NeuStar Registry Services approach to Malicious Activity

ICANN London Consultation

Jeffrey J. Neuman
VP, Law and Policy

July 15, 2009

NEUSTAR™

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

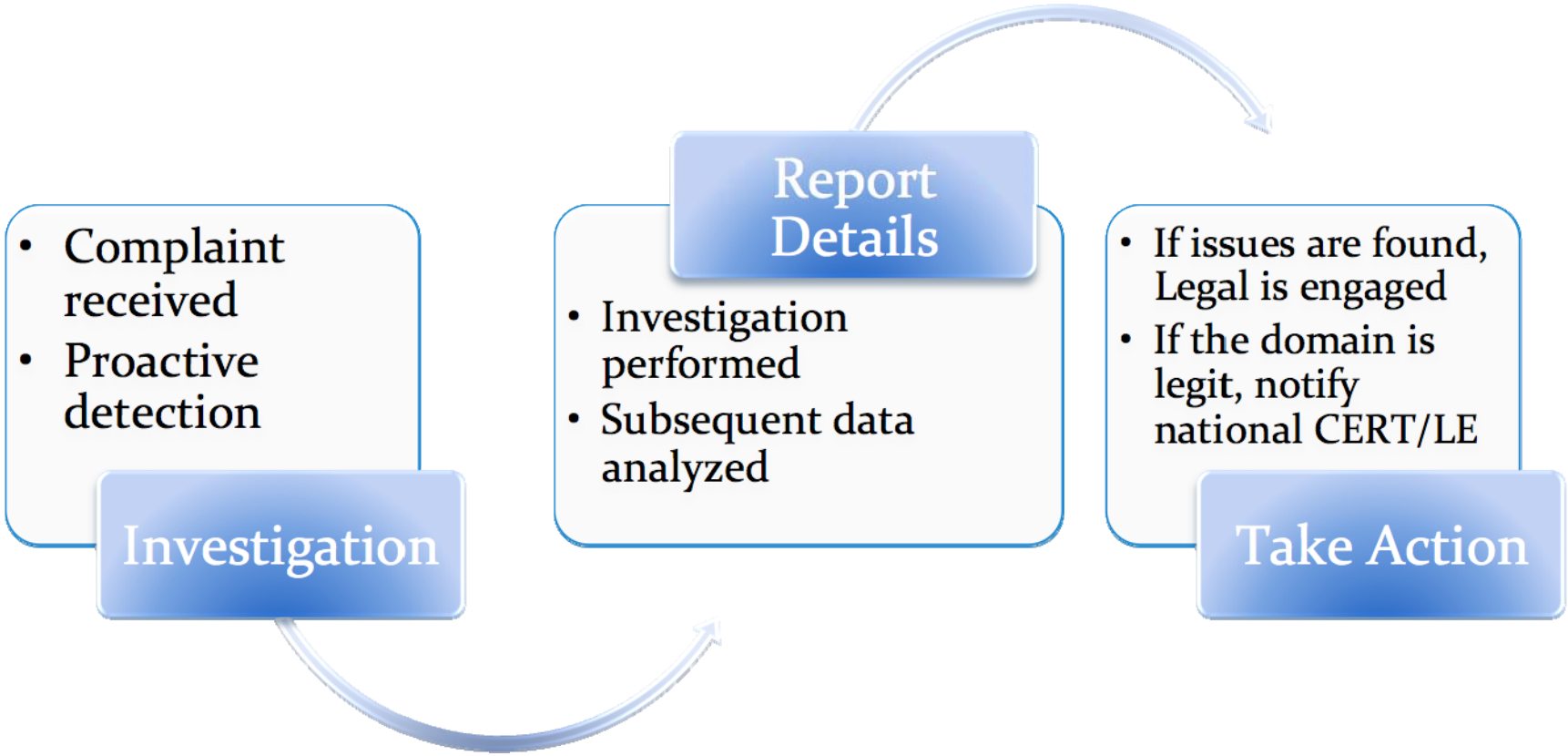
NEUSTAR™

DEFINITION OF ABUSE

- Appendix 11 .BIZ Registry Agreement
  - "Using the domain name for the submission of unsolicited bulk e-mail, phishing, pharming or other abusive or fraudulent purposes."
  - "reserves the right to deny, cancel, place on registry-lock or hold, or transfer any registration that it deems necessary, in its discretion, (i) to protect the integrity and stability of the registry . . (iv) to enforce, at its sole discretion, any of the Restrictions above….
- Does not include IP infringement, defamation, content or other use of a domain name.

NEUSTAR™

THE INVESTIGATIVE PROCESS



“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 (Not 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.

NEUSTAR™

“TAKE ACTION”

- 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)

NEUSTAR™

Coordination with Law Enforcement

- Respond promptly to LE Questions
- Claim “privilege” only when it is real
- Privacy and ToS are not necessarily in opposition
- Respond to Complaints from LE
- Have a clear and public policy

NEUSTAR™

Coordination with Other Registries – Registry Internet Safety Group

- RISG's mission is to facilitate data exchange and promulgate best practices to address Internet identity theft, especially phishing and malware distribution.
- Members include:
  - registry operators Afilias (.INFO), NeuStar (.BIZ, .US), Nominet (.UK), The Public Interest Registry (.ORG), and SIDN (.NL);
  - security firms Cyveillance, Internet Identity, McAfee, and Symantec;
  - registrars GoDaddy.com, MarkMonitor, MelbourneIT, Network Solutions, and Oversee.net;
  - observers from law enforcement agencies.
- Following points are consensus statements from the above members. *Individual RISG members have varying opinions and positions on new TLD issues.*

NEUSTAR™

Coordination with Industry Groups

- Anti-Phishing Working Group (APWG)
- Conficker Working Group
- Other DNS Abuse organizations, security groups and informal gatherings

NEUSTAR™

Summary – What should New Registries be doing?

- No “one size fits all” solution
- Registries and registrars face a number of challenges regarding abuse mitigation:
  - Legal: Varying privacy laws. Government regulation and control. Risks involved in suspending domain names (esp. false-positives).
  - Alleged malicious behavior can be difficult to identify and verify.
  - Technical challenges, including obtaining, examining, and acting upon high-quality data.
    - Registrant data may be dispersed and/or inaccurate.
    - Many forms of DNS Abuse involve other players beyond the control or scope of ICANN
- Costs. Security work is a cost center that impacts the bottom line.

What Should Registries do (con't) – NeuStar's view

- New gTLD applications should address abuse topics, such as proposing anti-abuse policies or procedures (based upon current best practices as defined by industry leaders). Applications that fail to include any mention of abuse should be referred to the Extended Evaluation process.

- New Registries should codify in their Registry Agreement and Registrar Agreements their Anti-Abuse policies and require that such policies be passed through to Registrants.

- Registries (or their back-end Operators) should join industry groups, including the RISG, APWG and others to collaborate on abuse issues.

What Should Registries do (con't) – NeuStar's view

- Registries, Registry Back-end Providers or their outsourced partners should have a process to receive complaints involving malicious abuse issues.
- Registries, either directly or through their back-end registry operators or other outsourced providers should investigate such complaints and attempt to verify such activity.
- Registries should, where appropriate, take appropriate actions against domain names that are objectively proven to be involved in domain name abuse.
- Registries should, subject to any legal prohibitions, share appropriate data with other registries, ICANN and other industry players that may be impacted by such abuse.

What Should Registries do (con't) – NeuStar's view

- Finally….

  Registries should seek out their local law enforcement agencies and find a way to legally collaborate with them.

- Thank you!

NEUSTAR™