DNS ABUSE – OVERVIEW AND EFFORTS

Brian Cimbolic, General Counsel, PIR

AGENDA

1. DNS Abuse
2. Quality Performance Index
3. Framework to Address Abuse
4. Internet & Jurisdiction - Toolkits
5. Questions

DNS ABUSE

- **Malware** - malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems.
- **Botnets** - Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator
- **Phishing** - tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites.
- **Pharming** - redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning.
- **Spam****

DNS ABUSE – BACKGROUND

"Protecting the public from security threats and DNS Abuse is an important public policy issue …. If the public is to trust and rely upon the Internet for communications and transactions, those tasked with administering the DNS infrastructure must take steps to ensure that this public resource is safe and secure." – Government Advisory Committee, September 2019

PROACTIVE AND REACTIVE MEASURES

- **Reactive**:
  - All new creates run against numerous Reputation Block Lists on a daily basis
  - All registrations put through similar process at least once a month as part of DNS Abuse “sweeps”
    - Work with registrar channel to address (particularly necessary in compromise situation).
- **Proactive**:
  - Creation of “Quality Performance Index” to foster healthy(non-abusive) registrations and reward .

QUALITY PERFORMANCE INDEX (QPI)

- Cut out deep discounts
  - Poor quality names do not generally renew
- “Carrot and Stick”
- Low scorers cannot participate in promotions at all – no discount/rebate
- High performers earn higher discounts/rebates (though not so high that abuse creeps up)
- Participating registrars saw a marked improvement (4 percent) in renewal rates.
- Approximately 50 percent of all .ORG new creates were registered through the QPI program.

QUALITY PERFORMANCE INDEX (QPI)

- **Abuse rate****
- DNSSEC
- Site usage
- SSL Certificates
- Renewal rates
- Iterative

APPEAL MECHANISM

- .ORG Registrants now have the right to challenge decisions under the Anti-Abuse Policy to a neutral third-party.
- PIR subsidizes more than half of each appeal; if Registrant wins, PIR reimburses Registrant appeal fee.
  - Registrant must first utilize PIR-internal appeal process which has no cost. We do reverse ourselves sometimes, particularly if domain could be compromised.

FRAMEWORK TO ADDRESS ABUSE

- 11 signatories in October 2019, now more than 50 participating
- Includes both “generic” top-level domains and country-code TLDs
- Sets forth a set of recommended practices on when for Registrars (RRs)and Registries (RYs):
  - When a RR/RY **must** take action – DNS Abuse; and
  - When a RR/RY **should** take action – certain categories of Website Content Abuse
- Learn more at DNSAbuseFramework.org

WHAT CAN A REGISTRY/REGISTRAR DO?

CAN Suspend an entire domain

CANNOT Affect a single piece of content

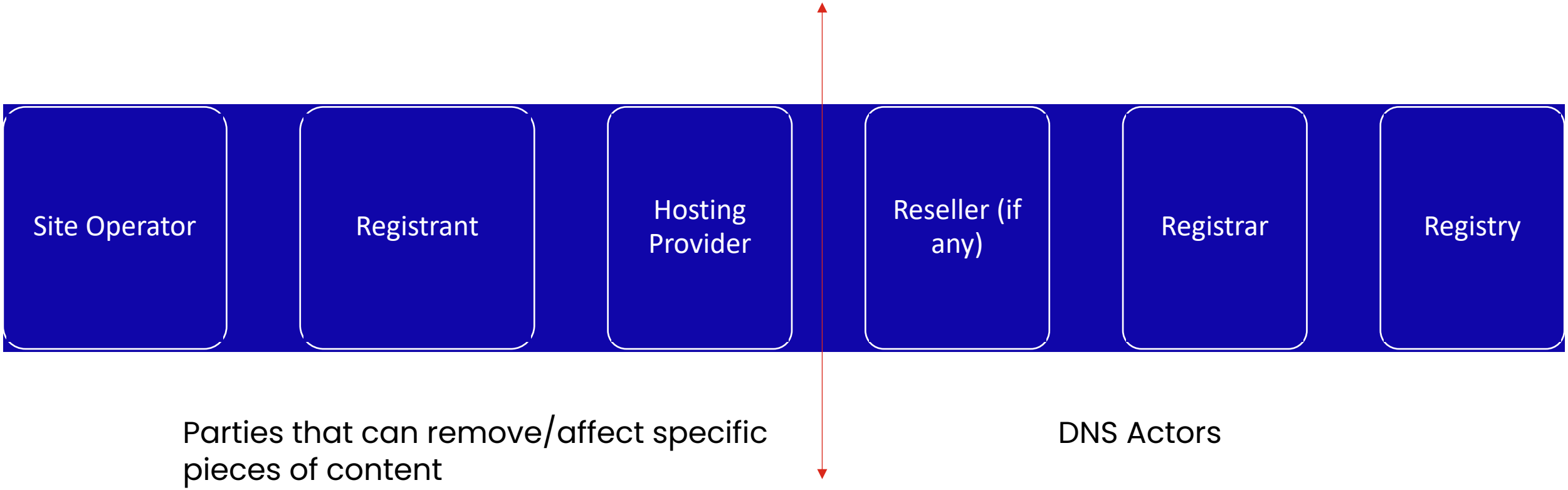
CANNOT Act at the URL Level

Instead, we have to act at the domain name level; it is all or nothing.

PROPORTIONALITY/COLLATERAL DAMAGE

- The blunt nature of using the DNS to address Website Content issues or DNS Abuse at the third-level (subpage.example.org) is typically disproportionate.
- If the abusive post is on a popular site or chat forum, the only remedy is to act on entire domain name.
  - This renders every non-abusive post inaccessible to end-users.
  - Knocks out associated email addresses as well.

CONTENT ABUSE REFERRAL PATH



WHEN SHOULD A RR/RY ACT ON WEBSITE CONTENT ABUSE

1. Child Sexual Abuse Materials (CSAM);
2. Illegal distribution of opioids online;
3. Instances of human trafficking; and
4. Specific and credible incitements to violence.

TRUSTED NOTIFIERS

- RRs and RYs are DNS operators, not trained to search for or locate things like CSAM or opioids online.
- Leverage expertise of third-party experts to find these instances for them.

- Trusted Notifiers have a higher level of confidence than outside referrals.
- These relationships typically spelled out in some contractual relationship.
- Examples include the US Federal Drug Administration (FDA) and Internet Watch Foundation (IWF).

INTERNET & JURISDICTION POLICY NETWORK

- Multistakeholder organization with more than 100 individuals from “governments, internet companies, technical operators, civil society, leading universities, and international organizations.”
- The Toolkits provide “substantive and procedural thresholds to determine when acting at the DNS may be appropriate as well as a framework for coordinating the interactions between relevant actors.”
- https://www.internetjurisdiction.net/domains/toolkit

I&J TOOLKITS - DOMAINS

- DNS Level Action to Address Abuse
- Phishing and Malware: A Procedural Workflow
- DNS Technical Abuse Choice of Action
- DNS Level Action to Address Technical Abuse: Due Diligence Guide for Notifiers
- Typology of Technical Abuse Notifiers
- Minimum Notice Components for Technical Abuse
- DNS Operators Decision Making Guide to Address Technical Abuse

QUESTIONS