White Paper: A Framework to Disrupt Systemic DGA-Based Threats

Preface

The purpose of this document is to share our perspective on this topic of interest with the GNSO Council, GNSO policy staff and the ICANN community at-large.

This white paper builds on the CPH DNS Abuse Community session at ICANN 83[1] to provide additional points for consideration in the anticipated DNS Abuse PDP on the issue of mitigating DGA-based threats at a larger scale[2] in a coordinated and efficient manner.

The highlights are:

- DGA-based threats remain a prevalent security threat to the security and stability of the DNS.
- Existing approaches can benefit with improvements at the operational and policy levels.
- From an operational standpoint, there might be a place for a central coordinating role between those with the technical information (e.g., law enforcement and cybersecurity research) and those with the competency to disrupt DGA domain names at the DNS level (e.g., gTLD registries).
- From a policy standpoint, it might be worth considering ways to expedite security response waiver processes to reduce guesswork from gTLD registries on using those tools.
- Another important topic for potential deliberation is the responsibility of registrars who may hold restricted domain names.

Introduction to Domain Generation Algorithm (DGA)

Cybercriminals and botnet operators use DGAs to create a large number of domain names automatically that they can use to launch cyber-attacks, including some forms of DNS Abuse. DGAs can take different forms: random strings (e.g., ska89ash2i9ln.tld), concatenated dictionary words (e.g., city-best-car.tld), or anything in between.

Criminals use DGAs as dynamic rendezvous points for command and control. This technique allows them to evade detection through normal/standard methods and consequently, extend their malicious activity.

[1] https://www.rysg.info/wp-content/uploads/archive/CPH-DNS-Abuse-WG-ICANN-83-Session-Report-23-July-2025.pdf

[2] Example of systemic DGA-based threats: Conficker (https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf)

To counter these threats, there are special purpose organizations — law enforcement (LE) and/or cybersecurity organizations — that analyze the malware to reverse engineer the DGA that created them to recreate and predict future domain names for command-and-control communications. When reverse engineering is successful, the information may be used for analysis and disruption purposes.

Current Approach

Disruption of a DGA-based threat may be done at the DNS level via registry action, by preventing the bad actor from registering or activating the registered domain name in the DNS. A registry operator would either conduct mitigation on a voluntary basis (by obtaining validated DGA information proactively) or at the direction of an LE entity.

The RySG and PSWG worked on a voluntary and non-binding framework[3] to address DGAs associated with malware and botnets.

LE is most likely to be involved in large scale operations involving multiple TLDs. At the aggregate level, the current process is inefficient.

The stakeholders typically involve:

- Law Enforcement Agencies — conducting criminal investigation and victim notification.
- Cybersecurity Organizations — reverse engineering of DGA, technical analysis to help in mitigation approaches
- ICANN — manager of the root zone, and party and enforcer of the Registry Agreement.
- gTLD Registry Operator — the party to the Registry Agreement and responsible for managing a top-level domain registry. The gTLD Registry Operator may create a domain, block the registration of a domain name or disrupt the resolution of a domain name to prevent a bad actor from using the DGA domain name. More details in the framework.

Areas for Potential Improvement

1. Create a role, inside the ICANN community, for the collection and distribution of DGA-based threat information
    - As the global coordinator of the Internet's unique identifiers, ICANN may be well positioned to perform these functions.

[3] https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf

- Collection and evaluation of *systemic* security threats to the DNS, such as those posed by a botnet or malware DGA, are congruent with ICANN's mission to support the security, stability and resiliency of the DNS.
- ICANN has existing, or can adapt, systems to reliably and confidentially distribute the relevant DGA-based threat information to applicable registry operators.

2. ICANN's Security Response Waiver
    - The Security Response Waiver (SRW) service was established for gTLD registries "to request a contractual waiver for actions it might take, or has taken, to mitigate or eliminate a present or imminent security incident to a gTLD and/or the DNS".
    - In the event of a *systemic* security threat ICANN may streamline or expedite the process to issue applicable SRWs to gTLD registry operators (e.g., a DGA SRW Protocol).

3. Disposition of DGA domain names
    - gTLD registries generally have the contractual rights and technical capabilities to disrupt the threat of *unregistered* DGA domain names to prevent miscreants from using them (e.g., reserving a domain name, creating a domain name). In certain cases, they may need an SRW. See Framework for additional considerations about registry actions.
    - In some instances, a DGA domain name might be already registered but dormant (e.g., not yet activated by the cybercriminal). In these specific cases, a gTLD registry may suspend the domain name to disrupt the resolution in the DNS. In other instances, the desired action is for the DGA domain name to continue to resolve in the DNS but under controlled name servers to allow for analysis and/or victim notification (i.e., sinkholing).
    - In the latter cases (i.e. registered DGA domain names), the sponsoring registrar is often burdened with the financial responsibility of registry fees.

Potential Assumptions and Policy Questions for a narrowly scoped PDP

CPH DNS Abuse WG Principles for a DNS Abuse PDP

- Narrow in scope: the issue is short and constrained—to solve for a specific, definable, problem.
- Technology agnostic: the discussion avoids prescribing specific tools—because tools can become obsolete over time.
- Business model agnostic: discussions should take into account the diversity of contracted parties—our aim is for a uniform framework that can be adapted to unique business realities.

Policy Questions

1. Should there be a centralized coordinating role within the ICANN community to perform the collection and distribution of systemic DGA-based threat information to help protect the security and stability of the DNS?
    1.1. What are the minimum parameters needed by a gTLD registry to contribute to the disruption of the security threat?
    1.2. What guardrails with respect to the threat information need to be put in place, for the collection and distribution of the information, by ICANN to the gTLD registries?
2. While the SRW is an established process and works for individual requests, are there ways to enhance the issuance process when an imminent threat to the security and stability of the DNS impacts several gTLDs?
    2.1. Should ICANN issue the SRW proactively? If so, under what circumstances?
    2.2. If an SRW cannot be granted proactively, are there ways to expedite the process? For example, providing a standard language template.
3. Should a registrar receive relief when a sponsored domain name is suspended or sinkholed by a gTLD registry pursuant to a DGA-based threat notice? If so, what type of remedies?
    3.1. Do remedies vary depending on disposition of the domain name, such as suspension or sinkholing?