ICANN | RrSG
Registrar Stakeholder Group

Appeal Mechanisms following DNS Abuse Mitigation

Introduction

As registrars continue to actively contribute to community efforts against DNS Abuse, there is an increased need for registrant appeal mechanisms. While registrars should only take action for DNS Abuse complaints that are sufficiently documented, there may be scenarios where a registrant may desire to appeal the suspension of domain name registration services, including complaints based upon false or incomplete information or where the registrant has resolved the issue. These appeal mechanisms are not intended to shelter abuse, instead as there is increased vigilance and enforcement, they are intended to provide processes to ensure registrant's rights are protected in light of increasing scrutiny (which increases the risk to registrants).

In this document, "DNS Abuse" means malware, botnets, phishing, pharming, and spam when it is used as a vector for the other forms of DNS Abuse. This is in accord with other RrSG and CPH documents, including the CPH Definition of DNS Abuse and the Framework on DNS Abuse.

Types of Appeals Mechanisms

There are several appeals mechanisms that registrars can provide to registrants through their internal processes as well as through external mechanisms. These appeals mechanisms should be integral to all DNS Abuse processes for registrars and be available to all registrants. Although all DNS Abuse complaints may be subject to these appeals mechanisms, the availability of such processes does not guarantee that appeals will be successful nor binding on the registrar.

Evidentiary

The first appeals mechanism involves the DNS Abuse complaint itself and may be considered a pre-emptive appeal's mechanism: all DNS Abuse complaints should be based on material, actionable reports that include verifiable evidence. Domains should not be labelled as abusive where there is no evidence, nor should registrars act where there is no evidence. This requirement ensures that registrants are not subject to spurious complaints that could jeopardize non-abusive conduct.

It is of the utmost importance to distinguish between domain names registered for a purely abusive purpose (spamming, phishing…) and those registered and used legitimately by the registrant but compromised by a third party. When registrars have evidence of the former case (domain portfolio composed only of abusive domain names, inaccurate contact details…) there is no need for any appeal mechanism.

However, in cases where the DNS abuse is the result of a third-party action, the registrar's suspension may be overturned.

Internal, Support-Based Appeals

The next appeals mechanism is to integrate an internal appeals mechanism within the registrar's customer support flow. When possible, a registrant should be informed about the reported abuse, the nature of the abuse, and additional information that can allow the registrant to review the veracity of the complaint. If the registrant disagrees with the abuse determination, the registrant should have the opportunity to rebut the allegation and, if substantiated, the registrar must have the discretion to reverse the abuse determination. In certain situations, such as when a security vulnerability is exploited by a malicious third party, a registrant can address the vulnerability (such as through deploying a software patch) to remove the abuse, which may be sufficient for the registrar[1] to reverse any action taken in response to the reported abuse.

Ombud

Because the customer service team is often involved in the initial DNS Abuse determination and action, some registrars may provide an independent internal appeals process (such as an ombud). This will result in a review by a third party that was not involved in the original abuse process, consideration of the abuse allegation, and any rebuttal evidence provided by the registrant. The benefit of internal independent review is that any determinations can be binding on the registrar.

Courts of Competent Jurisdiction

In addition to these appeal mechanisms, there are external processes available to registrants. These processes vary based upon the jurisdiction of the registrar, as does the ability of external appeals mechanisms to be binding on the registrar. Depending on the type of alleged abuse and action taken in response, registrants may be able to utilize local laws and authorities to object to the action. This may include public ombuds, consumer agencies, or law enforcement. None of these processes preclude the ability of registrants to utilize civil litigation to address abuse issues; however, these may be costly and time-consuming.

What Can You Do?

If you believe that your domain has been suspended for DNS Abuse and you disagree with that action, you should contact your registrar immediately to discuss what options may be available to you.

[1] In some cases, a Registry has taken action. The registrar in these cases, should facilitate the registrant's appeal to the Registry, which should follow the same recommendations.