ccNSO

DNS Abuse: Issues and Approaches

Xuebiao Yuchi (尉迟学彪)

CNNIC (.CN / .中国)

May 27, 2021

ccNSO

Outline

- Scopes and Concepts
  - "DNS Abuse" vs "Domain Name Abuse"
  - "Technical Abuse" vs "Content Abuse"
- Practices in Action
  - The DAAR
  - DNS Abuse Framework
  - Potential Updates
- Discussion

ccNSO

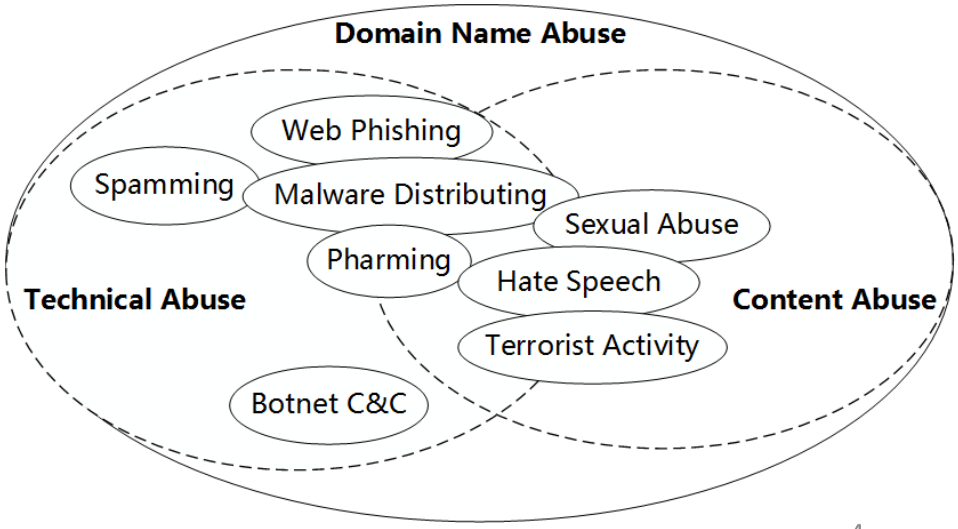
Scopes and Concepts

- "DNS Abuse" vs "Domain Name Abuse":
  - Usually, we treat this two terms equivalently in most of cases.
  - However, "DNS Abuse" can actually mean a lot more than "Domain Name Abuse".
    - All forms of misbehaviors (including DNS eavesdropping and security threats such as denial of service) that could lead to negative impact to the security, stability and privacy of the DNS infrastructure can be treated as "DNS abuse".
  - Therefore, when we are talking about DNS abuse, we are actually talking about the Domain Name Abuse.

Scopes and Concepts

- "Technical Abuse" vs "Content Abuse"
  - **Technical abuse**: malware, botnet, phishing, pharming, and spam*
  - **Content abuse**: trademark and copyright infringement, hate speech, terrorist activity, child sexual abuse, etc.

- ICANN is only responsible for "technical abuse" and thus registrars/registries are not contractually required to act against content abuse.
- However, the clear-cut distinction between technical and content abuse could be easily blurred in many practical scenarios.



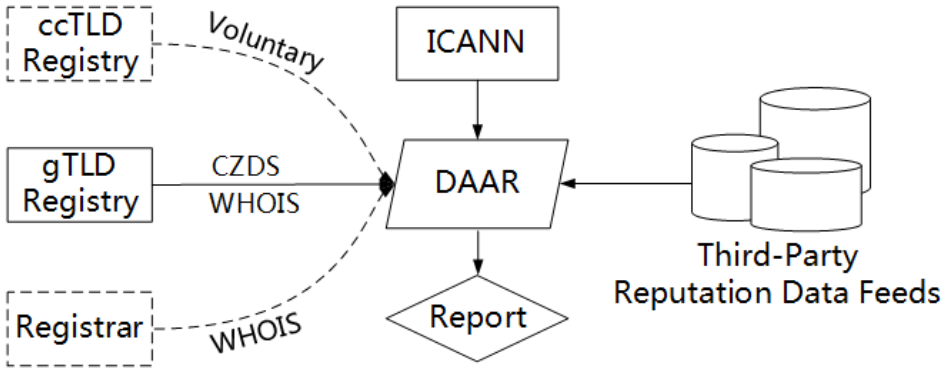
ccNSO

Outline

- Scopes and Concepts
  - "DNS Abuse" vs "Domain Name Abuse"
  - "Technical Abuse" vs "Content Abuse"
- **Practices in Action**
  - The DAAR
  - DNS Abuse Framework
  - Potential Updates
- Discussion

Practices in Action

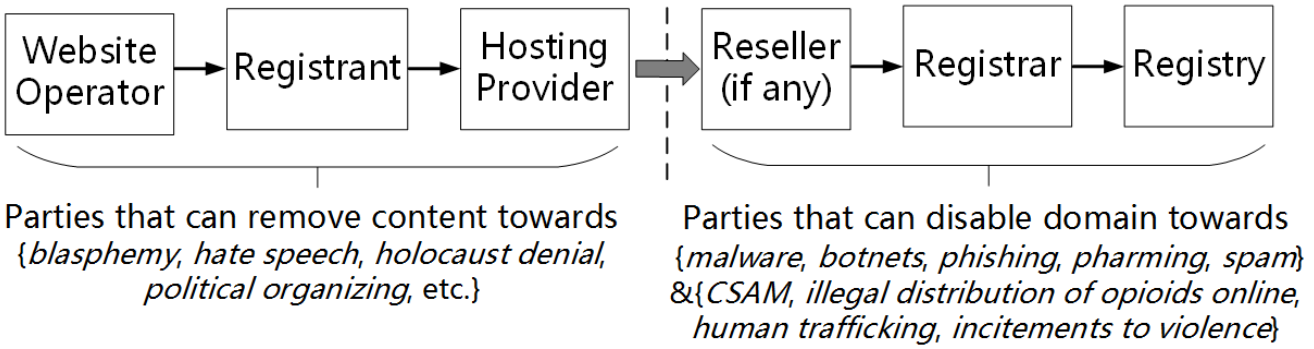
- The DAAR
  - Focuses on some limited forms of DNS abuse (phishing, malware, botnet, and spam).
  - By not including specific security threat information on a per registrar/registry basis, DAAR provides few actionable evidence of that abuse, which could be more valuable for registrars/registries.
  - The centralized data gathering and top-down information distributing schemes would lead to potential concerns from the community in privacy and neutrality issues.



Practices in Action

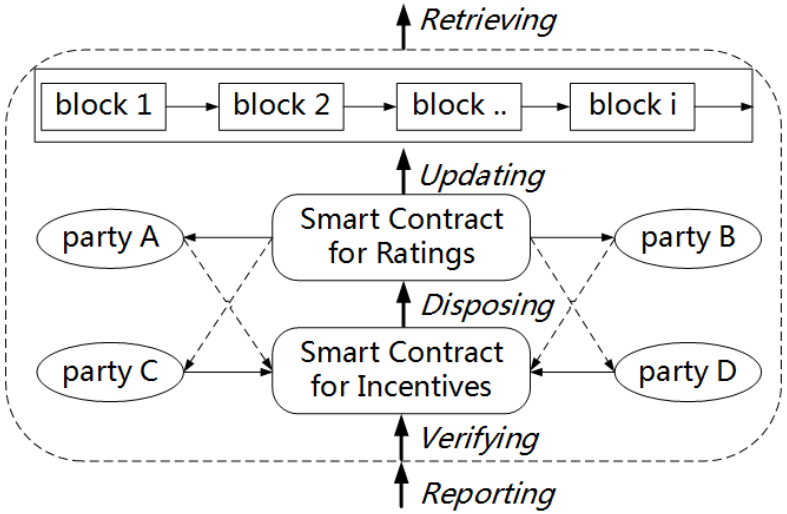
- DNS Abuse Framework
  - tries to emphasize and strengthen the roles that registrars/registries ought to take in DNS abuse handling, by explicitly pointing out as many forms of abuse as possible that need to be addressed straightforwardly at registrar/registry level.

  - Voluntary frameworks are not fully inclusive and have no incentive or penalty mechanism on those signed/unsigned parties, which could make themselves not so enforceable.



Practices in Action

- Potential Updates
  - We expect for some additional solution that could involve as many parties as possible, to handle all forms of abuse in a not voluntary only, but more decentralized & multilateral way.
  - A blockchain-based domain name abuse handling platform:
    - benefits all parties a lot by facilitating every single step of their DNS abuse handling procedure including abuse reporting, verifying, disposing and retrieving, while keeping their own pre-existing legacy system independent with each other.



ccNSO

Discussion

- There is no “one size fits all” solution for the DNS abuse handling, especially for the ccTLDs..
- An effective approach to handling DNS abuse by one party may not be effective for another.
- Besides the efforts made within each single ccTLD, we need to work out more across all ccTLDs.

ccNSO

Thanks!