Best Practices to Address the Abusive Registration of Domain Names

Workshop

Agenda

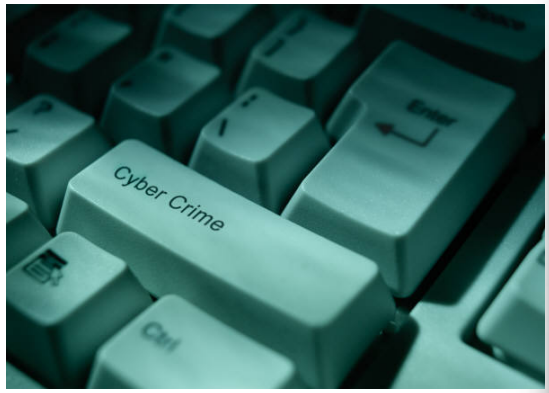
- Background & initial outline of Discussion Paper (Marika Konings & Steve Sheng)
- Registrar's Perspective (James Bladel, GoDaddy)
- Registry's Perspective (Jeff Neuman, Neustar)
- Commercial User perspective (Martin Sutton, HSBC)
- Non-Commercial User perspective (Wendy Seltzer)
- Perspective from those involved in development of best practices in other environments

  (Rod Rasmussen, Co-Chair APWG, Internet Identity - Greg Aaron, APWG Steering Committee, Afilias)

Background & Initial Outline of the Discussion Paper

Marika Konings & Steve Sheng

Background



- In its Final Report, the Registration Abuse Policies (RAP) Working Group recommended ‘the creation of non-binding best practices to help registrars and registries address the illicit use of domain names’.
- At its meeting on 3 February 2011, the GNSO Council requested ICANN Staff to prepare a discussion paper on this topic

ICANN Singapore 41 19-24 June 2011

- The effort should consider, but not be limited to:
  - Practices for identifying stolen credentials
  - Practices for identifying and investigating common forms of malicious use (such as malware and phishing)
  - Creating anti-abuse terms of service for possible inclusion in Registrar-Registrant agreements by registrars who adopt them, and for use by TLD operators who adopt them.
  - Identifying compromised/hacked domains versus domain registered by abusers'
  - Practices for suspending domain names
  - Account access security management
  - Security resources of use or interest to registrars and registries
  - Survey registrars and registries to determine practices being used, and their adoption rates

Best Practices in General

- Consideration of existing industry practices to see which are “best”
- Consideration of scope and applicability of industry practices
- Defining the “non-binding” nature of best practices
- Role of ICANN

Support for such an initiative

- ICANN resources
- Community process
- Security and Trust

Scope of Best Practices Effort

- Subjects identified by RAP WG
- Other areas?
- Resellers

Other Issues for Consideration

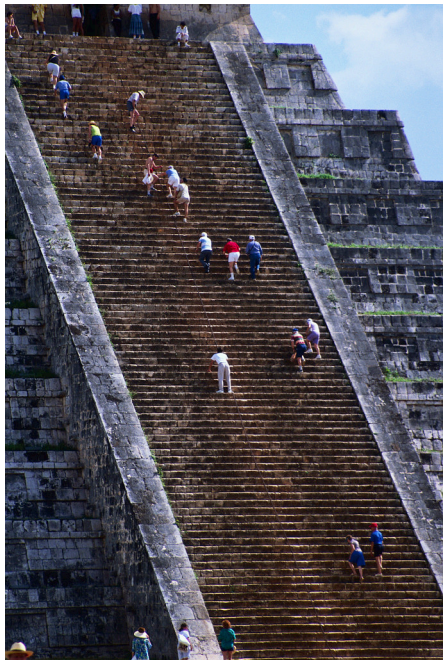
- Survey industry practices in operation globally
- Level of granularity that should be required in practices
- Updating and ongoing improvements
- Sensitivity organizations may have in disclosing practices
- Goals of evolving practices into best practices
- Promotion and dissemination of best practices that emerge from this activity
- Cost vs. benefit
- Means to identify and verify trusted abuse reporters
- Liability

Preliminary Inventory of Best Practices - Sources

- APWG: Anti-Phishing Best Practices
- SSAC: SAC 007, 028, 038, 040
- Anti-Abuse Policies and practices at various registries and registrars
- Conficker Working Group: Lessons learned / ICANN Conficker After Action Report
- MAAWG antiphishing best practices for ISPs and mailbox providers

Practice	Year	Developed By	Intended For
Investigate domain registrations/name servers related to known criminal activity.	2008	APWG	Registrars
Establish procedures in place with regard to handling phish domain termination to ensure handling an event in a timely and cost-effective manner.	2008	APWG	Registrars
Proactively use available data to identify and shut down malicious domains	2008	APWG	Registrars
Share fraudulent domain registration information with law-enforcement	2008	APWG	Registrars
Prohibit/minimize use of fast-flux domain	2008	APWG	Registrars
Offer stronger levels of protection against domain name registration service exploitation or misuse for customers who want or need them.	2009	SSAC	Registrars
Expand existing FAQs and education programs they offer to registrants to include security awareness.	2009	SSAC	Registrars
Consider the value of voluntarily having an independent security audit performed on their operations as a component of their security due diligence.	2009	SSAC	Registrars
Study whether registration services would generally improve and registrants would benefit from having an approved independent third party that will, at the request of a registrar, perform a security audit based on a prescribed set of security measures.	2009	SSAC	ICANN and Registrars
Establish Abuse Point of Contact	2009	SSAC	Registrars
Various Anti-abuse policies	2009	PIR, .INFO, Neustar, Godaddy	Registries and registrars
Various measures to reduce phishing threats	2008	SSAC	Registrars
Various measures to reduce Domain Name Hijacking	2005	SSAC	Registries and Registrars

Next Steps



- Learn from different perspectives today
- Update paper accordingly and outline options for the GNSO Council to consider as next steps
- Submit discussion paper to GNSO Council for its consideration

One World

One Internet

Questions?

One World

One Internet

A Registrar's Perspective

James Bladel

One World

One Internet

A Registry's Perspective

Jeff Neuman

One World

One Internet

A Commercial User's Perspective

Martin Sutton

One World

One Internet

A Non-Commercial User's Perspective

Wendy Seltzer

ICANN Singapore 41 19-24 June 2011

One World

One Internet

Perspective from those involved in development of best practices in other environments

Rod Rasmussen, Greg Aaron

ICANN Singapore 41 19-24 June 2011

Discussion