DNS Abuse
Nii Quaynor
At Issue

• The Africa region has dependencies on DNS but not aware how critical to systems
• The region is typically resource constrained environments limited bandwidth, high latencies, unreliable facility and environments
• Have some technical capacity constraints
Nature of Challenge

• Awareness and skills training; DNS works seamlessly for most use

• Lack operational technical skills; incidence response

• Information sharing, best practices and incidence response capabilities limited

• Insufficient Trust among operators, researchers, law enforcement, policy makers, end users ...
What Would Help

• DNS has not been focal point of CERTs
• CERTs perform similar functions but no community practice on DNS yet
• Need to build community around DNS operators and DNS abuse; Participate as POC of CERTs
• operators should include DNS issues in Acceptable Use Policies
What Would Help (2)

- ccTLD contributions to ICANN could be in kind
- same contributions to ICANN could be used to strengthen African ccTLD security operations instead of for global DNS CERT
Tools that Help

• Augment lack of technical capacity with tools in short term; education for long term
• Incidence response and monitoring tools
• DNSSEC in a box tools
• DNSSEC GUI
AfTLD

- Building a community of ccTLD operators in Africa
- Program to develop capacity with ICANN/ISOC/NSRC
- ACRP (contingency planning), SROC (security registry operations) in Arusha, TZ - April 2009
- Others scheduled
CERTs in Africa

• There are very few operational CERTs (4) in Africa according to www.africa-cert.org

• Several countries have started establishing CERT POCs

• Add DNS CERT function to new CERTS
Environment Issues Matter

- Planning for disaster is very important
- Disasters may also come from unstable policy environment for ccTLDs
Thank You