Global DNS CERT

Business case for collaboration in security
DNS Background

- Growing risks to DNS security and resiliency
  - Emergence of Conficker; growing domain hijacking
- Community calls for systemic DNS security planning and response
Key Constituency

- the 2009 Global DNS Security, Stability and Resiliency Symposium pointed out that:

- “...resource constrained organizations have difficulty establishing networks of professionals to reach out and solicit information from. An organization will instinctively turn to its professional network, either in reaction to an event/incident or for proactive assistance. It is imperative that organizations know where to begin establishing their networks.”
# Capacity gap analysis

** Private/selective groups are excluded from the list **

<table>
<thead>
<tr>
<th>Framework</th>
<th>Project Sponsor</th>
<th>Public/Private</th>
<th>Participants – function</th>
<th>Participants Geographical distribution</th>
<th>Scope/mission</th>
<th>Operating funding model</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS OARC</td>
<td>DNS OARC, inc.</td>
<td>Public</td>
<td>Key operators, implementers, security providers, and researchers</td>
<td>Global</td>
<td>Information/data sharing (DNS-ops), workshops, data analysis, tools</td>
<td>Membership fee</td>
</tr>
<tr>
<td>Registry Internet Safety Group (RISG)</td>
<td>.ORG The Public Interest Registry, SIDN, Affilias, etc</td>
<td>Public Membership organization</td>
<td>gTLD, ccTLD registry- focused, domain registrars, security vendors and law enforcement agencies</td>
<td>North America</td>
<td>Data sharing, ML, Combat Internet identity theft, share data to improve overall Internet user security</td>
<td>No annual membership fee but members contributes activities cost</td>
</tr>
<tr>
<td>CWG</td>
<td>Microsoft and others</td>
<td>Public</td>
<td>Collaborative effort with technology Industry leader/academia</td>
<td>North America</td>
<td>Collaborative response for Conficker Warm</td>
<td>Organization/individuals Voluntary base</td>
</tr>
<tr>
<td>FIRST</td>
<td>FIRST, Inc.</td>
<td>Public / membership</td>
<td>Vetted community of CERTs/ CSIRTs</td>
<td>Global</td>
<td>Information sharing for Cyber security incident/ threat response</td>
<td>Annual Membership fee</td>
</tr>
<tr>
<td>ISC SIE</td>
<td>ISC</td>
<td>Private</td>
<td>Network operators (ISPs, enterprise, academic, and research), law enforcement (internationally), security companies (anti-virus, intrusion detection, &amp;etc), research (academic, Internet do-gooder, government, and commercial)</td>
<td></td>
<td>Information/data sharing in the Internet Security field. Shares mainly DNS information. Supports DNS security measurements and also information (e.g. passive DNS discovery of fast flux DNS names)</td>
<td>Fee structure</td>
</tr>
</tbody>
</table>
Mission of DNS CERT

“Ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS”
Goals

• Validated need for standing collaborative response capability for systemic threats/risks
  ✦ Full-time/global; serve all stakeholders especially less resourced operators – ensure bridge to existing security organizations and resources

• Fostering situational awareness; incident response assistance /coordination
Participation and feedback

- DNS CERT must respond to constituency
- Participation by key constituents
  - Adds capability to CERT
  - Extends its geographic reach
  - Ensure resource constrained operators needs are met
- Need your input on requirements
Way Forward

• Seek community feedback

✦ Session scheduled for Nairobi meeting (Monday 1400- Consultation on Security Strategic Initiatives Paper)

✦ Public review