REGISTRYOFFICE

Fighting DNS Abuse at Scale

How RegistryOffice Abuse Monitor helps its clients to efficiently manage their abuse workflow, protect the reputation of their zone(s) and build a safer Internet.

14 January 2020

Executive Summary

Defining and fighting DNS abuse has been getting attention within the domain name industry in recent years, and was especially a major topic of conversation and debate in 2019. We believe this trend will continue during 2020 and beyond. Particularly because registry operators, registrars and hosters will continue to face increasing and new types of security threats, will grapple with how to coordinate identification, verification, and management of such threats, and face the possibility of new policies and regulations imposed by regulatory authorities and government.

Despite contractual specifications from ICANN and developed voluntary Frameworks for addressing abuse, both from ICANN and more recently from within the industry, there is in reality little guidance available on exactly how to deal with it, whether you are an individual "newbie" registry operator with few resources and little experience or an experienced larger operator with varied resources at your fingertips. It's up to the industry to figure it out.

Moreover, dealing with DNS abuse at scale only adds to resource time and costs, no matter if you are registry, registrar, reseller or a hoster.

This document will in part address how we help our clients limit time used for monitoring, checking and acting on reported DNS abuse. We will address our support of the recently published Framework to Address Abuse and our role as Trusted Notifier as defined in the framework.

We will discuss our general philosophy used as Trusted Notifier in developing our RegistryOffice Abuse Monitor utilized today by over 120 TLDs and now available to registrars and their resellers to improve their abuse workflow, reduce associated costs, protect their reputations and build a safer Internet.

Current ICANN Contractual Requirements, Voluntary Frameworks and Trusted Notifiers

Periodic technical analysis and reporting of whether registered domains in a TLD are being used to perpetrate security threats is contractually required of all new gTLD Registry Operators by the ICANN Registry Agreement Specification 11.3B.[1] In addition, the non-binding and voluntary ICANN Framework for handling abuse articulates how a Registry Operator **may** respond to identified security threats.[2]

The above is the result of multi-stakeholder cooperation prior to the introduction of the latest round of new gTLDs and contractual specifications are provided along with a voluntary framework. However they do not articulate exactly how to identify and deal with DNS abuse, and what is not. There is little guidance.

ICANN accredited registrars, by way of the 2013 Registrar Accreditation Agreement and its Section 3.18[3] specify the Registrar's Abuse Contact and Duty to Investigate Reports of Abuse. It is important to note that they are not contractually held to the same requirements as Registry Operators.

In October 2019, a separate Framework to Address Abuse was published by eleven original signatories and now has 48 signatory registrars and registries. RegistryOffice supports the Framework as it provides a common definition of certain types of DNS abuse and states that registries and registrars **must** act upon the defined categories. It also addresses important related matters such as:

- Website Content Abuse
- Disproportionality and Collateral Damage
- When Should a Registrar or Registry Act on Website Content Abuse?
- Proper Referral Procedures for Website Content Abuse
- What "Taking Action" Looks Like
- ICANN's Role

The Framework also talks about the "The Role of Trusted Notifiers":

> *"Registrars and registries may wish to consider using subject matter experts, often called "Trusted Notifiers," to monitor and help address some of the categories of Website Content Abuse identified above, or other sorts of abuse that may fall under an organization's policies. Trusted Notifiers are more than an abuse referral service. Befitting their designation, Trusted Notifiers earn the registries' and registrars' trust with a recognized subject matter expertise, an established reputation for accuracy, and a documented relationship with and defined process for notifying the registries and registrars of alleged abuse. While it is ultimately the responsibility of the registries and registrars to take action on verified forms of abuse, Trusted Notifiers can serve as a crucial resource to enhance the abuse monitoring and disruption procedures of registries and registrars."*

Through our Abuse Monitor service for registries and registrars, RegistryOffice acts as a Trusted Notifier and subject matter expert in providing a cost-effective and trusted SaaS platform to assist with DNS abuse notification, management and reporting.

[1] https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#specification11

[2] https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en

[3] https://www.icann.org/en/system/files/files/approved-with-specs-27jun13-en.pdf

Why RegistryOffice Abuse Monitor was developed

The team behind RegistryOffice Abuse Monitor operated .GLOBAL from May 2014 to August 2019. From day one, the Registry Operator monitored their namespace for DNS abuse in accordance with the RA Specification 11.3B.

Until March 2018 an external system was used for abuse monitoring. When the Registry Operator was informed that this service was to be terminated, an internal process was started to investigate alternatives.

With the objective to integrate an abuse monitoring system into the overall previously developed RegistryOffice Business Intelligence Dashboard platform, two major criteria were required:

1. Quality and quantity of abuse detected
2. How the reported abuse could be efficiently be processed

The investigation and research concluded that no external solution satisfied our criteria, thus it was decided to develop an in-house solution.

How we selected our Reputation Feeds

The initial product development phase included wide research of 200+ Reputation Block List feeds (RBLs). The objective was to find reliable feeds for the abuse categories defined in the RA Spec 11.3B. Not only the information provided by the RBLs was given attention, but also the feedback from registries and registrars. The RBLs were compared, assessed and quality checked for accuracy, false positives, and overlap.

When Abuse Monitor commenced operation, the following RBLs were configured:

- Google Safe Browsing: Pharming, Phishing, Malware, Botnets
- hpHosts: Pharming, Phishing, Malware, Spam
- Phishtank: Phishing
- URLhaus: Malware
- Openphish: Phishing
- SURBL: Pharming, Phishing, Malware, Botnets, Spam
- Spamhaus: Pharming, Phishing, Malware, Botnets, Spam

The RBLs used above are similar to the feeds used by the ICANN DAAR and covers the RA Spec 11.3B defined abuse categories in multiple ways (i.e. an abuse category will be identified in multiple RBLs).

In addition to the above, Abuse Monitor was designed to enable manual input of an abuse case (i.e. information given by other parties than the RBLs, such as submitted directly to a registry operator or registrar via their abuse contact email address published on their websites). The system proved to be extremely effective and it was decided to offer the Abuse Monitor to all registry operators, including ccTLDs, and most recently directly to registrars. .GLOBAL has since been sold and is no longer affiliated in any way with RegistryOffice AS.

How we limit time used for monitoring, checking and acting on reported DNS abuse

One of the objectives with the RegistryOffice Abuse Monitor is to limit the time to be used for monitoring, checking and acting on suspicious behaviour connected to DNS abuse. Seen from a Registry point of view, it is - in our opinion, of importance to reduce the number of notices to be sent to the sponsoring registrar, but still inform in a way that is seen as informational.

With this approach, we decided to organize the application logic for reported abuse for a domain name into “cases” where an “abuse case” can include several notices from RBLs. With this, the Abuse Monitor client receives less notifications but still gathers all information from the RBLs.

Grouping the abuse notices into cases also assists the abuse agent to weigh the importance of suspicious behaviour.

From the RegistryOffice Abuse Monitor dashboard, the agent can filter views of received, unactioned, open and closed DNS abuse cases in multiple ways (i.e. by abuse category, RBL feed, status, registrar, priority etc) and create/download reports for internal investigations. This in addition to predefined Google search settings for the domain name, information from Scamadvisor.com and MXtoolbox.com. The agent can easily check the abused label website from the dashboard ensuring that nothing “bad” is downloaded into the abuse agents computer.

Collecting information about the sponsoring registrar for the RBL noticed name, combined with registration data and the present EPP status, makes it possible for the agent to identify and act on suspicious patterns.

In addition, a feature to automatically close cases when a domain name is no longer being reported by the RBL, reduces the time to be used by the agent to monitor their TLD(s) namespace(s).

The RegistryOffice Abuse Monitor reporting can be viewed on a monthly basis along with specific reports for accredited registrars and a trend overview.

The system includes email templates to be used for communications with the Registry Operator’s accredited registrars and to registrants. These templates can be tailored based on the Registry Operator input and in all languages. Included in the templates is all information collected by the system for each DNS abuse case.

The Abuse Monitor API allows Registries and Registrars to be able to query Abuse Monitor for case information, status and be able to update this information through the API.

View our short 4½ minute video introduction of Abuse Monitor at https://registryoffice.blog/video/

Push the work to others?

In our January 2020 release of **Abuse Monitor for Registries**, the operator will have the option to push the abuse work to the Sponsoring Registrar for action and reporting. There will be support for separate login by the TLD's authorized registrars to view associated cases and take action, and an API that can be used externally of the system.

Also in our separate January 2020 release of **Abuse Monitor for Registrars**, the registrar will have the option to push the abuse work to their resellers for action and reporting. There will be support for separate login by the registrar's authorized resellers to view associated cases and take action. The registrar will also be able to utilize our API handles to query the number of current abuse cases for selected TLDs. This will enable registrars to maximize promotional revenue from selected TLDs by assessing their current zone abuse report metrics and trends before they execute a promotion. (i.e. Higher TLD abuse may mean higher backoffice abuse handling costs for the registrar.)

Continuous platform development and evaluation of RBL sources

RegistryOffice Abuse Monitor will be continuously developed both in functionality and reputation feeds.

The goal is to improve functionality based on client feedback and proposals. Our objective is that Abuse Monitor can be functional for all kinds of clients, from "brand TLDs" to high volume registry operators.

We are presently working towards being able to whitelist domains with selected RBLs.

In particular as it relates to functionality, and as mentioned just above, our January 2020 release of **Abuse Monitor for Registries**, the operator will have the option to push the abuse work to the Sponsoring Registrar for action and reporting. In addition, in our separate January 2020 release of **Abuse Monitor for Registrars**, the registrar will have the option to push the abuse work to their resellers for action and reporting.

The present RBLs will always be evaluated. New DNS abuse RBLs will be added to RegistryOffice Abuse Monitor if the list will add value and is commercial doable.

Per today, RegistryOffice Abuse Monitor is tailored for handling DNS abuse. Other sources for monitoring suspicious behaviour and forms of Website Content Abuse (i.e. child sexual abuse materials, illegal distribution of opiods online, human trafficking, specific and credible incitements to violence, fake webshops, fake news, etc.) other than "DNS Abuse" will be added if requested by authorities (example ICANN) or clients.

Conclusion

From 2020 and beyond, we believe that registry operators, registrars and hosters will continue to face increasing and new types of security threats. It is important that all entities establish a way to monitor their namespace for security threats. RegistryOffice Abuse Monitor is an excellent tool for keeping the namespace controlled.

Despite contractual specifications from ICANN and developed voluntary Frameworks for addressing abuse, both from ICANN and more recently from within the industry, there is in reality little guidance available on exactly how to deal with it.

It is important for all concerned to work together in order to coordinate identification, verification, and management of such threats and reduce false positive reporting. This is not only to negate the possibility of new policies and regulations being imposed by regulatory authorities and government, but also to protect the general public, partners, and the reputations of registries, registrars and the industry as a whole.

Let's work together to build a safer Internet.

For more information:

View our short video introduction of Abuse Monitor at https://registryoffice.blog/video/

Arrange a free trial or full demonstration by contacting us at sales@registryoffice.global

www.registryoffice.global