SSAC
ICANN Security and Stability
Advisory Committee

25 February 2009

SAC 038: Registrar Abuse Point of Contact

Introduction and Background

ICANN's current gTLD agreements require registries and registrars to operate a Whois service. Clause 3.3.1[1] of the Registrar Accreditation Agreement identifies the contact information that registrars and their agents (resellers) must collect from applicants when they register a domain name. Registration contact information commonly serves as the initial means of communicating with a domain registrant or an operator (administrator) of an Internet host (server) that is assigned a label in that domain. Parties identified as contacts for a domain name may be contacted for a variety of reasons including general (e.g., business) inquiries, attempts to notify the registrant of an erroneous DNS configuration and inquiries regarding the possible involvement of the domain name in a malicious, illegal or criminal activity.

Law enforcement, Computer Emergency Response Teams (CERTs), the anticrime and antiphishing community (interveners), businesses that provide online reputation protection services, network operators, and Internet users may attempt to contact ICANN accredited registrars when they are unable to communicate with a domain registrant using contact information obtained using Whois services. In the case of generic TLDs, the Whois record should always identify the ICANN accredited registrar's name (the sponsoring registrar). Thus, users should always be able to obtain the name of the registrar that sponsors a domain name by requesting domain name registration information via a Whois service. The user must then seek out contact information for that registrar's abuse handling staff from one of several possible sources.

Multiple lists and sources for contacting registrars exist, but not all the parties reached through these sources of contact information are able to process an abuse claim or deal with a criminal complaint. In cases where an explicit abuse contact is provided at the registrar's web site, the intervener often accesses a suitable registrar agent. In cases where abuse contact information is not prominently or easily located at a registrar's web site, however, attempts to resolve a dispute or investigate an abuse claim may be delayed while the user tries to locate appropriate contact information.

Users may also access ICANN's public list of registrar contact information. Registrars must provide ICANN with primary contact information for contractual notices. Registrars are not contractually obliged to maintain public contact information, nor are they obliged to maintain a separate contact for abuse. Currently, ICANN allows registrars to provide a

[1] See http://www.icann.org/en/registrars/ra-agreement-17may01.htm#3.3.1.

public alternative to their primary (contractual) contact information and ICANN publishes this alternative[2]. If registrars choose not to provide ICANN with separate public information, ICANN publishes the primary contact information. The point of contact identified on ICANN's list again may not be the appropriate party to pursue an abuse claim or criminal complaint.

Issues

The current requirements for publicly accessible contact information may not meet the community's needs for the following reasons:

- Information for several kinds of points of contact is published for registrars. Not all of these are the appropriate points of contact for dealing with abuse claims or criminal complaints. Sorting out the appropriate point of contact may delay an investigation.

- Users that make inquiries or investigate abuse and illegal activities potentially involving a domain name must rely on registrars to voluntarily publish contact information that in a readily accessible manner. Anecdotal information conveyed to SSAC indicates that:

  a) Not all registrars voluntarily publish public contact information on their web sites,
  b) Not all of the published contact information is accurate or complete,
  c) Personnel who are reached via certain published contact information may be unable to handle abuse inquiries or may be unfamiliar with escalation procedures that would put an investigator in touch with a suitable (e.g., technical) contact, and
  d) Not all registrars publish a separate abuse contact.

- A public contact may only be available during specific business hours, whereas an abuse contact should be available 24 x 7. Inquiries involving alleged abuse or criminal activities typically require timely if not urgent response. For example, inquiries that will lead to the suspension of a domain name used in a phishing attack, in support of an illegal activity (hosting of child pornography or illegal sales of prescription pharmaceuticals) are ideally processed within hours. In the case of a "double flux" attack[3], minutes of delay provide an attacker with sufficient time to divert his attack vector to other domain names he has registered or domains over which he has obtained unauthorized control.

[2] See http://www.internic.net/regist.html.

[3] See SAC 025, Fast Flux Hosting and DNS, http://www.icann.org/committees/security/sac025.pdf

Recommendations

SSAC recommends that registrars and resellers assist in the investigation and mitigation of abuses and illegal activities in cases where attackers exploit domain name resolution and registration services. We recommend that the GNSO consider the following and act accordingly:

1. Each registrar should provide an abuse contact.

    - The abuse point of contact should be responsive and effective. The abuse contact must answer the phone and email quickly, people handling abuses must be empowered to take effective action, and they must have well defined criteria for their actions. The GNSO should consider the criteria for availability and access to the abuse contact (e.g., 24x7 or normal business hours), and the mean time to respond to a complaint. ICANN and registrars should consider how compliance would be evaluated for these metrics.

    - Registars should provide complainants with a well-defined, auditable way to track abuse complaints (e.g. a ticketing or similar tracking system). The GNSO should study how registrar performance can be measure and evaluated for compliance.

2. Registrars should publish abuse contact information.

    - The registrar identified in the sponsoring registrar field of a Whois entry should have an abuse contact listed prominently on its web page. To assist the community in locating this page, SSAC recommends that registrars consider a uniform naming convention to facilitate (automated and rapid) discovery of this page, i.e., http://www.<registar>.<TLD>/abuse.html.

    - Registrars should provide ICANN with their abuse contact information and ICANN should publish this information at http://www.internic.net/regist.html.

3. The information a registrar publishes for the abuse point of contact should be consistent with contact details currently proposed as an amendment to Section 3.16 of the RAA. Each contact method (telephone, email, postal address) should reach an individual or organization able to attend to an abuse claim; for example, no contact should intentionally reject postal or email submissions.

    - The GNSO should identify what constitutes appropriate abuse contact information, how and where the information is published. SSAC calls attention to RFC 2142, Mailbox Names for Common Services, Roles, and Functions and suggests that registrars make use of the naming conventions therein.
    - Abuse point of contact information should be made available in a uniform, machine-readable format. The GNSO should decide whether one or all of these publishing options are appropriate.

4. ICANN and registrars should work cooperatively with the community to determine appropriate measures to safeguard against false complaints. The details of what constitutes abuse and what protections must be provided against false complaints must be worked out with the registrar community and the user community. Equally, the criteria for how quickly complaints have to be answered need to be worked out with the registrar and user communities. The GNSO should undertake this activity as part of a comprehensive study of registration abuse.

5. ICANN should periodically (no less frequently than annually) verify that these contacts are accurate.

SSAC believes that the community is best served when registrars and resellers make contact information readily accessible and that accessibility via a single list or searchable database offers the community the most expedient means to obtain contact information. A single repository, maintained by ICANN, provides ICANN with a straightforward means to verify that the contact information remains accurate and complete and provides the community with a visible demonstration that ICANN and its accredited registrars are committed to providing open, effective means of communication for general as well as abuse inquiries.

This recommendation focuses on gTLDs and ICANN-accredited registrars. SSAC notes that while each ccTLD may have its own frameworks, contracts and arrangements with registrars, treating abuse uniformly and making abuse contact information accessible across all TLDs is desirable. SSAC invites the ccTLDs to share their experience in handling abuse claims and to work in cooperation with ICANN to publish abuse contact information and do so consistently. SSAC is prepared to collaborate with the GNSO and ccNSO to study these issues further.