APWG Internet Policy Committee
Advisory on Potential Issues for Abuse with new TLDs

Peter Cassidy
Secretary General – APWG
www.antiphishing.org
pcassidy@antiphishing.org
Anti-Phishing Working Group
Institutional Profile

More than 3300 members from 1800-plus companies and agencies worldwide

• Financial institutions
• ISPs
• E-commerce sites
• Law enforcement agencies
• Technology & security companies

• Research partners (CERTs, Universities, Labs, Volunteer Responder Organizations)
• Consumer groups
APWG Roles

• Statistician – tracking and reporting on e-crime events and trends
• Advisor – Governments, international treaty organizations, law enforcement agencies, industry associations, press
• Mustering point – semi-annual meetings & peer-review research conference
• E-Crime Data Clearinghouse
• Research on policy and technology
91 Members from Across the Stakeholding Spectrum

• Registries
• Registrars
• ISPs
• CERTs
• Consumer groups

• Law Enforcement Agencies
• Brand owners
• Vendors
• Academic Research Centers
  • Carnegie Mellon
  • University of Alabama
  • Baylor University

Goal
Ensure counter electronic-crime concerns are represented during the creation or modification of Internet policies, regulations and laws

Development Focus
Promote, coordinate and publish original 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” advisory paper without conclusive prescriptions
  – 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
    • Control Fraud Risks

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

• 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
- Introduction of TLDs with intrinsic potential for abuse
  - .chase (70s rock band, town in Wisconsin and bank)
- Ownership and access to point-of-presence registration data
  - Reseller models diffuse domain registration responsibility, potentially complicating e-crime event response
- New (weak) anti-abuse policies and procedures
- Changes to registrant qualifications
- Attacks based on the new TLD name
  - TLD .BRANDx can give attackers info about a target that is useful for social engineering employees and company’s customers
Scaling Issues

• Capabilities of new registries
  – Will new registries and registrars have operational bandwidth to effectively manage fraud events

• Adding orders of magnitude to the system’s complexity
  – Complexity: the playground of the opportunist

• More data sources to consult for e-crime response
  – More TLDs increase system complexity and cost for 3rd party responders

• Costs imposed on third parties
  – Cost of zone file access agreements expand with number of new TLDs
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

• IPC Page: http://www.antiphishing.org/ipc.html
• Draft link: http://www.antiphishing.org/reports/APWG_IPC_gTLD_Expansion_Issues_DRAFT.doc

Rod Rasmussen, rod.rasmussen @antiphishing.org
+1 253 590 4100