Best Practices to Address the Abusive Registration of Domain Names

Council Update
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.
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
<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Year</th>
<th>Developed By</th>
<th>Intended For</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigate domain registrations/name servers related to known criminal activity.</td>
<td>2008</td>
<td>APWG</td>
<td>Registrars</td>
</tr>
<tr>
<td>Establish procedures in place with regard to handling phish domain termination to ensure handling an event in a timely and cost-effective manner.</td>
<td>2008</td>
<td>APWG</td>
<td>Registrars</td>
</tr>
<tr>
<td>Proactively use available data to identify and shut down malicious domains</td>
<td>2008</td>
<td>APWG</td>
<td>Registrars</td>
</tr>
<tr>
<td>Share fraudulent domain registration information with law-enforcement</td>
<td>2008</td>
<td>APWG</td>
<td>Registrars</td>
</tr>
<tr>
<td>Prohibit/minimize use of fast-flux domain</td>
<td>2008</td>
<td>APWG</td>
<td>Registrars</td>
</tr>
<tr>
<td>Offer stronger levels of protection against domain name registration service exploitation or misuse for customers who want or need them.</td>
<td>2009</td>
<td>SSAC</td>
<td>Registrars</td>
</tr>
<tr>
<td>Expand existing FAQs and education programs they offer to registrants to include security awareness.</td>
<td>2009</td>
<td>SSAC</td>
<td>Registrars</td>
</tr>
<tr>
<td>Consider the value of voluntarily having an independent security audit performed on their operations as a component of their security due diligence.</td>
<td>2009</td>
<td>SSAC</td>
<td>Registrars</td>
</tr>
<tr>
<td>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.</td>
<td>2009</td>
<td>SSAC</td>
<td>ICANN and Registrars</td>
</tr>
<tr>
<td>Establish Abuse Point of Contact</td>
<td>2009</td>
<td>PIR, .INFO, Neustar, Godaddy</td>
<td>Registrars and registrars</td>
</tr>
<tr>
<td>Various Anti-abuse policies</td>
<td>2009</td>
<td>PIR, .INFO, Neustar, Godaddy</td>
<td>Registrars and registrars</td>
</tr>
<tr>
<td>Various measures to reduce phishing threats</td>
<td>2008</td>
<td>SSAC</td>
<td>Registrars</td>
</tr>
<tr>
<td>Various measures to reduce Domain Name Hijacking</td>
<td>2005</td>
<td>SSAC</td>
<td>Registrars</td>
</tr>
</tbody>
</table>
Next Steps

• Get your views and input
• Workshop on Thursday 23 June from 11.00 - 12.30 (see http://singapore41.icann.org/node/24623) to get Community input
• Update paper accordingly and outline options for the GNSO Council to consider as next steps
• Submit discussion paper to GNSO Council for its consideration
Questions?

One World

One Internet
Thank you!