SAC115
SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS

Rod Rasmussen, Chair, Security and Stability Advisory Committee (SSAC)

20 May 2021
Agenda

- Scope and purpose of report
- Defining the problem
- Framework for interoperable approach
- Findings
- Recommendation
Scope and purpose of report
Purpose of report

**Goal:** Reduce victimization of Internet users

**Strategy:** Interoperable approach based on universal standards for DNS abuse handling

**Desired Outcome:** SAC115 acts as a catalyst to channel ongoing efforts in order to begin establishing universal standards
Defining the problem
Defining the problem

DNS abuse in SAC115 refers to the use of domain names or the DNS to perpetuate abusive activities. The report does not define “DNS Abuse” but points to definitions commonly used in the ICANN Community.

ICANN Community Recognized DNS Abuses

- Malware
- Botnets
- Phishing
- Pharming
- Spam*

- Many other forms of DNS abuse exist, are reported, and are acted upon by service providers
- New types of abuse are commonly created, and their frequency waxes and wanes over time
- No individual list of abuse types will ever be comprehensive
- The SSAC supports the concept of regular, community-driven review of DNS abuse definitions
## Defining the problem

### What are we doing about DNS abuse?

<table>
<thead>
<tr>
<th>Blocking and filtering</th>
<th>Notification and take down</th>
<th>Leading efforts</th>
<th>Notifier Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Quick to implement</td>
<td>• May take a long time</td>
<td>• APWG</td>
<td>• Expedite DNS abuse remediation</td>
</tr>
<tr>
<td>• Difficult to maintain at scale</td>
<td>• Inconsistent outcomes</td>
<td>• M3AAWG</td>
<td>• Explicit network of trust</td>
</tr>
<tr>
<td>• High number of false positives</td>
<td>• Possibility of collateral damage</td>
<td>• FIRST</td>
<td>• Scaling is difficult by its nature</td>
</tr>
<tr>
<td>• Blacklists go stale</td>
<td></td>
<td>• Internet &amp; Jurisdiction Policy Network</td>
<td>• Each program sets its own definitions and standards</td>
</tr>
<tr>
<td>• Possibility of collateral damage</td>
<td></td>
<td>• Cybersecurity Tech Accord</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PIR DNS Abuse Institute</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Digital Trust and Safety Partnership</td>
<td></td>
</tr>
</tbody>
</table>

### Findings

- Leading efforts:
  - APWG
  - M3AAWG
  - FIRST
  - Internet & Jurisdiction Policy Network
  - Cybersecurity Tech Accord
  - PIR DNS Abuse Institute
  - Digital Trust and Safety Partnership

- Notifier Programs:
  - Expedite DNS abuse remediation
  - Explicit network of trust
  - Scaling is difficult by its nature
  - Each program sets its own definitions and standards
Framework for interoperable approach
Proposed Framework

- Primary Point of Responsibility for Abuse Resolution
- Escalation Paths
- Evidentiary Terminology and Standards
- Reasonable Time Frames for Action
- Availability and Quality of Contact Information
# Primary Point of Responsibility for Abuse Resolution

**Principle:** Each incident of DNS abuse should have a reporting entry point in the DNS ecosystem where that abuse is resolved by policy and process.

<table>
<thead>
<tr>
<th>Manifestation of Abuse</th>
<th>Primary Party</th>
<th>Secondary &amp; Escalation Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name registered to perpetuate abuse</td>
<td>Registrar for domain</td>
<td>Registry for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web host for web content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email provider for spam accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISP for abusive activity</td>
</tr>
<tr>
<td>Domain name registered to perpetuate abuse (Registry operator policy exists to receive abuse complaints)</td>
<td>Registrar and Registry operator</td>
<td>Web host for web content</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email provider for spam accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISP for abusive activity</td>
</tr>
<tr>
<td>Website compromised for abuse</td>
<td>Owner of domain name Hosting provider</td>
<td>Registrar of domain (for contacts)</td>
</tr>
<tr>
<td>Account on major Internet platform</td>
<td>Platform service provider</td>
<td></td>
</tr>
</tbody>
</table>
Escalation Paths

**Principle:** When a reporter either reports to the wrong party or does not get a response, there needs to be a documented and actionable escalation path to assist in mitigating the abuse.

- Evidence of both the abuse and the time of report can be conveyed to the next party in the escalation path
- Standardized paths will allow for eventual automation
- SAC115 does not include proposed escalation paths beyond Appendix B
- Escalation paths and standardized documentation should be determined by stakeholders
Principle: Reporters of abuse have the responsibility of providing evidence and documentation. Setting objective standards of evidence to support action will enhance transparency and accountability for service providers.

Temporal Relevance
- When did it happen?
- How long after the registration did the abuse occur?
- How long after the abuse was detected did the evidence get logged or captured?

Visual
- Was there an “A” or “AAAA” DNS record logged for the domain?
- Was there content hosted on the domain that was not a parked page record and that was captured via screenshot or other means?

Behavioral
- Are there logs of activities regarding the domain name itself?

Demonstrative
- What is the abuse for which the domain was used?
- How did it violate ToS that supports rapid action?
- What is the impact of abuse?
- What are the anti-abuse policies of the responsible party?
Reasonable Time Frames for Action

**Principle:** The timely mitigation of DNS abuse is extremely important to minimize victimization of the abuse.

- **Escalations:** maximum time for escalation and remediation should be no longer than 96 hours
- **Expedited escalations:** escalation and remediation of urgent requests should be commensurate with the potential harm threatened

**Scope**
- Registry: 24 hours
- Registrar: 24 hours
- Registrar reseller: 24 hours
- Hosting provider: 24 hours
Availability and Quality of Contact Information

**Principle:** Accurate, thorough, and accessible contact information for entities in the DNS ecosystem is critical to establishing escalation paths and mitigating abuse.

- Readily accessible contact information becomes increasingly difficult to find the further downstream from the registry.
- Uncertainty incentivizes reporting parties to use a ‘scattergun approach’.
- Possible solution is to create a single point of contact determination where a reporter can identify the type of abuse and get directed to appropriate parties.
Findings
Findings

Lack of coordination leads to inconsistent approaches to DNS abuse management

Opportunity for a Common Abuse Response Facilitator
Recommendation 1: The SSAC recommends that the ICANN community continue to work together with the extended DNS infrastructure community in an effort to

(1) examine and refine the proposal for a Common Abuse Response Facilitator to be created to streamline abuse reporting and minimize abuse victimization; and

(2) define the role and scope of work for the Common Abuse Response Facilitator, using SAC115 as an input.
Discussion