ICANN’s Name Collision
Controlled Interruption

Edward Lewis
Technical Services
ICANN
Agenda

- Name Collisions
- Controlled Interruption
- Check Your Logs/Intrusion Detection Systems
- Where to Get Help
Name Collision – The Leak

Private network configured in such a way that could “leak” the request to the public Domain Name System, when using a name in a private network that *does not exist* in the public DNS.
Name Collision – The Roaming Leak

Private network configured in such a way that could "leak" the request to the public Domain Name System (DNS), triggered by the use of a name in the private network matching a name in the public DNS.

User tries to access a service on a private network when connected to the Internet outside of that network.
Why Does This Happen?

- **Local DNS Name spaces**
  - Use of “adopted” names, from documentation
  - Split-brain DNS
- **Search List Processing**
  - Use of short unqualified domain names
  - Falling back on DNS lookup failure
Name Collision – The “Crunch”

Private network configured in such a way that could “leak” the request to the public Domain Name System (DNS), triggered by the use of a name in the private network matching a name in the public DNS.

User tries to access a service on a private network when connected to the Internet outside of that network.
As New Top-Level Domains are Added

• Once-failing names might “succeed”
  o The name to address result may be different

• Operational Interruption
  o At best, updates are needed
  o At worst, data and information may be leaked
How to Avoid Interruption

• Pre-emptive strike
  o Use only Fully Qualified Domain Names
  o Avoid or limit reliance on search lists
  o Use globally-recognized registered names
  o Deterministic - good!

• But you may not catch all the places where short, unqualified domain names have been used
Controlled Interruption

• When a new top-level domain opens
  o A set of responses are returned to names that might be subjects of collision
  o Designed to be a nuisance to those leaking queries
  o Designed to contain the damage of a data breach

• “Breadcrumbs” left in
  o Logs (of connection failures)
  o Intrusion Detection Systems (suspicious addressing)
127.0.53.53

• A “curious” loopback address
  o Meant to make connections fail, no data sent out
  o Meant to encourage operators to “look this up”

• Other clues that fixes are needed
  o Mail server (MX) is “your-dns-needs-immediate-attention”
  o SRV lookup returns that same hostname
  o TXT record says “Your DNS configuration needs immediate attention”
What to Do?

• If there is a reasonable belief of demonstrable, severe harm, report it to ICANN
  o https://forms.icann.org/en/help/name-collision/report-problems

• For further information, consult

• Or
  o https://www.icann.org/resources/pages/name-collision-2013-12-06-en
Q&A

• The URL for the Mitigation Guide, once again:

• Want to know “what’s coming”?
  o https://newgtlds.icann.org/newgtlds.csv
  o Includes TLD name, contract date, delegation date
Social Media

https://twitter.com/ICANN

http://gplus.to/icann

https://www.facebook.com/icannorg

http://weibo.com/icannorg

http://www.linkedin.com/company/icann