Update from ICANN staff on SSR Activities

Greg Rattray

Tuesday 21st 2010

Malicious Conduct & New gTLD Program

As ICANN initiated work with the community on the new gTLD program, the community raised concerns regarding the potential for increased malicious conduct within the new gTLD space.

- ICANN initiated malicious conduct study in March 2009 as one of four overarching issues
- Malicious conduct study included participation from various sources:
  - Anti Phishing community and APWG members
  - Registry Internet Safety Group (RISG)
  - Security and Stability Advisory Committee (SSAC)
  - Computer Emergency Response Teams (CERT)
  - Banking and finance industries
  - Internet security experts
- ICANN concluded and published initial study in October 2009; posted with DAG 3 materials

Malicious Conduct Results

- **Study provided nine recommendations related to new gTLD program**
  - Vet registry operators – in DAG
  - Demonstrate plan for DNSSEC deployment – in DAG
  - Prohibit wildcarding – Board resolution; in DAG
  - Remove orphan glue records – in DAG
  - Require thick WHOIS – in DAG
  - Document registry level abuse contacts and procedures – in DAG
  - Expedited registry security request process – in place
  - Centralize zone-file access – advisory group formed; recommendations provided – seeking community comment; potential implementation
  - Create a framework for high security zone verification – advisory group underway; technical framework developed;awaiting recommendation
    - Not new gTLD specific

Recommendation - Document Registry Level Abuse Contacts and Procedures

Recommendation overview

- Establish a single point of contact for TLD abuse complaints
- Registries provide a description of their policies designed to combat abuse.
- Fundamental step in allowing successful efforts to combat malicious conduct

Current status

- Requirement for all new gTLDs per the latest Registry Agreement

Recommendation - Centralize Zone-File Access

Recommendation overview

- Make registry zone file data available through centralized source
- Allows for more accurate and rapid identification of key points of contact
- Reduces the time necessary to take corrective action

Current status

- Zone File Access Advisory Group ("ZFA AG") created
  - Created proposal for mechanism to support centralization of access to zone files
  - ZFA AG completed work on strategy proposal on 12 May 2010

  http://www.icann.org/en/topics/new-gtlds/zfa-strategy-paper-12may10-en.pdf
- ICANN staff currently planning implementation for recommendations

Recommendation – Draft Framework for High Security Zone Verification

Recommendation overview

- Create a voluntary program designed to designate TLDs wishing to establish and prove an enhanced level of security and trust
  - Provides a certification mechanism for TLDs that desire to distinguish themselves as secure and trusted
  - May benefit certain TLD business models

Current status

- ICANN formed High Security Zone Top Level Domain Advisory Group (“HSTLD AG)
  - HSTLD AG to propose an approach to a voluntary HSTLD program
  - Program operated by a 3rd party
- Latest progress on the HSDTLD program available here:
  - http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

Way Forward

- Update memo published May 2010
  - Located at www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf
  - Measures will contribute significantly to security and combating the conduct of malicious conduct within the
- Seek to support advisory group efforts outlined on ZFA strategy paper and HSTLD advisory group
  - ○ ZFA: www.icann.org/en/topics/new-gtlds/zfa-strategy-paper-12may10-en.pdf
  - ○ HSTLD: www.icann.org/en/topics/new-gtlds/hstld-program-snapshot-2-16jun10-en.pdf

All posted as part of the DAG 4 explanatory memos

Strategic Security Initiatives/DNS CERT: State of Play

- DNS CERT Operational Requirements Workshop - April
- Posting of Documents
  - Summary of Comments; Workshop report; List of Consults
- Exchange of Letters with ccNSO/GSNO/ALAC
  - Call for and preparation steps for working group
- Discussion within OARC of two-tier model for organization/foundation for DNS security and supporting DNS-CERT

Strategic Security Initiatives/DNS CERT: Main Themes

- Topic worth discussing
- Need deeper understanding of threats & risks
- Understand current response capabilities
  - Does this overlap with current CSIRT capabilities?
  - Focus on strengthening CSIRT capabilities
- Limited response capabilities in less-resourced regions

Strategic Security Initiatives/DNS CERT: Way Forward

- From formal summary
  - Work on threat and risk understanding
  - Continue to work with FIRST/CISRTs; initiate survey with CERT/CC on National CERT perspectives
  - Recognize desire ICANN not operate; focus on working with others and facilitating dialogue
  - Discuss workshop and Conficker reports
- Support community dialogues on DNS-CERT requirements, organizational and resources

DNS Risk Assessment

- Security Strategic Initiatives paper suggested ICANN conduct a gap analysis and system-wide DNS Risk Assessment as well as contingency planning and exercising
  - Risks on the “write” side
  - Contingency planning & response on response side
- Interest in the community for such an assessment, leveraging previous work from ENISA, IT Sector Baseline Risk Assessment, SSAC, others
- Seeking dialogue with community on next steps