An Overview of ICANN’s Training Program for *Investigating DNS Abuse/Misuse*

Dave Piscitello  
VP, Security and ICT Coordination

John L. Crain  
Chief Identifier Systems SSR Officer
Identifier Systems SSR Training Portfolio

- Registry (TLD) Operations
- Secure Registry Operations (SROC)
- DNSSEC (Robust & Reliable DNS Operations)
- Investigating DNS Abuse & Misuse
- Security Awareness for ICT end users
- Foundational Security for ICT administrators

Training partners or ICANN staff
ICANN staff
Future training for trust-based collaboration partners
What We’ll Discuss today

• Purpose of “Investigating DNS...”
• Topics we cover
• Who participates?
• Investigative methodology
• Resources we share
Purpose of the training

- To assist participants in understanding
  - DNS and name registration system operations
  - DNS and registration ecosystems and players
  - How criminals abuse or misuse domain names or DNS
  - How to collect indicators or evidence of abuse or misuse
  - How the data collected may be relevant to investigations
Topics we cover

- What are indicators of misuse/abuse in
  - DNS (zone) data?
  - Domain registration data?
  - DNS traffic?
  - Authoritative name servers and resolvers?
  - Addressing and routing information

- What additional information can you use?
  - Reputation (scoring) systems
  - Content analysis
Where can you find these indicators?

• *Primary sources are publicly available*
  – The DNS
  – Domain and IP Whois
  – Web-based services
    • commercial, free, open source, research projects

• Trust-based collaborative communities
  – Interveners, researchers, investigators, operators
  – Certain of these are vetted communities
Inves&ga&ve Philosophy

Markers include checks like these...

- Recent domain registration creation date
- Suspicious registrant contact data
- Privacy protection service
- Spoofing or confusing use of a brand
- Name composition or length
- Known DGA or malware control point
- High frequency/volume of Name errors
- Suspicious or notorious name servers
- Suspicious or notorious hosting location
- What’s the neighborhood like?
- Base site content is non-existent or bad
- Anomalies or clues in DNS Zone data
- Reputation

“Match fingerprints” analog

no one marker is sufficient to conclude a domain is malicious

Course adapts to changes in adversary behavior
Who participates?

• Individuals with roles in combatting cybercrime
  — Law enforcement
  — Jurists
  — ICT network operators
    (government, infrastructure, registry)

• Individuals with roles in capability building programs
  — Security community members
  — Partners in capability building collaboratives
Resources We Show and Share

• Tools to identify abuse points of contact
  – Domain names, host names, IP addresses, ASNs
  – Domain and IP registrants, registries, registrars
  – DNS, Content hosting, or Mail Exchange providers
Resources we show and share

- Publicly available tools to identify, collect or analyze
  - Content (web pages, sites,
  - Malicious content (URL, file, email, attachment)
  - Reputation system operators
Tools we show and share

- Hosting (web, DNS, mail) or traffic origins
- ISPs, mail exchange, or DNS operators
- Block list services
Questions?