New Generic Top-Level Domains: Malicious Conduct

New York/London City

July 2009

Overview

- Potential for Addressing Malicious Conduct
  - Relationship to Trademark Protection
- Inputs on this Issue
- Overview of Key Inputs So Far

Placing “malicious conduct” in the overarching issues construct

- Our efforts focused on malicious conduct as criminal activity
  - Eg. Phishing to conduct financial fraud/identity theft, spread of malware/establishing botnets
- Distinct from trademark protection
  - Different processes for determination of what at issue and to authorize response
  - Certain remediation steps may address both issues – strengthen mechanisms for ensuring registrars and registrants can be contacted

3

Inputs on Malicious Conduct

- Comment on Applicant Guidebook v1 & v2
- Comment via Overarching Issues Wiki
- Relevant SSAC reports and recommendations (SAC 38 – Registrar Abuse Contact; forthcoming SSAC 41 – DNS Redirection and synthesized DNS responses)
- Outreach to Involved Groups
  - Anti-Phishing Working Group
  - Registry Internet Security Group
  - FIRST/CERT community
  - Banking/Finance Associations (BITS/FSR, ABA, FS-ISAC, FSTCC)
- Public Consultation at Sydney and through July/August

4

APWG Draft Input

- New threats
- Issues of Scale
- Long-Standing Issue**s**

Final report expected; focus on remediation measures

5

Comment on APG v2 & Analysis

- Key Themes of Comment
  - Need to leverage outside expertise
  - Develop standardized remediation approaches
- Potential changes for implementation

6

Addressing Key Issues

- Addressing control of security-implicated new gTLDs
  - Understand appropriate standards for registrar/registrants in these TLDs & registry-level security/continuity practice
- Ensuring effective practices in all new gTLD operation
  - Implement DNSSec; prohibit wildcarding; remove glue records
- Ensuring ability to react to malicious conduct
  - WHOIS requirements and enhanced compliance
  - Registrar-level requirements such as abuse point of contact
  - Include approach as part of application/evaluation

Way Forward

- Continue consultations here and in NY, London, Hong Kong, Dubai
  - Discuss possible mitigation approaches
- Work with Banking/Finance on security-specific TLD concerns and mitigation approaches
- Develop appropriate mitigation processes and explanatory memoranda for AGB3

8