ccTLD Security Incidents

Janelle McAlister
Domain Management Liaison
April 8, 2013
Domain Name Security Breaches on the Rise

- Individuals, now more than ever, recognize that domain security can be breached
- Registries and registrars are exploited as technical and social vulnerabilities are uncovered
- Once a TLD has been compromised it is highly likely that they will be a target again
- Since 2009, 31 TLDs have been compromised
Number of TLDs Compromised
Domain Name Security Breaches (continued)

- Once the hackers gain access to a system they update the DNS on high profile or high traffic domains so that the site will redirect to their ‘brag page’
- These incidents can damage the reputation of the registrants brand as well as the TLD
Targeting Domain Related Vulnerabilities

- DNS Administrator
- Registrar
- DNS Provider
- Registry

- Infrastructure Breaches
- Process Exploits
- Social Engineering Attacks
- Domain Hijackings
- Infrastructure Breaches

- Credential Theft
- Identity Theft
Precursors to Attacks

- Multiple requests to modify high profile domains
- Multiple requests to reset accounts or domain passwords
- Hacker posts instructions on social media sites
Securing Domain Related Vulnerabilities

- Early Detection
- Ability to Quickly Respond
  - Account Lock
  - Registry Domain Lock

- Operational Policies
- Hardened Infrastructure
- Two-Factor Authentication
- IP Address Restrictions

- Portal Locking
- Registry Locking

- Operational Policies
- Third-Party Evaluations
- Hardened Infrastructure
- Two-Factor Authentication
- IP Address Restrictions
  - Portal Locking
  - Registry Locking

- Two-Factor Authentication
- IP Address Restrictions
Registry Lock

- This feature would remove a high profile domain from the registry web interface

- All domain modification requests would be processed manually between the domain registry and registrar after a security protocol is followed

- Registry lock is used in conjunction to a registrars internal security practices
Questions?