28. Abuse Prevention and Mitigation - Supplement

Infibeam will staff a Single Point of Contact (SPoC) Abuse team to address abuse and malicious use requests. The role of the abuse team is to monitor registry services and review complaints lodged online by end users, customers, or from Law Enforcement. The complaints are managed in accordance with the Acceptable Use Policies (AUP) and Terms of Service (TOS) which allows the Abuse Team discretion to suspend a domain instantly or send the complaint thru the appropriate escalation channel for complaint resolution.

Complaints are received via email abuse@registry.ooo as noted on the .ooo website (http://registry.ooo). Access to Infibeam's Abuse Team for Registrars will be provided with a hotline number, email address, and personnel for filing direct requests. Complaints may be submitted 24x7 and each request path requires the submitter to provide personal contact information. Infibeam will acknowledge the complaint within one business day and will provide the requestor acceptance and/or resolution within three business days depending on severity and complexity of the complaint.

Infibeam views domain name abuse as a serious matter that produces direct harm to internet users and .ooo customers. As such, Infibeam will handle each abuse complaint as a direct threat and intends to resolve each validated complaint with a sense of urgency. .ooo Abuse Policies recognize many forms of abuse related to the registrations and use of domain names. Abuses and their respective mitigation strategy listed here is not an exhaustive list, but is meant to highlight general process and procedure by which .ooo will manage the most common forms of abuse. The Infibeam Abuse Team collaborates and participates with industry experts and forums to understand the latest forms of abuse in an attempt to protect customers of our services where possible.

28.1 DRAFT Abuse Remedy Process

1. Customer or end user submits abuse complaint to abuse@registry.ooo
2. Abuse Coordinator receives request and acknowledges receipt of complaint
3. Abuse Coordinator analyzes request to determine the abuse type to be addressed and references the .ooo knowledgebase for detailed procedures
4. Abuse Coordinator assigns a Severity rating based on complaint type
5. Abuse Coordinator resolves the complaint based on the following decision tree:
    a. Is the request a court ordered seizure and transfer?
        i. Yes – See section 28.1.1
        ii. Else, next step
    b. Does the request reflect a potential DDOS Attack?
        i. Yes – See section 28.1.2
        ii. Else, next step
    c. Is the request a phishing complaint?
        i. Yes – See section 28.1.3

ii. Else, next step

d. Is the complaint a notice of a trademark infringement?
    i. Yes – See section 28.1.4
    ii. Else, next step
e. Is the request a possible hijacking case or a transfer dispute?
    i. Yes – See section 28.1.5
    ii. Else, next step
f. Is the request an email service abuse?
    i. Yes – See section 28.1.6
    ii. Else, next step
g. For all other abuses not defined:
    i. Escalate request to Abuse Manager for guidance and resolution

28.1.1 Court Ordered Seizure and Transfer

Definition: Law enforcement via a court of legal jurisdiction orders that domain be seized due to illegal activity of applicable law

Service Level: 1 business day

Procedure:

- Abuse Coordinator contacts the legal jurisdiction to request signed copies of the court order
- Upon receipt of court order, Abuse Coordinator confirms request with the Abuse Situation Manager
- If the request is determined to be valid, Abuse Coordinator will submit a request to the Registry Support team to have the domain pushed to the requested registrar as directed by the governing body
- If the request is determined to be invalid or documents submitted are in question, the Abuse Coordinator will contact the legal jurisdiction requesting the appropriate documentation or reasons as to why the request cannot be fulfilled.

28.1.2 DDOS Attack

Definition: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users.

Service Level: 1 business day

Procedure:

- Abuse Coordinator will confirm the DDOS attack with the Abuse Manager
- If the complaint is confirmed as a DDOS attack:

    - Abuse Coordinator will escalate the request to the respective Registrar Support Team
    - Else, Abuse Coordinator will respond to the complainant as unable to confirm and request additional information or close the complaint
- Registrar Support team will suspend the domain registration until further notice

28.1.3 Phishing

Definition: Phishing is a Web site fraudulently presenting itself as a trusted site (often a bank) in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords).

Service Level: 1 business day

Procedure:

- Abuse Coordinator will confirm the Phishing scam with the Abuse Manager
- If the complaint is confirmed as a legitimate phishing event
    - Abuse Coordinator will escalate the request to the Registry Support Team
    - Else, Abuse Coordinator will respond to the complainant as unable to confirm and request additional information or close the complaint
- Registry Support Team will immediately suspend the domain.
- Abuse Manager will investigate the Phish event and deemed the intent of the Domain owner, the Registry Support team seize and/or delete the domain from the zone.

28.1.4 Cybersquatting / Trademark Infringement

Definition: Cybersquatting is currently defined in the gTLDs as the deliberate and bad-faith registration and use of a name that is a registered brand or mark of an unrelated entity, often for the purpose of profiting (typically, though not exclusively, through pay-per-click advertisements).

Service Level: 3 business days

Procedure:

- If request appears to be an initial complaint on a possible infringement, Abuse Coordinator will direct complainant to the UDRP/WIPO process
- Else, if the request of transfer is from a .ooo registrar, Abuse Coordinator will work with the Registrar to ensure the domain in question is transferred appropriately.

28.1.5 Transfer Disputes / Hijacking

Definition: Domain hijacking or domain theft is the act of changing the registration of a domain name without the permission of its original registrant.

Service Level: 3 business days

Procedure:

- Abuse Coordinator will confirm the request with the Abuse Manager
- Abuse Coordinator will escalate request to and Registrar to investigate the transfer

28.1.6 Email Service Abuse

Definition: An illegitimate use of email systems to distribute abusive content or in a manner that violates the Acceptable Use Policy. Examples of this abuse are Un-Solicited Commercial Email (UCE/SPAM)

Service Level: 3 business days

Procedure:

- Abuse Coordinator will validate the complaint for UCE/SPAM elements and collaborate with Complainant to acquire the examples of the offensive material.
- If Abuse Coordinator deems the offensive material to violate Acceptable Use Policy and is deemed to be offensive material, Abuse Coordinator will escalate the request to the Registry Support team for suspension
- Registry Support team will immediately suspend the domain
- If a .ooo Customer is found to be unknowingly sending UCE, Customer shall be allotted the opportunity to correct the situation and assurances must be received by offender to ensure against future occurrences

- If one or more of the above is confirmed and validated, the Abuse Coordinator or Technical Services will notify the Customer that they are in violation of our Terms of Service
- An email will be sent immediately to the Registrant, Admin and Technical contact on file to advise of the violation. The email should instruct the Customer to take the appropriate action within 24 hours to remove the offending content or they may be subjected to a suspension of services.
- During Business Hours, the Abuse Coordinator will contact the Customer via phone in addition to sending the email to inform the Registrant, Admin or Technical contacts of the offending violation. The Technical Services agents will follow the same process for After Hours handling.
- If no response is received within 24 hours, a second phone and email attempt will be made to reach the Registrant, Admin and Technical contact.
- If the offending party does not respond by the end of the second business day, action will be taken to remove the offending content that is causing server degradation
- Technical Support team will suspend the Hosting services
- The Registry Support team will place the domain on Registrar hold to de-resolve the name

- If the offending party responds and agrees to remove the offending content within the 24 hour time frame, the Abuse Coordinator or Technical Services agent must confirm the material has been removed, and note the appropriate remediation within the CRM system
- If the offending party responds and agrees to remove the offending content after the service suspension, the Registry Support team may remove the suspension and allow customer to remove the content. Support will confirm the offending material has been removed, and note the appropriate CRM systems.
- If the offending party requests that .ooo remove the offending material, the Abuse Coordinator agent must call the Customer and obtain confirmation to remove the content on behalf of the Customer. The Abuse Coordinator will also obtain written confirmation from the Customer via the Registrant, Administrative or Technical Contacts that are listed. The confirmation should be noted in the appropriate CRM system.
- If there is no response from the offending party after 7 Days, the Abuse Coordinator will submit a request to delete the offending content from the servers to the Abuse Manager for approval to delete the content.
- Prior to deleting the content, an email will be sent to the appropriate Legal point of contact to advise of the issue and obtain approval to delete the content.