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

ICANN

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."

ICANN

Capacity gap analysis

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

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

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"

ICANN

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

ICANN

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
    - http://icann.org/en/public-comment/#dns-cert

ICANN