Framework for Registry Operators to Respond to Security Threats – Draft Outline for Discussion

NGPC Proposal for Implementation of GAC Safeguards Applicable to All New gTLDs

Version 1.1 | 12 August 2015

1. **Introduction and Background**

- To Include references to:
    - New gTLD Program context: relevant GAC Advice, NGPC proposal, RA Specification 11
    - Context of this effort to Draft a Framework for Response to Security Threats: Initial consultation of Registries and GAC
    - References to relevant precedents in ICANN Community discussion regarding security threats and abuse mitigation
        - Discussion Paper on the Creation of non-binding Best Practices to help Registrars and Registries address the Abusive Registrations of Domain Names (Sept. 2011)
        - Registration Abuse Policies Working Group Final Report (May 2010)

2. **Objectives and Principles of the Framework**

- Consideration and references to:
    - NGPC Proposal for Implementation of GAC Safeguards Applicable to All New gTLDs (19 June 2013): "*ICANN will solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality.*"
    - Call for Volunteers to draft the Framework: "*ICANN is now seeking volunteers from affected parties to draft a Framework grounded in industry experience, accepted best practices (if any) and consultation with the memberships of relevant communities. Once drafted, this Framework will be subject to public comments*"

- Consider definitions of:
    - *Identified Security Risks* (in connection and consideration of with Spec 11 3b reference to *Security Threats* and other existing definitions of *Abuse* in registration or use of domains)
    - *Risk of harm*
    - *Accepted Best Practices*

- Consider input from preliminary consultation:
    - Reduce time to harm as mitigation objective

- Standardization/harmonization should not be an objective
- There should be no one-size-fits-all measures.
- Measures should be aligned with the objective and risk profile of TLDs
- Present industry with multiple solutions to choose from
- Recognition that Registries' capabilities are limited (no access to
- Registrant, cannot eliminate abuse)

3. Threat landscape assumptions and risk model

- Consider input from preliminary consultation:
  - Take into account evolutionary nature of threats in Framework approach
  - Need for a common taxonomy vs. per-registry taxonomies
  - Inclusion of spam in scope, as "gateway abuse"
  - Consideration of risk profile (or varying vulnerability levels) of TLDs

4. Monitoring and Detection Model

- Consider definitions of:
  - All statistical models and methodologies used: certain classes or categories of statistics must be collected, or activities monitored, to allow for periodic analysis of threats;
  - Metric models and methodologies used: metrics must be defined that allow for a data-corroborated, objective determination of whether or not harm has been inflicted as well as the extent of the harm;

- Consider input from preliminary consultation:
  - Frequency of threat analysis should vary with:
    - TLD risk profile (Brands: low frequency to no analyses)
    - Type of threat and likelihood of harm
    - Observed frequency of abuse reports or evolution of abuse over time
  - Frequency of analysis
    - TLDs should be continually monitored for abuse (high degree of time affinity, timeliness of detection is critical)
    - Threat detection must be performed real-time or daily
    - Data Collection should be continuous, daily or weekly
    - Processing and analysis of data should be done bi-annually
  - Nature of technical analyses should be left to the registry to determine and adjust
  - There should be cooperation of registries and registrars for registration security, including anomaly detection
  - Regarding the use of Block lists and reputation data feeds:
    - Use reliable data feeds, continuously kept up to date

        - Care should be given to false positive
        - Registries should be able to rely on their trusted lists or their mix of feeds
        - Block lists should be informational only, may be disproportionate for Brand TLDs
        - Block lists limitations: lack a standard of trust; lack of context on why/when entries created; latency of updates
        - It is inappropriate to prescribe use of Block lists: Problems with administration of evolution of list; Impact on industry perception (endorsement/criticism); opportunity for circumvention, or specific harm; Reports may not be actionable
    - Various reporting sources should be considered, including: Reports to abuse contact (may not be sufficient); Sampling of domains by registry if statistically significant (only mean to cover all IDN and countries?)
    - Various forms of monitoring should be considered: New approaches from academia, including threat prediction; Vulnerability scanning, passive DNS monitoring, canary accounts[1] …
    - Registries should be able to rely on their internal resources
    - Human intervention should be strongly recommended
    - Metrics should be subject to cost/benefit analysis
    - Metrics should include:
        - Summary of new abuse
        - Number and type of abuse per TLD
        - Absolute number of actionable identification and domains under management
        - Established industry metrics in relevant industry forums
        - Normalized indices

5. Reporting model

- Consider definition of:
    - A retention model for data and reports, including Data Privacy considerations;
    - A transparency and accountability models: data and metrics should be made available for ICANN or 3rd party analysis and corroboration; and

- Consider input from preliminary consultation:
    - Data collection may have policy and legal implication

[1] In analogy to the idiomatic expression "canary in a coalmine" (see here for a definition: https://en.wiktionary.org/wiki/canary_in_a_coal_mine), a canary account in an account set up for the sole purpose of monitoring whether it is accessed or not, as an early warning system for detecting potential compromission of systems, credentials and/or data.
This is related to the notion of "honeypot" which more generally is "a program that takes on the appearance of a service, a set of services, an entire operating system or even an entire network, but is in reality a tightly sealed compartment built to lure and contain an attacker" (see this link for more details).

- Use of reported data
  - For / Not for comparing TLD performance
  - Not for targeting contractual compliance action
  - To be discussed before defining metrics
  - Reporting should/should not be public unless all gTLDs are subject to such requirement after a PDP.
  - Confidential reporting should be permitted
- Type of reporting data
  - Lifespan of malicious activity
  - False positives
  - Nature of malicious activity
  - Hijacked domains
  - Percentage of fraudulent/criminal domains per registrar
- Reporting should be done on a quarterly basis

6. Mitigation model

- Consider definition of:
  - Suspension processes as per GAC advice,
  - Holistic measures[2], i.e., changes to operational practices that would mitigate abuses that are the result or consequence of how a RO manages its delegation

- Consider input from preliminary consultation:
  - Prevention against Registrars with history of abuse
  - Reporting suspected criminal offence to law enforcement in relevant jurisdiction

[2] Holistic measures would be any sort of system-wide measure that registry Operators determine would improve security, stability and resiliency, reduce threats, etc.
Below are examples to illustrate what "holistic" means in the Spec 11 context (please bear in mind that these are examples only):
1) Fast Flux mitigation: Fast flux is a technique where an attacker sets the TTL for a resource record very low, and alters the binding between a name and IP address frequently, to thwart threat identification and isolation. A possible holistic measure to mitigate fast flux would be an adopted practice where registries or registrars would reject attempts by a registrant to set RR TTLs below a minimum value. This measure could make Fast Flux less useful to attackers. (Please do not get caught up in considering what the value might be. It is just an example.)
2) New registration data validation: Registry operators could apply a set of validation checks to reduce the number of registration records with false or inaccurate data as registrations with such data are often malicious registrations.
3) Baseline elements of AUP: Registry operators could identify certain abuses of domain names as violations of a baseline AUP that is enforced by all ROs. For example, imagine a holistic measure where all registry operators were to treat domains demonstrated to be algorithmically generated for the purpose of botnet command and control communications as violating such an AUP.

7. Consultation with Relevant Communities

- Description of Consultation Opportunities (Consultation with specific community segments, Public Comments, etc.)
- Outcome of consultations

8. Useful material to be considered by the Framework Drafting Team

- Registries and GAC contributions for the development of a Framework for Registry Operators to conduct periodic security checks and respond to identified security threats (Dec. 2014 – Mar. 2015)
- Abuse policies of new gTLD Registries (July 2013 onwards) – *To be shared by Registries if applicable*
- Discussion Paper on the Creation of non-binding Best Practices to help Registrars and Registries address the Abusive Registrations of Domain Names (Sept. 2011): http://gnso.icann.org/en/issues/rap/discussion-paper-rap-best-practices-28sep11-en.pdf
- Registration Abuse Policies Working Group Final Report (May 2010): http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf
- Mitigating Malicious Conduct - New gTLD Program Explanatory Memorandum (Oct. 2009): https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf
- Relevant SSAC Reports

One World, One Internet

ICANN.ORG