# Looking at corp.com as a proxy for .corp

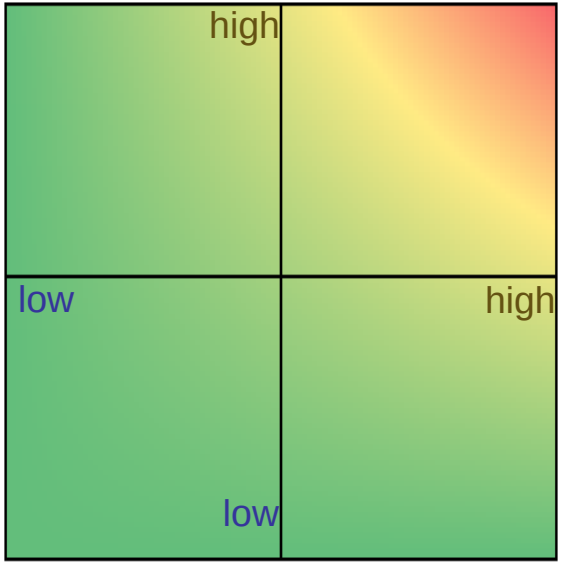
Colin Strutt
Interisle Consulting Group

# Concerns about name collisions

- ICANN's Security and Stability Advisory Committee (SSAC) (among others) had expressed concerns:
  - SAC 045 (2010) Invalid Top Level Domain Queries at the Root Level
  - SAC 057 (2013) SSAC Advisory on Internal Name Certificates
- ICANN engaged Interisle to study name collisions
  - Start mid May 2013
  - Draft report end June 2013 for ICANN meeting in Durban
  - ICANN published "Name Collision in the DNS" report

# Assessing risk of name collisions

- Risk comprises two variables:
  1. Probability of occurrence
     - Primary focus of the Interisle study
  2. Severity of consequences
     - Magnitude/cost of consequences
     - Who would be harmed
     - Cost of remediation
     - Responsibility for remediation
     - Capability of remediating parties

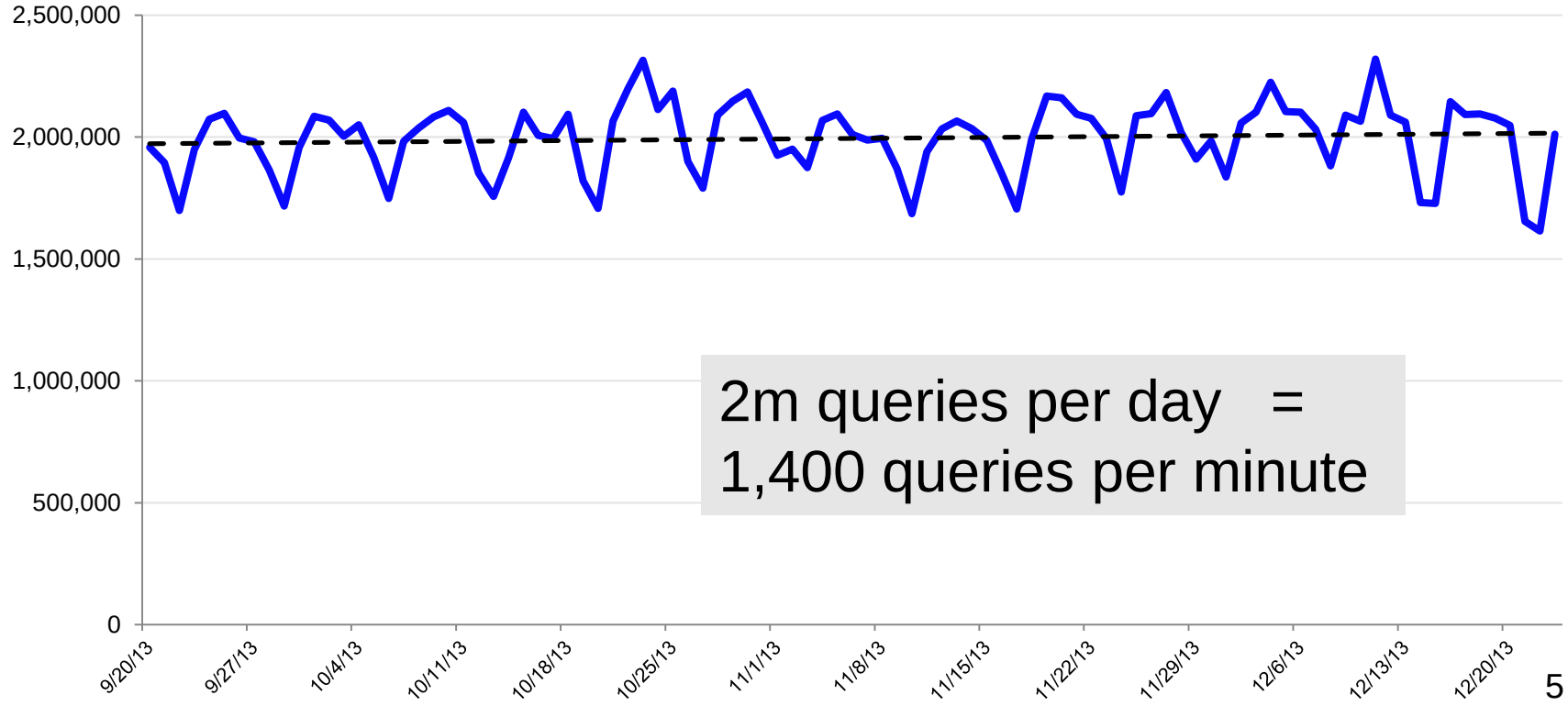


# The corp.com domain

Interisle Consulting Group

- Mikey O'Connor registered corp.com in 1994
- No subdomains registered
- But he was seeing a **lot** of DNS queries
- Could we learn anything about TLD name collisions using corp.com?
- Advantage: corp.com was already delegated
- Initial short study sponsored by Mikey and NetChoice
- Configured DNS for corp.com to monitor query logs

# DNS queries per day to corp.com



# What we found

Interisle Consulting Group

- Queries from
  - ~300,000 IP addresses in ~30,000 subnets
  - Using ~14,000 AS numbers
  - Across >200 countries
- Predominantly from large resolvers, including:

# Nearly 6 million distinct 3LDs

Interisle Consulting Group

_msdcs win co benq ce wpad _tcp

accent tsi _sites trx alv gbp invsfoxepo01

c00 ns1 ns2 bqc gek ati bqa usfxbinvscm01pv

usrenalcare mwp cbt mexichem isatap sms_slp invshouxchmbx04

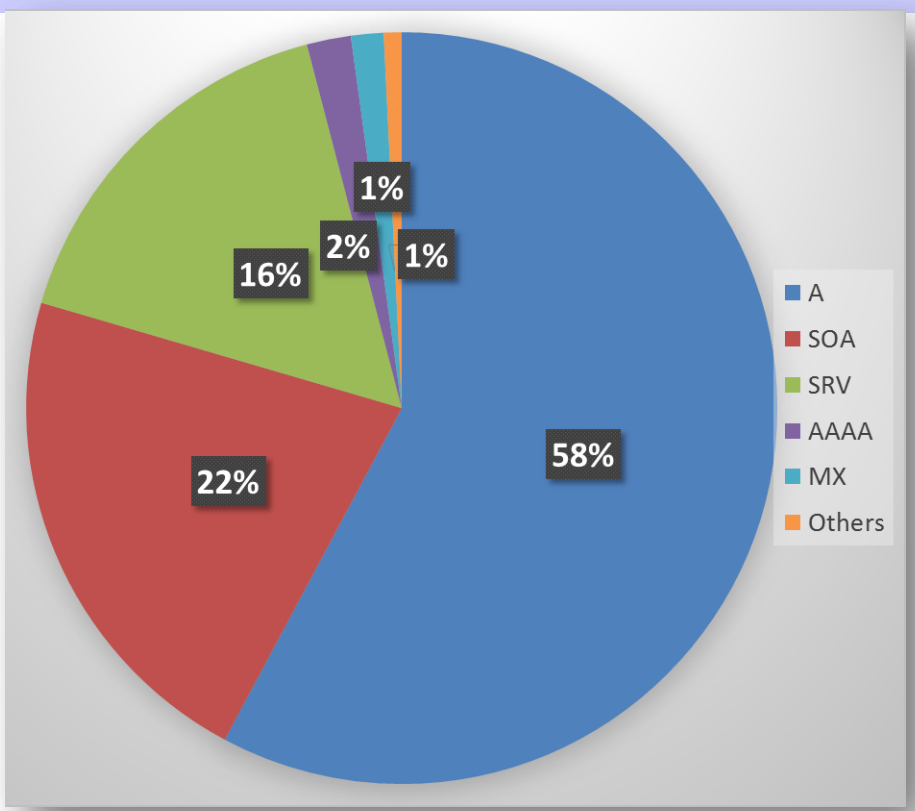
wm bluerhino invsfoxxchmbx02 invshouxchpub01 invsfoxxchmbx01

invsfoxxchpub01 invshouxchmbx03 invsfoxepo02v invsfoxwdc01 bqeu dedussrvfil001

invscopweb01 rumosiomfil01pp egcaisrvfil002 ctlman0012 skbrasrvfil001 invsfoxwdc02

inchnsrvapp008 invspdascm01 invsfoxwdc03 ctlmonhpdm01v twkhhsrvfile002 delimiomfil01pp pleurtycfs01 ips-sol07

# QTYPEs in corp.com queries




| QTYPEs | % |
|---|---|
| A | 58% |
| SOA | 22% |
| SRV | 16% |
| AAAA | 2% |
| MX | 1% |
| NS | 0% |
| PTR | 0% |
| TXT | 0% |
| ANY | 0% |
| SPF | 0% |
| CNAME | 0% |
| DS | 0% |
| A6 | 0% |
| DNSKEY | 0% |

# Predominant query patterns

| | | |
|---|---|---|
| 3LD.corp.com | ~50% | |
| QTYPE = SOA | ~20% | (from ~60% of addresses) |
| Underscore | ~20% | |
| QTYPE = SRV | ~15% | |
| Chrome | ~ 5% | (from ~10% of addresses) |
| wpad…corp.com | ~ 3% | (from ~10% of addresses) |
| QTYPE = MX | ~ 1% | (from ~35% of addresses) |
| isatap…corp.com | ~ 1% | |

# Deconstructing ‘underscore’ patterns

Interisle Consulting Group

SIP: _sip…

XMPP: _xmpp…

Apple’s Bonjour: …_dns-sd…

Active Directory: _sites _gc _dc _pdc (~15%)

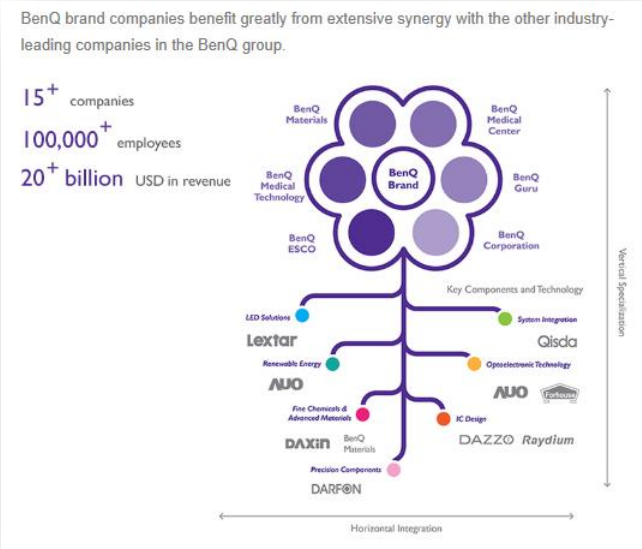
Other uses of underscore – but lower query volume

sms_.... _mssms… _vlmcs… nlb_... mp_...

# Active Directory example

Interisle Consulting Group

- benq.corp.com
- Most AD traffic through a Taiwan telecom ISP
- >400 queries per hour to the same DNS names
- Not all from one IP address
- But we do see repeated queries
- Apparently, AD cannot take “no” (non-existent domain) for an answer



# QNAMEs for two QTYPEs

Interisle Consulting Group

| MX<br>~1% queries ~29k QNAMEs | |
|---|---|
| corp.com | 15.3% |
| mitsubishi.corp.com | 1.7% |
| sp.corp.com | 1.4% |
| accuride.corp.com | 1.3% |
| ioa.corp.com | 1.2% |
| cabot.corp.com | 1.2% |
| urs.corp.com | 1.1% |
| idex.corp.com | 1.0% |
| asn.corp.com | 0.9% |
| idg.corp.com | 0.9% |

| SOA<br>~20% queries ~40k QNAMEs | |
|---|---|
| corp.com | 21.2% |
| ctlply0417.corp.com | 1.0% |
| win.corp.com | 0.7% |
| wrsabneh3732.corp.com | 0.6% |
| egcaiiom6ytj2l.corp.com | 0.5% |
| alvmnrlt0249.alv.corp.com | 0.5% |
| xp076596.win.corp.com | 0.5% |
| fact01.corp.com | 0.4% |
| invshq00763l.corp.com | 0.4% |
| ushouiom01710l.corp.com | 0.4% |

# QNAMEs for two patterns

Interisle Consulting Group

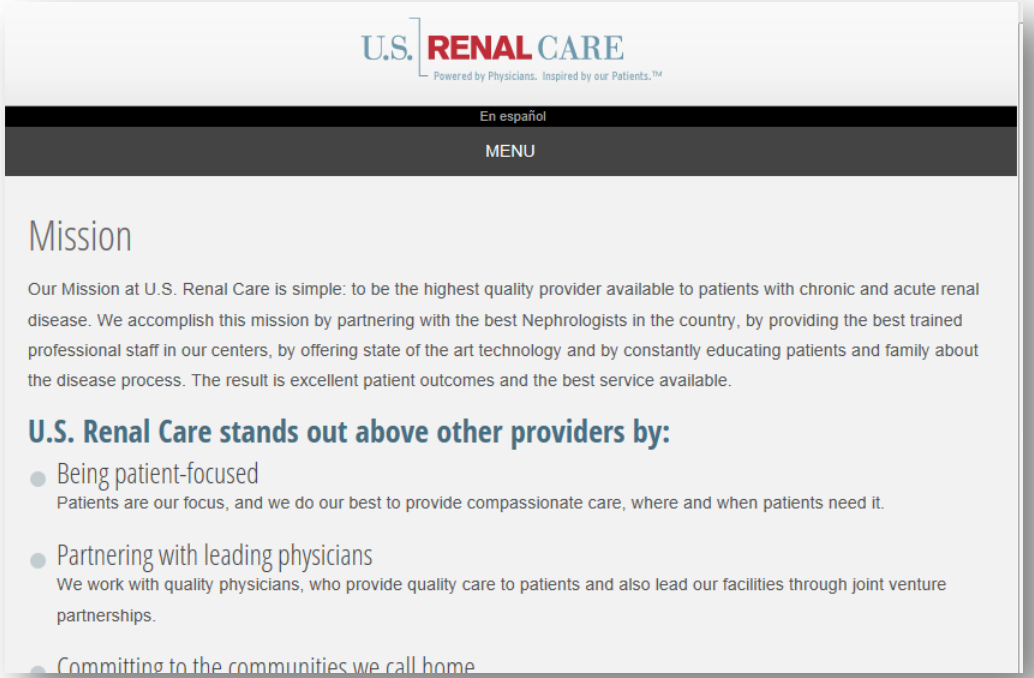
| wpad ~3% queries ~700 QNAMEs | |
|---|---|
| wpad.corp.com | 52.7% |
| wpad.benq.corp.com | 4.2% |
| wpad.accent.corp.com | 3.3% |
| wpad.win.corp.com | 2.9% |
| wpad.bluerhino.corp.com | 2.0% |
| wpad.tsi.corp.com | 1.9% |
| wpad.wm.corp.com | 1.8% |
| wpad.bqa.corp.com | 1.8% |
| wpad.trx.corp.com | 1.7% |
| wpad.dmz.trx.corp.com | 1.6% |

| isatap ~1% queries ~650 QNAMEs | |
|---|---|
| isatap.corp.com | 40.8% |
| isatap.benq.corp.com | 7.6% |
| isatap.accent.corp.com | 4.6% |
| isatap.win.corp.com | 3.6% |
| isatap.tsi.corp.com | 3.1% |
| isatap.bqa.corp.com | 2.9% |
| isatap.wm.corp.com | 2.2% |
| isatap.usrenalcare.corp.com | 2.1% |
| isatap.bluerhino.corp.com | 2.0% |
| isatap.bqc.corp.com | 1.9% |

# Trying to contact one affected user

Interisle Consulting Group

- The string “usrenalcare” appears in ~1% of queries
- >5k IP addresses
- Is it US Renal Care?
- Contact attempts
  - Email using WHOIS
    - no reply
  - Phone from WHOIS
    - voicemail, no reply



# Contacting ISP customers

- “Customer” should be easier than a cold call?
- Identifying a customer takes time
- Finding the right contact at a company takes time
- Explaining observed DNS queries and TLDs is tricky
- Results:
  - Thank you for telling us
  - It was a guest network over which we have no control
  - We’ve fixed it (but we won’t tell you how it happened)

# What the ISP saw

Interisle Consulting Group

- An ISP, or other organisation, can determine potential name collisions from DNS query logs

- Locating the source of those queries can be problematic
  - DNS log (at an ISP resolver or root) shows an IP address, but…
  - An IP address can be DHCP-assigned – e.g., cyber-café
  - The IP address might be that of another DNS server
  - Timestamp basis may vary in different logs
  - The IP address may not be from the ISP's customers

# Identifying a name collision

Interisle Consulting Group

- How will users know that the problem they're experiencing is a result of a new TLD?
- Will a support group be able to diagnose a name collision from reported symptom(s)?
- Will a collision-based security hole be detectable?
- Most users won't recognize a name collision problem
- Companies are not highly motivated to explore mitigation strategies

# ISPs role in supporting customers

- For an ISP or similar organisation
  - They’re between a rock and a hard place
  - Between their customers and the new TLDs
  - They may be the first line of support
- But are ISPs prepared?
  - Will support staff be trained?
  - Will they have the knowledge and expertise to help users?

# Where does that leave ‘users’?

Interisle Consulting Group

- Choice 1 – the user is responsible
  - They should not have used those TLDs
  - They are responsible for fixing their problem
- Choice 2 – the user needs information and help
  - Those who created the problem may no longer be around
  - Current people may not have the requisite knowledge/skills
    - To diagnose problems resulting from name collisions
    - To resolve the problems
    - It could be vendor software

# Outreach approaches

- The pull model
  - Provide information for users to find and retrieve
- The push model
  - Provide information to users
  - Before delegation – notification of potential problems
  - After delegation – resolving observed problems

# Call for action

- New TLDs are already delegated
- Users may not be adequately prepared
- Augment the ICANN “outreach” activities
- Prepare ISP support organisations
  - Develop specific outreach materials for ISP customers
  - Develop training materials for ISP support staff

Interisle Consulting Group

# Questions?