussion: Eligibility, process and technical details, and codes of conduct
  - The community is invited to provide input at gdpr@icann.org

Expedited Policy Development Process

- The ICANN Generic Names Supporting Organization has initiated an expedited policy development process for the model. Read more here.

Authentication Technology for Access to Non-Public Registration Data

- A survey/study will be conducted to gather user input on authentication technologies available for for access to non-public registration data. Email gdpr@icann.org if you are interested in participating.


TLD Zone Data
Whois
Security Threat Data
The Domain Abuse Activity Reporting system (DAAR)

The Domain Abuse Activity Reporting system

A system for reporting on domain name registration and abuse data across TLD registries and registrars

How does DAAR differ from other reporting systems?

- Studies all gTLD registries and registrars for which we can collect zone and registration data
- Employs a large set of reputation feeds (e.g., blocklists)
- Accommodates historical studies
- Studies multiple threats: phishing, botnet, malware, spam
- Takes a scientific approach: transparent, reproducible

Project Goals

- DAAR data can be used to
  - Report on threat activity at TLD or registrar level
  - Study histories of security threats or domain registration activity
  - Help operators understand or consider how to manage their reputations, their anti-abuse programs, or terms of service
  - Study malicious registration behaviors
  - Assist operational security communities

The purpose of DAAR is to provide data to support community, academic, or sponsored research and analysis for informed policy consideration

ICANN Government Advisory Committee (GAC) Public Safety Working Group (PSWG)

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann