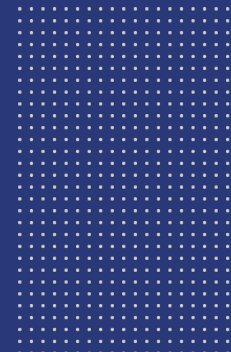




Mitigating DNS Abuse

APTLD 2024-09



The NetBeacon Institute

- Created in 2021 by Public Interest Registry (.ORG) in service of its nonprofit mission (formerly: The DNS Abuse Institute)
- Functionally separate from the operation of the registry
- Provides tools, education, and resources to reduce DNS abuse
- Everything we do is **free**

Mission: Reduce DNS Abuse.

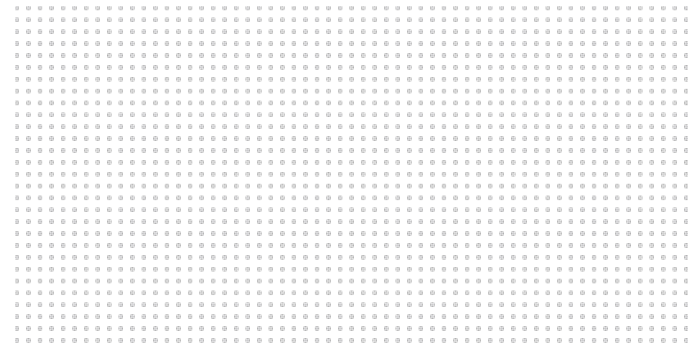
What is DNS Abuse?

DNS Abuse means **malware, botnets, phishing, pharming, and spam** (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse)

TL;DR: Harms appropriately mitigated at the DNS

Why is this Important for ccTLDs?

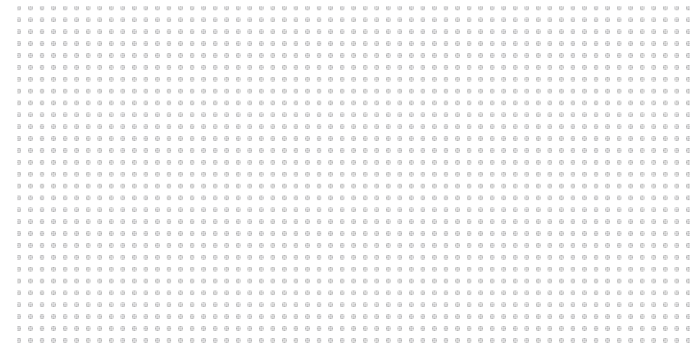
- gTLD changes may make ccTLDs more attractive for criminals
- Changes in technology make targeting smaller audiences cheaper and more effective
- Regulatory context is changing



Approaches to Mitigation

Do you have:

- The policies/Terms of Service in place in order to take action?
- The tools to collect, and manage reports of abuse?
- The processes and training to identify and mitigate abusive domains?



Reactive Approaches

Can we improve:

- The % of abusive domains identified?
- How quickly abusive domains are identified?
- How quickly identified abusive domains are referred to the appropriate registrar/registry?
- The information included in reports of abuse?
- The time it takes for mitigation to take place?

Preventative Approaches

- Incentive schemes
 - QPI from PIR
- Registration restriction
- AI detection
 - At registrar
 - At registry

