Domain Name Abuse Forum

Finding solutions for a safer .nz

Infrastructure abuse

Background

The Domain Name Abuse Forum has a broad focus, covering a variety of abusive behaviour online, specifically with respect to domain names. Abusive behaviour on the Internet is generally divided into three main categories: infrastructure abuse, registration abuse, and content abuse.

Working definition

Infrastructure abuse covers abusive behaviour that negatively impacts Internet infrastructure. This type of abuse can emerge in several forms and is often perpetuated using domain name registrations.

Phishing domain names
These are names that support web pages that claim to be a trustworthy entity like a bank. It is often associated with financial fraud but can also be used to steal identities.

Malware domain names
These are names that host or facilitate intrusive software that is installed without consent.

Botnet and command and control domain names
These are names that are used to identify hosts that control botnets. Botnets are collections of malware infected computers that can be used to perpetuate abusive activities.

Issues for consideration

Tackling infrastructure abuse can be especially challenging, as it is closely related to the security and stability of the Domain Name System (DNS). Since these issues pose significant threats to the DNS, it is typically considered appropriate for both registries and registrars to work to combat infrastructure abuse.

The Domain Name Commission's registration detail validation process (outlined in "our current approach") is not a fast process. It tackles various types of domain name abuse, including infrastructure abuse, using the principles of natural justice and procedural fairness.

The pace of this current approach is problematic, since many instances of infrastructure abuse require a rapid response to minimise harm.

InternetNZ

DOMAIN NAME COMMISSION nz

InternetNZ, operating the .nz Registry, tries to mitigate harm in this space by undertaking activities like intelligence gathering and sharing, and implementing certain technical protocols to limit the risk of infrastructure abuse. The Registry monitors threat feeds and passes on relevant information to Registrars. Additionally, several security measures are in place to prevent a large-scale attack on the .nz Registry infrastructure, which include:

- mechanisms like DNS response rate limiting to help prevent .nz Registry infrastructure from being used as part of a DNS amplification attack on other organisations
- serving the .nz DNS service from a widely distributed Anycast network with many nodes and providers both nationally and globally to help mitigate the risk of a denial of service attack taking the .nz DNS infrastructure offline.

The Registry also maintains rate limiting technology to protect registration data from bulk harvesting. More recently, the Port 43 protocol was changed to limit the information returned. Finally, registrants in the .nz space have the option to use DNSSEC to improve website security.

Questions

- Is registration detail validation process fit-for-purpose when tackling infrastructure abuse, or is a speedier solution required?
- Should one entity have sole responsibility for handling infrastructure abuse? Is this an issue that should be left to the registries to address?