Combatting DNS Abuse - Registry Operator Available Actions

The gTLD Registries Stakeholder Group is pleased to announce our "Output Series" of topic-by-topic guides on issues related to DNS Abuse. For the purposes of each "Output Series" guide we rely on the Contracted Parties House agreed definition of DNS Abuse:

> DNS Abuse is comprised of five categories of technical abuse: *phishing, pharming, malware, botnets and associated spam*.[1]

This first output in our series identifies actions registry operators can take in response to DNS Abuse for Compromised Domains; Maliciously Registered Domains; and Unregistered Domains (also known as domain generating algorithms or DGAs).

Registry Operator

A domain name registry is the technical operator and manager of a Top Level Domain (TLD). When a member of the public registers a domain name, they do so through a registrar – an organisation that registers domain names for the public. The person/entity who registers a domain name is known as the registrant.

Registries do not host content and therefore *cannot* remove a piece of content from websites- the only way to remove content from the Internet is to delete it from the computer that hosts it via the hosting provider, or permanently remove that device from the Internet.[2] Registry operators can work with registrars and registrants to resolve abuse, or they can take some limited and blunt actions themselves. When taking action at the registry level it is important to consider the effectiveness and proportionality of an action and potential unintended consequences. For example, registry action necessarily impacts the entire domain name of concern, it cannot be targeted at subdomains (e.g., "subpage.example.tld").

Registrant Culpability

A registry operator cannot always assume that reports of DNS Abuse are, by default, attributable to the actions of the registrant. As a preliminary review point, the registry operator must consider broadly two types of malicious behaviour, which ordinarily necessitates a different approach to mitigation from the parties involved. This is the first and sometimes essential distinction when addressing DNS Abuse: determining whether the domain was maliciously registered or if the domain has been "compromised."

---

[1] Contracted Parties House, *CPH Definition of DNS Abuse*, https://rrsg.org/wp-content/uploads/2020/10/CPH-Definition-of-DNS-Abuse.pdf.

[2] For more introductory information on content and domain registries: Council of European National Top-Level Domain Registries (CENTR). *Domain name registries and online content.* https://centr.org/library/library/policy-document/domain-name-registries-and-online-content.html

Compromised Domains

A domain name has been compromised when an otherwise legitimate (non-abusive) domain, or the web site or service hosted at that domain, has been "taken over" by a third-party for the purposes of DNS Abuse without the consent (and usually without the knowledge) of the registrant. Registries can do little to directly remediate a compromised domain; instead, they can work with the sponsoring registrar, who is in a better position to get control of the domain back in the hands of the registrant, which also has the effect of addressing the DNS Abuse.

Maliciously Registered Domains

Unlike compromised domains, malicious registrations are made for the purpose of engaging in DNS Abuse. Two existing documents summarize the options a registry has available to it from a technical perspective when it has identified a maliciously registered domain engaged in DNS Abuse.

- The "Framework for Registry Operators to Respond to Security Threats " is a document that was jointly drafted by the Government Advisory Committee Public Safety Working Group (PSWG) and domain registries.
- The Internet and Jurisdiction Policy Network has issued guidance entitled "DNS Technical Abuse: Choice of Action," which explains the technical actions available to registries and registrars and their impacts in mitigating DNS Abuse. …

As explained in those documents, there are essentially six options available to a registry operator when it has identified a malicious registration:

- **Refer to the sponsoring registrar**: Registrars have the direct contractual relationship with the registrant and should be given "a time-bound opportunity to investigate" the purported DNS Abuse.[3] If a registrar does not take action on the abuse, the registry maintains the right to directly take action.
- **Suspend the domain**: This is the most common and typically the most effective remedy for mitigating DNS Abuse. Suspending, or applying the status of serverHold to, the domain removes the domain name from the TLD zone file and the domain will no longer resolve.[4] This disrupts access and email will be disabled. The content of the website may still exist on a server and could be available via the IP address directly.[5]

---

[3] *Framework for Registry Operator to Respond to Security Threats,* https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en ("Security Framework").

[4] Id.

[5] Internet and Jurisdiction Policy Network, *DNS Technical Abuse: Choice of Action*, https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-114-Choice-of-Action.pdf ("I&J Choice of Action"), at 2.

- **Lock the domain:** Locking the domain on its own does not affect the content on the site or affect mail servers; it does however mean that the domain cannot be transferred, deleted or have its registration details modified.[6] Locking the domain may aid in the investigation of the domain by third parties.[7]
- **Redirect:** A registry can redirect a domain by changing the nameservers. This is often done as part of a government seizure (where the domain is redirected to a splash page along the lines of "This page has been seized by [governmental agency]") or for "sink-holing." A sink-holed domain logs traffic to help identify victims affected by DNS Abuse such as malware.[8]
- **Transfer:** A registry has the ability to transfer the domain, which may allow for the prevention of DNS Abuse, while still allowing the management of lifecycle, EPP status codes, and expiration of the domain.[9] This action is typically only done in response to a court order.
- **Delete:** Deletion is both ineffective since the domain can be re-registered and put to the same abusive purpose and extreme in that it is irreversible. For both of these reasons, suspension is almost always the better option to address DNS Abuse.[10]

Unregistered Domains (Domain Generating Algorithms)

As noted by the Security Framework, "[a] security threat may be associated with a domain name that is not yet registered. This can happen when the domain name is the result of an automatic Domain Generation Algorithm (DGA) associated with botnet activity."[11] These DGAs often involve tens of thousands of domains at a time associated with a particular botnet. To mitigate threats associated with these DGAs and potentially other large-scale botnets and malware, there are two actions a registry might take:

- **Reserve the domains:** A registry has the ability to put domains on a "reserve" list, which means that they are not registerable by potential registrants. This action will disrupt a botnet from propagating and does not require any specific ICANN permission.
- **Create the domains:** "Registering a potentially malicious domain name seems counterintuitive,"[12] but one of the most effective means of combating DGA botnets is by creating the domain at the registry level and then either suspending the domain, or sink-holing the domain for the purposes of victim identification.
    - Creating the domain directly may require permission from ICANN to waive contractual requirements: (i) prohibiting a registry from serving as its own

6 Security Framework.
7 I&J Choice of Action at 2.
8 Security Framework.
9 I&J Choice of Action at 2.
10 Id. at 3.
11 Security Framework.
12 Id.

registrar; and (ii) waiving ICANN fees associated with the created domains. This waiver process is handled through ICANN's Expedited Registry Security Request (ERSR) Process.