APWG Internet Policy Committee – Potential Issues for Abuse with new TLDs

MARTIN SUTTON
APWG
Manager, Group Fraud Risk & Intelligence
HBSC

July 15, 2009
Anti-Phishing Working Group
Institutional Profile

Membership restricted to:

- Financial institutions
- ISPs
- E-commerce sites
- Law enforcement agencies
- Technology & security companies
- Research partners (CERTs, Universities, Labs, Volunteer Responder Organizations)
- Consumer groups

More than 3000 members from 1700-plus companies and agencies world wide
APWG Roles

• Statistician – tracking and reporting
• Advisor – Governments, law enforcement, industry groups, press
• Mustering point – semi-annual meetings
• eCrime Data Clearinghouse
• Research
APWG Internet Policy Committee

91 Members
• Registries and registrars
• ISPs
• CERTs
• Law enforcement
• Brand owners
• Vendors
• Academia

Goal
Ensure anti-phishing concerns are represented during the creation or modification of Internet policies

Research
Promote and coordinate research into e-crime and e-crime prevention
Malicious Conduct in New TLDs

• Responding to internal interest and ICANN request for input from the community
• APWG will not address trademark issues
• All ideas included are subject to change, as we do not have full consensus on all issues yet
• Current draft is an “issues only” paper
  – Working on new paper that will include recommendations
    • Potential for policy/contract requirements (e.g. “thick whois”)
    • Likely to include many “best practices” suggestions
• Raise security awareness for new TLD operators
  – Security is hard to implement “after the fact”
Three Categories of Issues

• Potential issues introduced with this unprecedented roll-out of new TLDs
  – Issues inherent in the attributes of the TLD strings themselves and/or delivery to the marketplace

• Issues of scale
  – Concerns based on the vast increase in the number of registries

• Addressing longstanding concerns
  – Handle at the outset rather than “patch” later
  – Many potential new registry operators seeking advice
New TLD Attribute Issues

• Registry control/ownership
  – Could a criminal group control a registry?
• Introduction of TLDs with intrinsic potential for abuse
• Ownership and access to point-of-presence registration data
• New (weak) anti-abuse policies and procedures
• Changes to registrant qualifications
• Vulnerabilities and issues created by some potential new TLD strings
• Attacks based on the new TLD name
Scaling Issues

• Capabilities of new registries
• Adding orders of magnitude to the system’s complexity
• More data sources to consult
• Costs imposed on third parties
Longstanding Issues

- **Whois**
  - Character set
  - Continued access
  - Proxy registrations
- **DNS Authentication (DNSSec)**
- **Prevention of fraudulent registrations**
- **Malicious fast flux and other DNS attacks**
- **Standards for domain suspension**
- **Trading on names in own registry account**
For More Information

• http://www.apwg.org/

Thank You!