May 27, 2021

CNNIC (.CN / .CN)

Xuebiao Yuchi (周汝超)

Issues and Approaches

DNS Abuse
Outline

• Scopes and Concepts
  • "DNS Abuse" vs "Domain Name Abuse"
  • "Technical Abuse vs Content Abuse"

• Practices in Action
  • The DAA
  • Potential Updates

• Discussion

• Practices in Action
  • The DAA
  • Potential Updates

• Discussion
Talking about the Domain Name Abuse:

Therefore, when we are talking about DNS abuse, we are actually talking about the Domain Name Abuse.

Usually, we treat this two terms equivalently in most of cases.

Scopes and Concepts:
Scopes and Concepts

- "Technical Abuse" vs "Content Abuse"

Technical Abuse:
- Malware abuse
- Botnet, phishing, pharming, and spam*

Content Abuse:
- Trademark, copyright infringement, copyright, terrorism, hate speech, 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.

"Technical Abuse" vs "Content Abuse"
Outline

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

• The DAAR focuses on some limited forms of DNS abuse (phishing, malware, botnet, and spam).
Practices in Action

- DNS Abuse Framework

Voluntary frameworks are not fully inclusive and have no incentive or penalty enforcement mechanisms on those signed/unsigned parties, which could make them less effective.

It is also possible that need to be addressed straightforwardly at registrar/registry level.

In DNS abuse handling, by explicitly pointing out as many forms of abuse as tries to emphasize and strengthen the roles that registrars/registries ought to take.

Parties that can remove content towards a registrar and/or an operator.

Doctoral organizing, etc. (blasphemy, hate speech, Holocaust denial, malware, botnets, phishing, pharming, spam, illegal distribution of opioids online, human trafficking, incitements to violence, etc.)

DNS Abuse Framework

• tries to emphasize and strengthen the roles that registrars/registries ought to take.

• Voluntary frameworks are not fully inclusive and have no incentive or penalty enforcement mechanisms on those signed/unsigned parties, which could make them less effective.

• It is also possible that need to be addressed straightforwardly at registrar/registry level.

Practices in Action
Practices in Action

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 systems independent with each other.
- possible to handle all forms of abuse in a not voluntary only, but more.

Potential Updates
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.
Thanks!