Abuse Reporting for Fact-Based Policy Making and Effective Mitigation

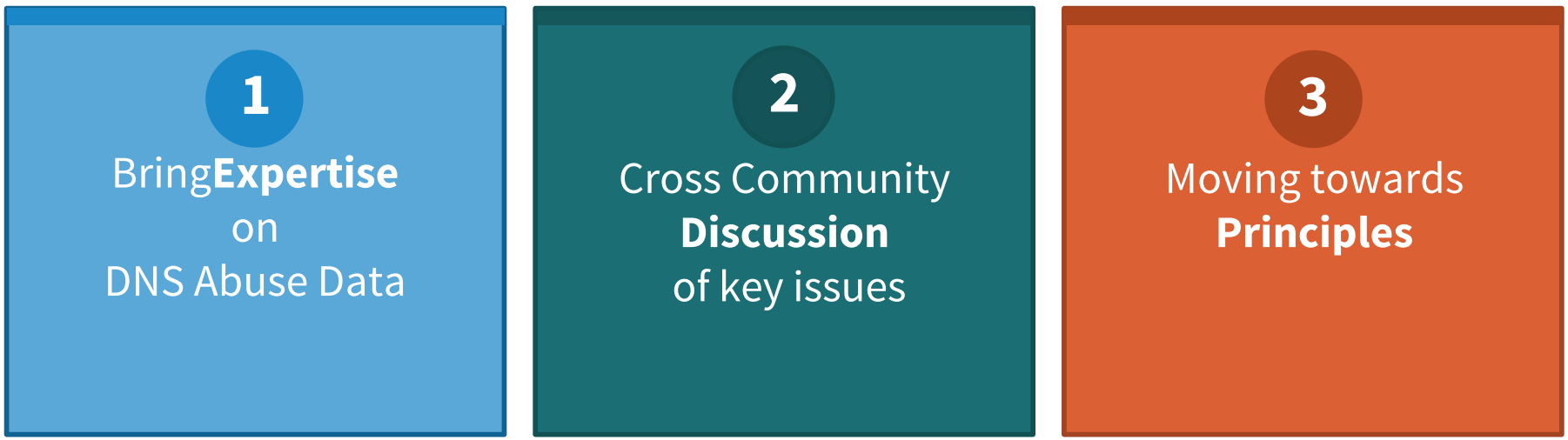
Cross Community Session

ICANN 60
30 October 2017

Objectives

Ensure the ICANN Community has **Reliable Public Actionable Abuse Data**

Goals of this Cross Community Session:



Session Moderated by:
Cathrin Bauer-Bulst, GAC PSWG Co-Chair (European Commission)
Iranga Kahangama, GAC PSWG Topic Lead (US FBI)

ICANN Org. Executive Sponsors:
David Conrad, CTO
Jamie Hedlund, VP Contractual Compliance & Consumer Safeguards

Agenda & Speakers

- Presentations
  - Domain Abuse Activity Reporting Project's Approach to Abuse Data
    David Conrad (ICANN)
  - DNS Abuse and Data Driven Policy Making
    Drew Bagley (Secure Domain Foundation, CrowdStrike)

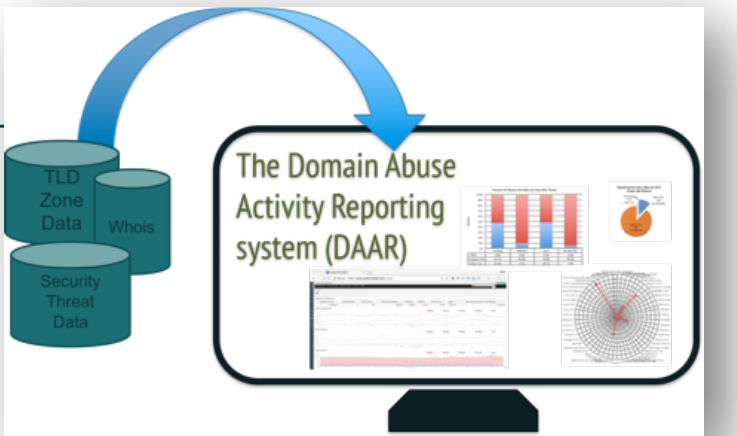
- Discussion with Audience and Panelists:
  - **Alan Woods** Registry Stakeholder Group
  - **Graeme Bunton** Registrar Stakeholder Group
  - **Tatiana Tropina** Non-Commercial User Constituency
  - **Denise Michel** Business Constituency
  - **Jonathan Matkowsky** Intellectual Property Constituency
  - **Rod Rasmussen** SSAC (Incoming Chair)
  - **Jamie Hedlund** ICANN Compliance & Consumer Safeguards

Key Questions for Discussion

1. How do we identify DNS Abuse in a reliable way ?
2. How to create effective and transparent Abuse Reporting ?
3. How could Abuse Reporting support registries and registrars in their prevention and mitigation efforts ?
   How could it be used in contractual compliance enforcement ?
   How could it be used in policy making ?

Topical Presentations

The Domain Abuse Activity Reporting System (DAAR)



David Conrad

ICANN60 Abuse Reporting Session
October 2017

The Domain Abuse Activity Reporting system

What is 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

DAAR Uses Many Threat Data Sets

- DAAR collects the same abuse data that is reported to industry and Internet users
  - The abuse data that DAAR collects are used by commercial security systems that protect millions of users and billions of mailboxes daily
  - Academic and industry use and trust these data sets
  - Academic studies and industry use validate these data sets exhibit accuracy, global coverage, reliability and low false positive rates

- Extensible framework
  - Experimenting with doing analyses using subsets of data

DAAR reflects how entities external to ICANN community see the domain ecosystem

Criteria for DAAR Data Sets (RBLs)

- Operational and security communities trust these for accuracy, clarity of process
- Chosen RBLs provide threat classification that matches our purposes
- Chosen RBLs have positive reputations in academic literature
- The RBLs are broadly adopted across operational security community
  - Feeds are incorporated into commercial security systems
  - Used by network operators to protect users and devices
  - Used by email and messaging providers to protect users

Reputation Block Lists: Protecting Users Everywhere

- RBLs in Browsers
  - Google Chrome uses APWG, and Safe Browsing URL Data
  - Firefox BlockSite extensions
- RBLs in the Cloud and Content-Serving Systems
  - Akamai use blocklists such as SURBL, Symantec, ThreatSTOP, and custom RBLs
  - AWS web application firewall (WAF) uses RBLs to block abuse or volumetric attacks
  - Google Safe Browsing blocks harmful or fraudulent advertising in the AdWords program
- RBLs in Your Social Media Tools
  - Facebook makes its ThreatExchange platform
- RBLs in the DNS
  - ISPs and private networks use Resource Policy Zones (RPZs) at their resolvers.
  - Spamhaus and others provide RBLs in RPZ format

Reputation Block List Uses: Private Network Operators

- RBLs in commercial firewalls, UTM devices
  - Admin guides from Palo Alto Networks, Barracuda Networks, SonicWall, Check Point, Fortigate, Cisco IronPort, and WatchGuard
  - TitanHQ SpamTitan, Sophos UTM, andProofpoint also provide RBL-based filtering to protect users from visiting malicious URLs
  - External RBLs mentioned: Spamhaus, SURBL, SpamCop, Invaluement, abuse.ch, Open ORDBL, Spam and Open Relay Blocking System **(**SORBS), Squidblacklist.org,
- RBLs in enterprise mail/messaging systems
  - Spam solutions from GFI MailEssentials, SpamAssassin, and Vamsoft ORF include Spamhaus or SpamCop RBLs available for Microsoft Exchange
- RBLs and Third-Party Email Service Providers (ESPs)
  - Amazon Simple Email Service RBL or DNS block lists
  - Look at ESPMail Exchange (MX) and Sender Policy Framework (SPF) resource records

Current Reputation Data Sets that Report to DAAR

- SURBL lists (domains only)
- Spamhaus Domain Block List
- Anti-Phishing Working Group
- Malware Patrol (Composite list)
- Phishtank
- Ransomware Tracker
- Feodotracker

SpamAssassin: malware URLs list
Carbon Black Malicious Domains
Postfix MTA
Squid Web proxy blocklist
Symantec Email Security for SMTP
Symantec Web Security
Firekeeper
DansGuardian
ClamAV Virus blocklist
Mozilla Firefox Adblock
Smoothwall
MailWasher

Why Is DAAR Reporting Spam Domains?

- The ICANN Governmental Advisory Committee (GAC) expressed interest in spam domains as a security threat in its Hyderabad correspondence to the ICANN Board of Directors.
- Spam is a major means of delivery for other security threats.
- Most spam messages are sent via illegal or duplicitous means (e.g., via botnets).
  - Spam is no longer singularly associated with email
  - Link spam, spamdexing, tweet spam, messaging spam (text/SMS)
- DAAR mainly measures domain names found in the bodies of spam messages
- MOST IMPORTANTLY FOR DAAR, spam domain reputation influences how extensively or aggressively security or email administrators apply filtering

Thank You

Visit us at **icann.org**
Email: email

 @icann

 facebook.com/icannorg

 youtube.com/icannnews

 flickr.com/icann

 linkedin/company/icann

 slideshare/icannpresentations

 soundcloud/icann

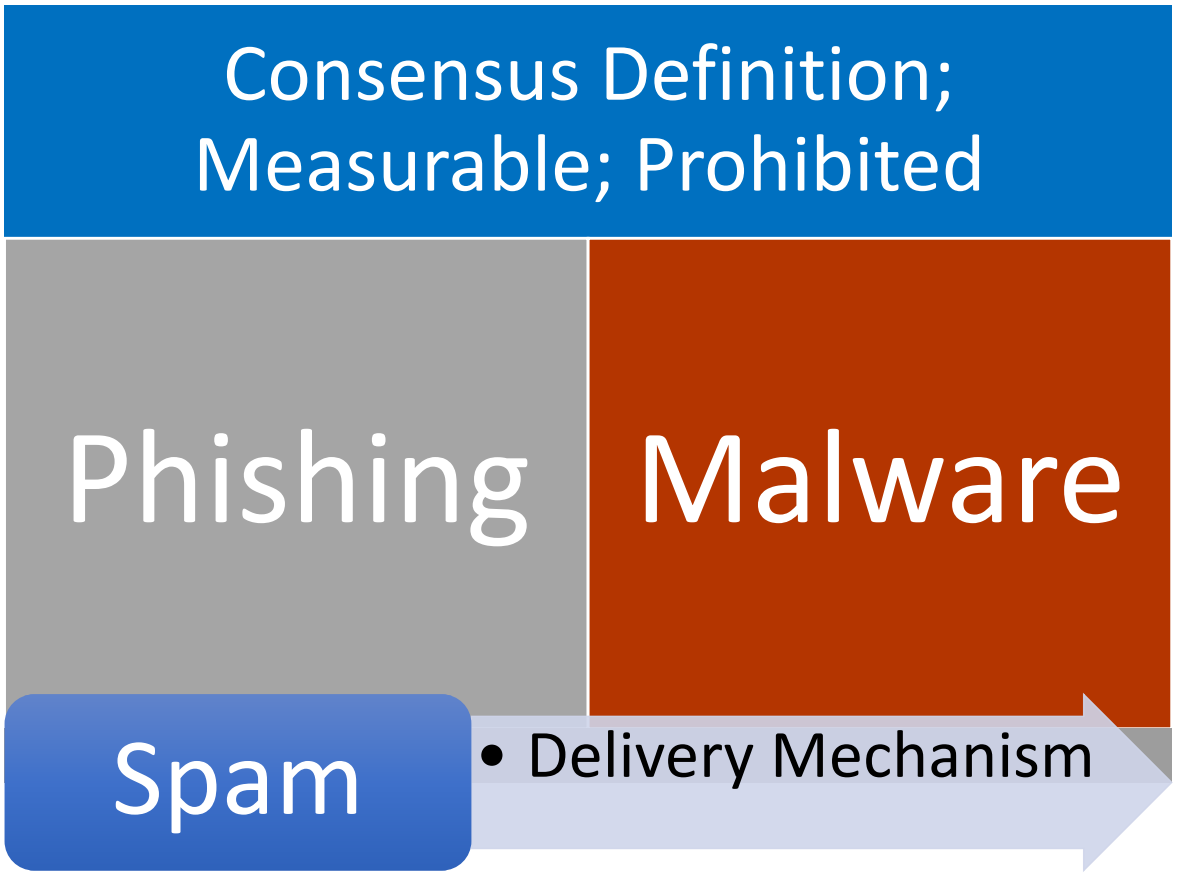
DNS ABUSE
AND DATA DRIVEN POLICY MAKING

Drew Bagley

Secure Domain Foundation/CrowdStrike

ICANN60, 30 October 2017

Begin with Technical DNS Abuse:



Statistical Analysis of DNS Abuse in gTLDs (9 August 2017)

Competition, Consumer Trust, and Consumer Choice Review Team abuse analysis

- Measured the effectiveness of technical safeguards put in place as part of the new gTLD program.
- Analyzed rates of spam, phishing, and malware distribution in the global gTLD from 2014 to 2016, distinguishing between legacy and new gTLDs.
- Data provided by Spamhaus, the Anti-Phishing Working Group, StopBadware, SURBL, the Secure Domain Foundation and CleanMX

Base Research Model

Explanatory Variable:
DNS Expansion

Response Variable:
DNS Abuse Rate

Intervening Variable(s)
Safeguards to Mitigate DNS Abuse

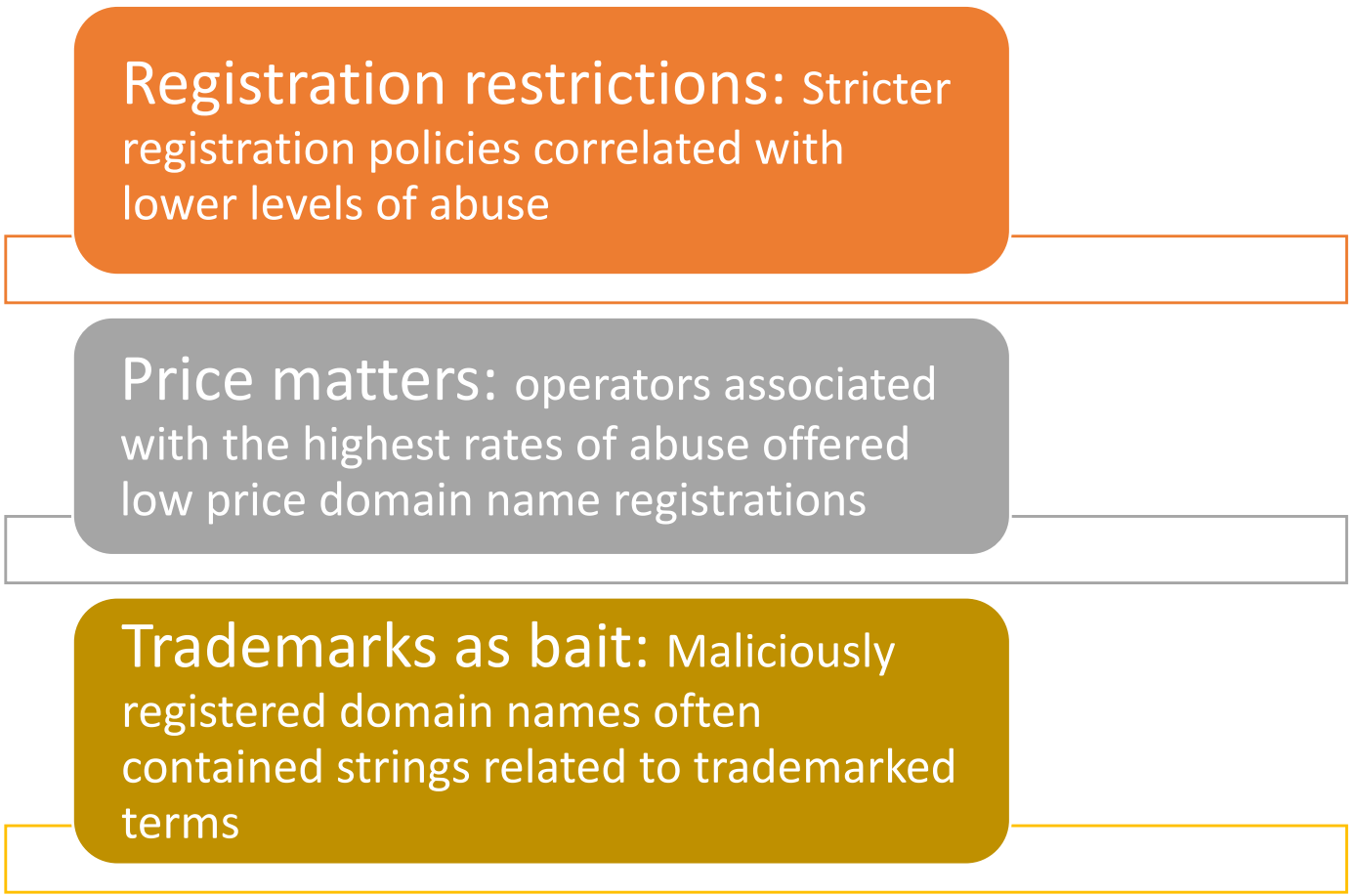
Potential proxy metrics:
- Number of domain names
  - Legacy TLDs
  - New TLDs
  - Entire DNS

What about…
- Pricing?
- Operational policies and/or practices?
- Systemic policies and/or practices?
- Cybercriminal preferences and practices?

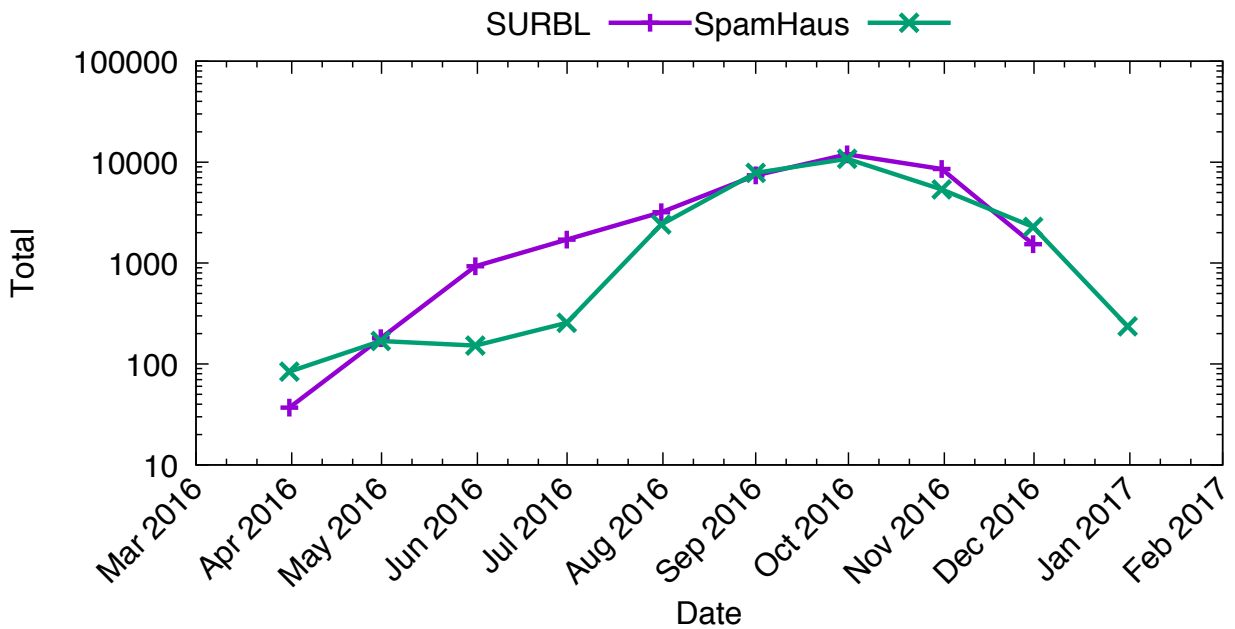
Potential proxy metrics:
- Spam rate
- Phishing rate
- Malware rate
- Others as relevant to the "effectiveness" objectives of the safeguards

Widespread Abuse is not Inevitable

- Abuse is neither universal nor wholly random



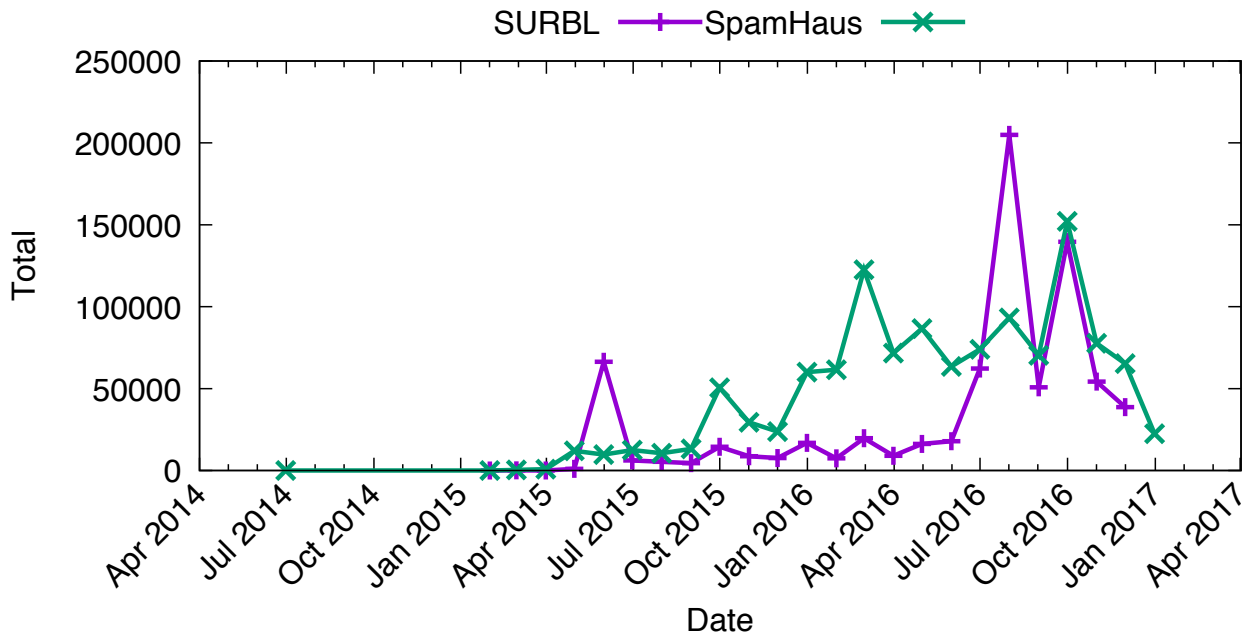
The Data Shows a Policy Gap



Nanjing Imperiosus Technology (China)

- More than 93% of the new gTLD registrations sold by Nanjing appeared on SURBL's blacklists.
- ICANN eventually suspended Nanjing in January 2017, citing its failure to comply with the Whois verification, abuse reporting, and record keeping requirements of the RAA and failure to pay ICANN fees.
- However, the sustained, unabated, high abuse rates alone did not constitute grounds for suspension.

The Data Shows a Policy Gap



Alpnames Ltd. (Gibraltar)

- Associated with a high volume of abuse from .SCIENCE and .TOP domain names.
- Used price promotions that offered domain name registrations for $1 USD or sometimes even free.
- Permitted registrants to randomly generate and register 2,000 domain names in 27 new gTLDs in a single registration process.
- Bulk domain names using domain generation algorithms are commonly associated with cybercrime.
- Alpnames remains ICANN-accredited.

DNS Abuse Data can be Actionable

- Inform policy to improve contracts and enforcement
- Identify and develop methods and best practices to prevent systemic, unabated abuse problems
  (i.e. CCT Review Team recommendations)
- Measure progress, success, and failures
- Evolve from reactive to proactive anti-abuse efforts

Discussion with Audience and Panelists

Discussion 1/3

How do we identify DNS Abuse
in a reliable way ?

Discussion 2/3

How to create effective and transparent Abuse Reporting ?

Discussion 3/3

How could Abuse Reporting support registries and registrars in their prevention and mitigation efforts ?

How could it be used in contractual compliance enforcement ?

How could it be used in policy making ?

Thank You

Visit us at **icann.org**
Email: email

 @icann

 facebook.com/icannorg

 youtube.com/icannnews

 flickr.com/icann

 linkedin/company/icann

 slideshare/icannpresentations

 soundcloud/icann