New gTLD Program & Mitigating Malicious Conduct

Patrick Jones & Margie Milam

ICANN Seoul Meeting

October 2009

General Process to Address the Issue

Identify issues through experts

↓

Comment forum and consultations

↓

Summarize comment and solutions

↓

Develop draft positions and explanatory memoranda

↓

Post proposals in draft Guidebook

↓

Iterate through public comment

Input Sources

- Comments on Applicant Guidebook v1 & v2
- Comments via Overarching Issues Wiki
- Relevant SSAC reports and recommendations
- Public Consultations at Sydney, New York and London
- Consultation with expert participants
  - Anti-Phishing Working Group (APWG)
  - Registry Internet Safety Group (RISG)
  - Computer Incident Response Community (FIRST/CERTs)
  - Banking / Finance Assns (BITS , ABA, FS-ISAC, FSTCC)

Key Issues identified

A. How do we ensure that bad actors do not run Registries?

B. How do we ensure integrity and utility of registry information?

C. How do we ensure more focused efforts on combating identified abuse?

D. How do we provide enhanced control framework for TLDs with intrinsic potential for abuse?

Mitigation Steps – Vetted Registry Operators

- Deny applications based on following criteria for key personnel associated with proposed registry
  - History of financial misconduct or fraud
  - History of prior bad behavior related to cybersquatting and violations of ICANN contractual requirements
    - Disclosure of previous involvement in UDRP process
  - Explore approaches to establish criteria based on prior criminal conduct

Ensure malicious conduct not enabled at registry level

Mitigation Steps – Registry Data Integrity

- Require DNSSEC deployment
  - Implementation plan as part of application
  - DNSSec-enabled from start of operations
- Prohibition on Wild Carding
  - For all DNS zone files maintained by registry operator
- Require plan for removal of Orphan Glue Records

Reduce opportunities for malicious actors to mislead users

Mitigation Steps – Enabling Response

- Requirement for “thick WHOIS” data
- Requirement to allow for centralization of zone-file access
- Require Registry level abuse contacts and documented abuse policies
- Availability of Expedited Registry Security Request process

Enable access to information and ensure documented processes for responses

High Security Zones Designation Program
Agenda

- “Drivers” behind Program
- Program Overview
- 3 Key Principles
- Program Elements
- Next Steps
- Questions

High Security Zones Designation Program

Drivers

- Establish unified approach to variety of public comments received on new gTLD security and compliance issues
- Provide mechanism for interested parties to provide input to define and enhance controls necessary to combat malicious abuse
- Enhance user trust in “designated” TLDs
- Provide ICANN new gTLD Program Manager with a “tool” to address fraud and malicious abuse

High Security Zones Designation Program
Overview

- Establish a common set of standards for gTLD security and operational controls
  - Designed for gTLDs with intrinsic potential for malicious abuse
  - Voluntary participation by gTLD registry and registrars
  - Allows registry to require specific security measures by registrars
  - Separate from gTLD application and scoring process
  - Focused on gTLD registry operator
- Require registry and its registrars to demonstrate an effective security program that complies with defined standards of security and operational controls

High Security Zones Designation Program
Principles

- Registry establishes and maintains effective internal controls to ensure **core IT functions** are authorized, accurate and performed in a timely manner in accordance with Program
- Registry establishes and maintains effective internal controls to ensure **core business functions** are authorized, accurate and performed in a timely manner in accordance with Program
- Registry maintains effective controls to establish and authenticate the **identity of participating registrars and registrants** in accordance with Program

High Security Zones Designation Program
Elements

- Objectives and Sample Criteria
- Assessment Methods
- Preparation, Training and Remediation
- Governance
- Administrative Practices

High Security Zones Designation Program
Next Steps

- Publish concept paper for public review and comment
- Development, modification and improvement of program to occur in parallel with new gTLD program
- Form ICANN Working Group to establish:
  - Guidance on objectives and required control criteria
  - Guidance on the designation processes and timelines
- Report on progress through ICANN global meetings

Recent Publications

- Draft Applicant Guidebook, version 3 + other documents:
  - Update on Cost Considerations
  - Malicious Conduct
  - Voluntary Security Designation program
  - Summary changes Registry draft agreement
  - Root scaling study
  - Draft Global Communications Plan
- Summary analysis on public comments
  - IRT Final report
  - Consultations - Sydney, NYC & London
  - Excerpts Comments
  - Root scaling TOR
- Two Trademark Protection mechanisms proposals
  - URS
  - TM Clearing House

What's next?

- Staff continues to balance the desire to move ahead with the launch plans while addressing the Community raised concerns
- Actively working with experts and seeking community input on Overarching Issues through participation in Global consultation events + dedicated Wiki
- Operational readiness – retain evaluation panels

New gTLD Seoul Sessions

- Sunday 09:30 – 10:30 “Introduction to new gTLDs”
- Monday 10:30 – 12:00 “Program update and sessions for the week”
- Monday 15:00 – 17:00 “Registry/Registrar Separation”
- Monday 17:00 – 19:00 “Mitigating Malicious conduct”
- Wednesday 12:30 – 14:00 “Trademark protection”
- Wednesday 12:30 – 14:00 “Root scaling study results”

Upcoming events

- Latin America
  - Sao Paulo – Nov 24
  - Buenos Aires – Nov 27
- Africa and webinars under development

Thank you!