Prohibiting Redirection & Synthesized DNS Responses

June 2009
Ram Mohan
SSAC Board Liaison
Redirection of DNS Responses

• **Issue**
  • Wildcarding of DNS records
  • Provides “valid” address and routing even when domain names do not exist

• **Consequences**
  • Breaks core DNS systems & legacy applications
  • Erodes trust relationships
  • Creates new opportunities for malicious attacks, without ability of affected parties to mitigate problem

*Reference Document: SAC041*
What breaks?

- Most basic Internet tools and applications break
  - Emails won’t bounce anymore
  - Search engines won’t be able to function as normal
  - Link checkers won’t find any broken links anymore
- And other software, applications, and equipment that depends upon the DNS “working” will break
SSAC Advice:

Clear & Significant danger to security & stability of the DNS

June 2009
Redirection: Board Recommendations

Take all available steps with appropriate entities to prohibit such use

Prohibit redirection/synthesis for all TLDs (gTLD & ccTLD, including IDN TLDs)

- Revise new gTLD Guidebook
- Consult with ccTLD community/GAC for new ccTLDs
- Revise existing gTLD agreements
- Add appropriate guidelines to existing ccTLD arrangements

Reference Document: SAC041
Questions?

Reference document SAC041 can be found at http://www.icann.org/committees/security/sac041.pdf