Contractual Compliance Report on Registry Operator Audit for Addressing DNS Security Threats

17 September 2019

Table of Contents

Background

The mission of the Internet Corporation for Assigned Names and Numbers (ICANN) is to ensure the stable and secure operation of the Internet's unique identifier systems, including the Domain Name System (DNS). In carrying out its mission, ICANN is charged with ensuring the operational stability of a critical, shared global resource.

Over the course of several years, the ICANN community has raised concerns about behaviors that threaten the stability, security, and resilience of the DNS. For example, the Competition, Consumer Choice and Consumer Trust Review Team's final report includes a lengthy chapter on DNS infrastructure abuse and several related recommendations. Additionally, in its 2013 Beijing Communique, the Governmental Advisory Committee (GAC) identified several DNS security threats and advised the Board of Directors to incorporate provisions into the base Registry Agreement for Registry Operators to effectively address those threats. The Board accepted the advice and contractual obligations were incorporated into Section 3(b) of Specification 11 of the Agreement ("Spec 11 3(b)"), which states: "*Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.*"

In response to Community concerns, and as an organization with an obligation to act in the global public interest to help ensure the operational stability of a critical, shared global resource, ICANN has a responsibility to understand more about the security threats that impact the DNS. To better understand these threats, ICANN org implemented two initiatives: The Domain Abuse Activity Reporting (DAAR) project, which is a system for studying and reporting on domain name registration and security threat (domain abuse) behavior across top-level domain (TLD) registries and registrars, and audits focused on DNS security threats through the Contractual Compliance Audit Program.

Data collected from DAAR and through the course of the registry audit confirms that the vast majority of registry operators are committed to addressing DNS security threats. The prevalence of DNS security threats is concentrated in a relatively small number of registry operators. At the same time, it became clear that some Registry Operators interpret the contractual language of Specification 11 3(b) in a way that makes it difficult to form a judgment as to whether their efforts to mitigate DNS security threats are compliant and effective. To address this issue, ICANN org proposes to enter into a dialogue with Registry Operators to develop a shared understanding of the scope of Specification 11 3(b).

With the conclusion of this audit, ICANN will launch next an audit of registrars that will also focus on DNS security threats.

Executive Summary

The Contractual Compliance Audit Program is an ongoing and continuous activity. On 6 November 2018, ICANN Contractual Compliance (Compliance) launched a Registry Operator Audit for Addressing DNS Security Threats. This report summarizes the results of the audit that took place from November 2018 through June 2019.

The goal of this audit was to assess the extent to which Registry Operators (ROs) comply with their contractual obligations related to DNS security threats.

Any findings of non-compliance would correspond to specific obligations established in the Registry Agreement (Agreement).

Contractual agreements typically do not specify the questions and mechanics of an audit. It is a standard procedure in industry audits to seek information that would demonstrate compliance with the obligations. In this audit, we asked the ROs to show what processes, procedures and controls they use to fulfill the DNS security threat obligations. The November 2018 Registry Audit questions were tailored specifically for this purpose.

Summary of Findings:

High-level conclusions from the Registry Operator Audit for Addressing DNS Security Threats include:

- Most ROs undertake significant efforts to address DNS security threats[1], including efforts that are not grounded in any contractual obligations.
- The prevalence of DNS security threats is concentrated in a relatively small number of registry operators.
- The frequency of abuse also appears to be lower in some types of new gTLDs. For example, Reputation Block Lists (RBLs) currently do not identify threats originating from .brand gTLDs.
- Little information is available about the efforts to address DNS security threats undertaken by some of the legacy ROs, who have no contractual obligations to do so.
- In contrast, new gTLD registry operators are subject to obligations regarding DNS security threats (e.g., Specification 11 3(b)).
- Five percent (5%) of ROs were found not to be in compliance with their obligations under Spec 11 3(b) and remediated findings of non-compliance.
- Dialogue between Registries and ICANN org is needed to develop a shared understanding of the scope of RO obligations under Specification 11 3(b).

This report is provided for information purposes only. Information contained in this report should not be relied on to make commercial or investment decisions.

[1] For purposes of this audit, "DNS security threats" are listed in Specification 11 3(b) (phishing, malware, and botnets).

Registry Operator Audit

On 6 November 2018, ICANN Contractual Compliance (Compliance) launched a Registry Operator Audit for Addressing DNS Security Threats. This report summarizes the results of the audit that took place from November 2018 through June 2019.[2]

The goal of this audit was to assess the extent to which Registry Operators (ROs) comply with their contractual obligations related to DNS security threats.

The audit plan, scope, notifications, and risk-mitigation plan are published on ICANN's Contractual Compliance Audit page.

This audit consisted of six (6) phases with specific milestone dates and deliverables:

1) **Planning –** ICANN planned the audit scope and timeline.
2) **Request for Information –** ICANN issued a notice of audit to the selected contracted parties (the auditees). During this phase, the auditees compiled information and responded to the audit request. This phase followed the overall compliance approach.
3) **Audit –** ICANN reviewed the responses and, where applicable, tested and validated the responses to ensure compliance with the contractual obligations.
4) **Initial Report –** ICANN issued a confidential, initial audit report to each auditee. It contained the initial findings and requested the contracted party to address the findings or provide clarity, if needed.
5) **Remediation** – ICANN collaborated with the auditees to remediate any initial findings of non-compliance[3] discovered during the audit phase as appropriate.
6) **Final Report –** ICANN issued a confidential final audit report to each auditee. In addition, ICANN summarized the audit round in an overall audit report.

This audit focused on reviewing new gTLD RO processes and procedures related to the prevention, identification and handling of DNS security threats. Specifically, the testing focused on verifying the existence of RO security threat monitoring and reports and reviewing the reports against publicly available data.

ICANN also sought information from legacy ROs (including those with the largest volume of domain names under management) that have no contractual obligations with respect to DNS security threats in order to understand whether these ROs had nonetheless adopted procedures or processes to handle DNS security threats. While some of these ROs elected to share information about their efforts to identify and address DNS security threats, others declined to do so.

For new gTLDs, the audit focused on the Public Interest Commitment of Specification 11, Section 3(b) of the Base Registry Agreement. This provision requires ROs to periodically

[2] The audit population included all gTLDs, including legacy gTLDs that had executed an Agreement with ICANN as of November 2018, and excluded gTLDs that successfully completed the March 2018 audit round and one gTLD subject to the Emergency Back-End Registry Operators (EBERO) program. Review the list of gTLDs in scope of this audit round.

[3] Initial findings are instances found during the audit phase where auditees appear to be non-compliant. Confirmed findings are initial findings that are deemed valid after discussions with auditees during the remediation phase.

conduct a technical analysis to assess whether domains in the gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. In addition, ROs are required to maintain statistical reports on the number of security threats identified, including the actions taken as a result of the periodic security checks for the term of the Agreement. ROs are also required to provide copies of these reports to ICANN upon request. In this audit report, these reports are called "Security Threats Reports" (STRs).

Compliance sent a Request for Information (RFI) to the ROs, which included questions related to ROs' procedures with respect to DNS security threats and a request for a sample of STRs. In response, ROs generally provided STRs and described their mechanisms to monitor DNS security threats, as well as their actions to act on the identified domains.

To increase transparency into the audit, Compliance published the list of RFI questions and held two audit-outreach webinars with registries to address their questions and concerns. Read the responses to questions and concerns raised during the webinars.

The audit assessment was conducted by reviewing responses received to the RFI questions and by comparing data related to DNS security threats listed in RO's STRs to publicly available data provided by several DNS security threat monitoring organizations – Reputation Block Lists (RBLs) including Spamhaus, SURBL, Anti-Phishing Working Group, Phishtank, Malware Patrol, Ransomeware Tracker and Feodotracker. Compliance worked closely with ICANN's Office of the Chief Technology Officer (OCTO) team during the assessment process. The assessment also considered threats identified by RBLs with information provided by the ROs and reviewed relevant documentation, registry websites, and correspondence between the selected registry operators, their contracted Registrars, and Compliance.

During the audit phase, ICANN Compliance reviewed thousands of documents collected in multiple languages. Documents reviewed include Security Threats Reports, Anti-Abuse Policies, Law Enforcement Agency Reports and communications of reported threats. Registries were issued initial audit reports with initial findings and/or observations.

During the remediation phase, all registries collaborated and remediated findings of non-compliance.

Observations from the Audit

Means of security threat monitoring. ROs use various methods to monitor DNS security threats. Some use internal proprietary tools, while others use third-party products and services, such as Neustar's "Registry Threats Mitigation Service" (RTMS) and Dot Global Domain Registry Limited's "RegistryOffice Abuse Monitor" (ROAM), CSC Global, mambo$^+$, DOTZON, Afnic, AusCERT, Shadowserver, Telefonica, Secure Domain Foundation and Netcraft. Regardless of the methods used, Compliance sought to understand the frequency and types of threats included in each analysis.

ICANN cannot dictate whether and which RBLs should be used in security threat monitoring, but encourages ROs to consider including RBLs in their security threat monitoring.

Questions regarding the scope of RO obligations under Spec 11 3(b). ROs uniformly acknowledge their obligations to (1) conduct a technical analysis; (2) maintain statistical reports on the number of security threats identified, including responsive actions; and (3) to provide copies of these reports to ICANN upon request in the form of "Security Threats Reports"

(STRs). Many do not, however, interpret the Specification to obligate them to share the details of their existing DNS security threat programs with Compliance or information about specific domains investigated (as opposed to aggregated statistical information). It is important to note that these findings do not support a suggestion either that registry operators who interpret the scope of Specification 11 3(b) narrowly are tolerating DNS security abuses or that those who agree with ICANN org's broader interpretation are effectively mitigating DNS security threats.

Variance between RBL and STR data. Some (but not all) ROs who narrowly interpret Spec. 11 3(b) declined to provide detail beyond statistical data contained in their STRs. In these cases, it was not possible to determine the cause of any discrepancies between STR data and the number of security threats reported by RBLs, making it difficult to form a judgment as to whether their efforts to mitigate DNS security threats are effective. In these cases, Compliance reported the variance between the number of threats in the STRs and RBLs to the RO to facilitate self-assessment of the effectiveness of security threat-monitoring systems.

For those STRs that provided information about specific domains involved in abuse (rather than aggregated statistical data only), Compliance compared the domains listed to security threats identified by publicly available RBLs in the same timeframe. Any variances were presented to ROs as observations with a request to review the variances (reviewing a sample of domains was acceptable) to assess whether there were gaps in the ROs' monitoring systems and/or inaccuracies in the publicly available data. While some ROs asserted that a variance review is out of scope for Specification 11 3(b), several explanations for such variances emerged, including:

- Domains cited by Compliance had been identified by the RO's security threats monitoring in a different time period;
- Domains cited by Compliance were derived from data provided by an RBL deemed by the RO not to provide reliable and/or actionable information at this time;
- Domains cited by Compliance were derived from data provided by an RBL that the RO was not monitoring but, going forward the RO agreed to include the RBL in its monitoring efforts; and/or
- The RO may have investigated and taken action on a security threat not reflected in its STR.

Non-compliance. The audit revealed that approximately five percent (5%) of the audited ROs subject to Specification 11, Section 3(b) were not performing any security threat monitoring, despite having domains registered in their gTLDs.[4] In most of these cases, ROs cited a low number of registrations or tightly controlled and exclusively internal registration (e.g., where the gTLD has an ICANN-approved Specification 13 .brand designation). While the audit revealed that RBLs currently do not identify any threats originating from .brand gTLDs, Compliance explained to these ROs that monitoring is a contractual obligation that does not depend on the number or type of registrations. Remediation was required in all cases.

Good practices. Despite the instances of non-compliance and reporting variances described above, the audit did demonstrate that many ROs deployed good practices for identifying and addressing DNS security threats. In those cases, there was little to no variance between a RO's STRs and publicly available RBLs, STRs included almost all security threats that had been listed in publicly available security threat reports for the same time period, and ROs were able to

[4] Appendix – Statistical Data (located at the end of the report)

document actions taken on such domains; for example, ROs reached out to registrars managing these domains, requesting a review of the domains, while placing them in suspension.

Appendix – Statistical Data

The following table summarizes the statistical data obtained during the audit and illustrates the breakdown of the TLD population used for the statistics.

NOVEMBER 2018 REGISTRY AUDIT - STATISTICAL DATA		
TLDs in Scope for the Audit (Received RFI)		1,222
TLDs Terminated / In Process of Termination During Audit (termination unrelated to audit)		(14)
TLDs Postponed		(1)
TLD Population for Statistical Data		1,207
Technical Analysis Performance		
Technical Analysis (Security Threats) is performed		80%
Technical Analysis (Security Threats) is not performed (no domains)		15%
Technical Analysis (Security Threats) is not performed, domains registered, remediating		5%
Types of Threats & Frequency		
Analysis covers types of threats listed in Spec 11 3(b)*		94%
Technical Analysis (Security Threats) performance frequency*		
	Daily	80%
	Weekly	2%
	Monthly	8%
	Quarterly or Less Frequently	8%
	Reviewer Unable to Determine	2%
Technical Analysis Methodology & Report Retention		
Technical Analysis Methodology Described*		47%
Security Threats Reports Retained and Examples Provided*		94%
Additional RFI Questions		
% of ROs performing analysis and responsive to additional RFI questions		
	Described how threats are addressed*	44%
	Threats being reported to Registrars*	53%
	Examples of communications to Registrars provided*	10%
	STRs shared with external parties*	34%
	Any other actions taken to address security threats	30%
	Reports from LEA received	26%
	Examples of LEA reports provided	5%
	Examples of non-LEA reports provided	5%
	Monitoring blogs, articles, etc.	21%

Percentages with an (*) were calculated using the segment of TLDs (~80%) performing the Technical Analysis. All other percentages were calculated using the TLD Population for Statistical Data (1,207).