A Registry Operators Perspective

Jeff Neuman, Vice President, Law & Policy
NeuStar, Inc.
NeuStar’s Anti-Abuse Program Timeline

- **2006**
  - Conducted legal and technical feasibility review
  - Added extra provisions to .BIZ restrictions doc.
  - Began reactive program to verify complaints of phishing, pharming, malware, bot-nets through in house experts.
  - Became first gTLD registry to “take down” domain names.

- **2007**
  - Began proactive program to find malicious domains
  - Reached out to Law Enforcement organizations
  - Began to share takedown data with other registries, security groups, law enforcement, educational institutions.

- **2008**
  - Created groups to tackle takedown issues
  - Joined industry associations

- **2009**
  - Play various critical roles in Conficker
Why Did NeuStar Get Involved in 2006?

- Feedback / avoid “dangerous domain” blacklist
- Internal desire to stop abuse of NeuStar infrastructure.
  - We did not want to give malicious parties the ability to organize their attacks
- Technical and legal expertise was available
  - Legal expertise required to formulate contractual obligations and discover and mitigate liability issues
  - Technical expertise required to perform verification and validation of complaints and proactively investigate domains
The Investigative Process

- Complaint received
- Proactive detection

Investigation

- Investigation performed
- Subsequent data analyzed

Report Details

- If issues are found, Legal is engaged
- If the domain is legit, notify national CERT/LE

Take Action
“Take Action”

- Once verified, we send report to Registrar sponsoring registration.
- Report contains a subset of investigation results
- Gives Registrars 12 hours to take down the name
- If no response, or if Registrar does not comply, we take the name out of the zone (Note Delete)
- Large majority of take down performed by Registrar within time
- Thousands of names taken down in .biz in past 3 years
  - No complaints, No legal actions.
Important Pieces of the Puzzle

- Industry participation a critical factor
  - Security forums
  - Security conventions
  - Security groups (private/public)
- Integration of law enforcement into processes
  - Collaborative effort to share/verify data
    - Verification of Child Porn done by LE
    - Results of our investigative process shared with LE
- Do not want to hinder current investigations
- Still need to continue these efforts (lots of work to be done still)