

NCAP Discussion Group | 3 February 2021 | 19:00 UTC

Agenda:

1. Welcome and roll call
2. Update to SOI
3. Update on Study 2
4. .LAN Case
Study: https://docs.google.com/presentation/d/1LeiVG3t94kqCNPPvMklvQtTJx0iKEMKqvUDPggnnWEY/edit#slide=id.gb590d7797c_0_19
5. .LOCAL Case
Study: https://docs.google.com/presentation/d/1_luvm2MtGNu8sdj1NT8GVHfRf1tkajlFRJ1o_r4Ww8/edit#slide=id.gb5b9e08a3d_0_25
6. Next analysis measurements?
7. AOB

Table of Contents

***Conflict of Interest discussion*.....2**

***Study 2 update*2**

***.LOCAL*.....2**

Slide 1: Daily Query Volume3

Slide 2: Qtype Distribution3

Slide 3: Unique Daily Source IPs4

Slide 4: GEOGRAPHICAL Distribution5

Slide 5: ASN Distribution5

Slide 6: Root ASN Overlap and IP Growth.....6

Slide 7: Label Analysis6

Slide 8: Data Attributes7

***.LAN*7**

Slide 1: Daily Query Volume8

Slide 2: Qtype Distribution8

Slide 3: Unique Daily Source IPs9

Slide 4: Geographical Distribution.....9

Slide 5: ASN Disribution.....10

Slide 6: Root ASN Overlap and IP Growth10

Slide 7: SLD Overlap analysis.....10

Slide 8: SLD Analysis11
Slide 9: Label analysis 212
Data Attributes12

Conflict of Interest discussion: Warren’s title has changed from Standards Technical Program Manager to Director of Internet Standards,

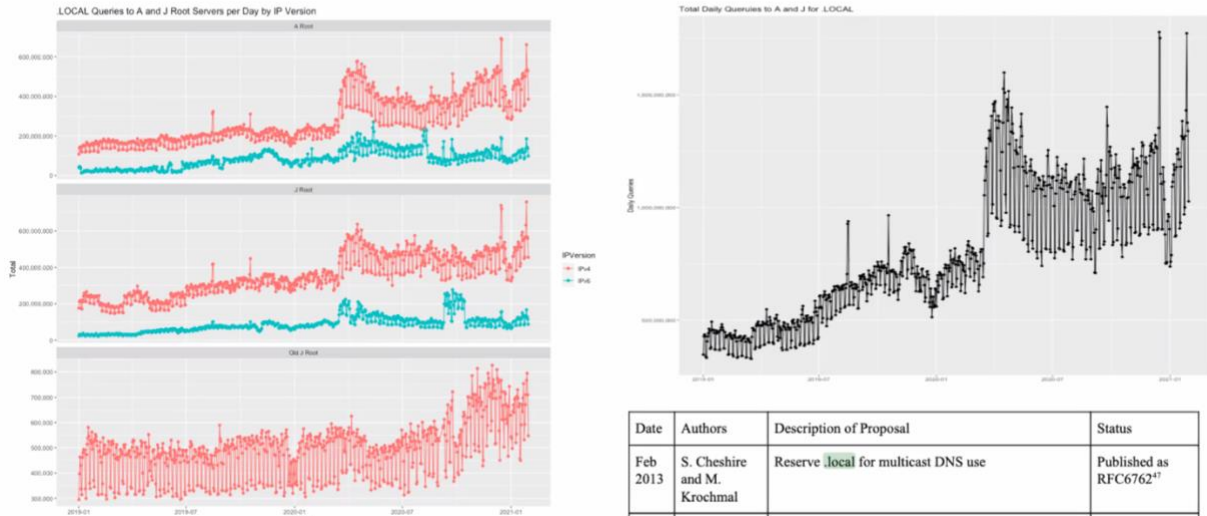
Study 2 update: package for Board is complete.

.LOCAL

Name Collision Analysis .LOCAL

Slide 1: Daily Query Volume

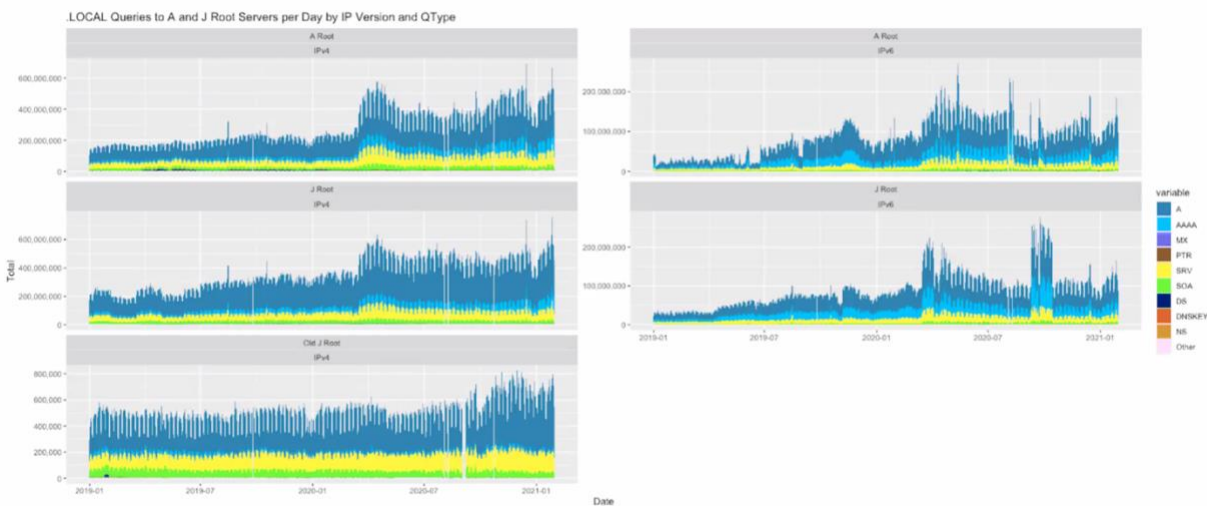
.LOCAL Analysis :: Daily Query Volume



Traffic volumes over 1.5 billion queries per day. Covid issue with transient devices used at home at non-standard DNS environment
 SAC113: highlighted that .local was tagged for multicast DNS use

Slide 2: Qtype Distribution

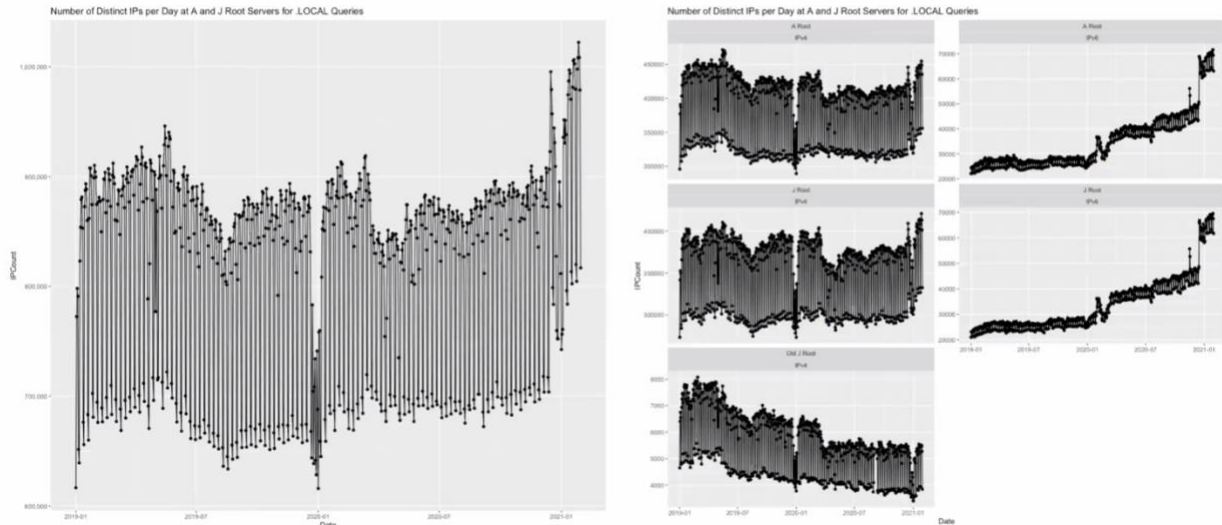
.LOCAL Analysis :: Qtype Distribution



See soa records, different than other strings

Slide 3: Unique Daily Source IPs

.LOCAL Analysis :: Unique Daily Source IPs



Increased traffic without increase in # of sources (unusual). # of sources just increased recently though.

Rod: doesn't match pandemic pattern. Are source Ips due to broad use of public resolvers, or a large IP infrastructure

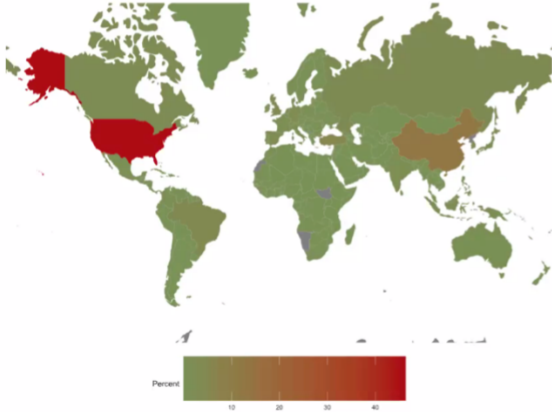
In future might want to do analysis of known large public ISP recursivers and differentiating their traffic from AS numbers, for example.

STEVE: what might account for this phenomena : An IP address used even once and then there's, an increase that will show up as no change the range of IP addresses, whereas before you had IP addresses that had never been used, presumably that are then included, so If there were a phenomenon which there was kind of a background of all of the IP addresses occurred a little tiny bit. And then you had a massive increase you wouldn't be able to see that phenomena exactly in the way that this is being analyzed so I was just another thought trying to explore why this is behaving as it is.

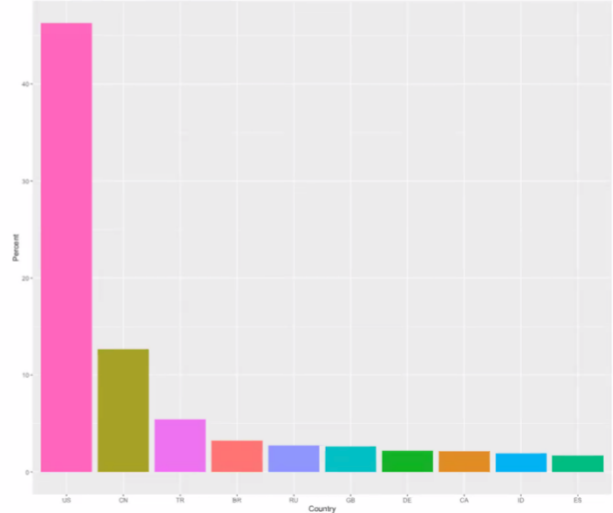
Slide 4: GEOGRAPHICAL Distribution

.LOCAL Analysis :: Geographical Distribution

.LOCAL Global Distribution



Top Countries for .LOCAL to A and J Root Servers

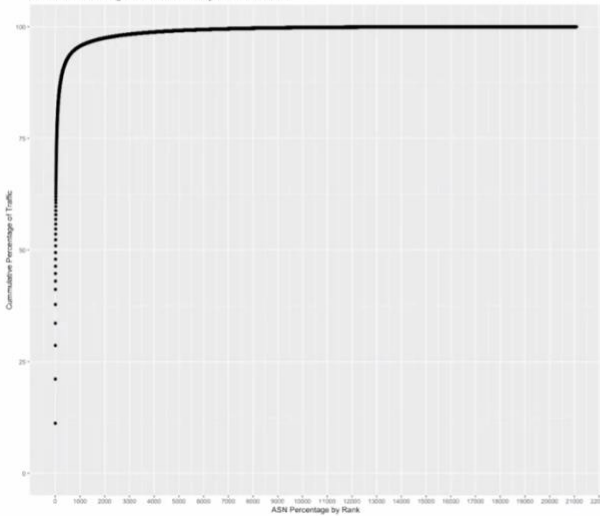


US mostly

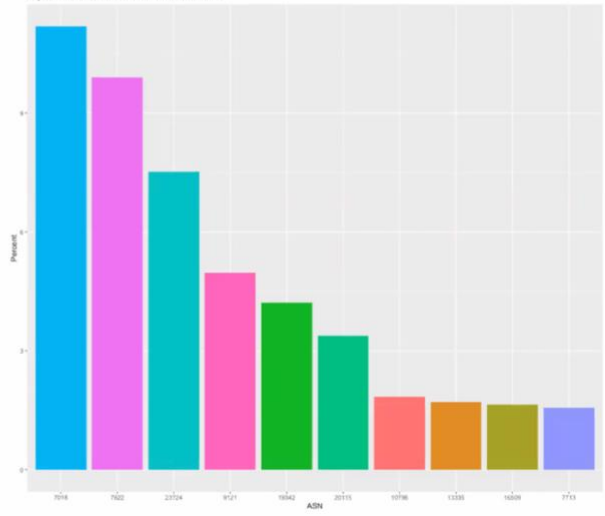
Slide 5: ASN Distribution

.LOCAL Analysis :: ASN Distribution

Cummulative Coverage of .LOCAL Traffic by Rank Order ASNs



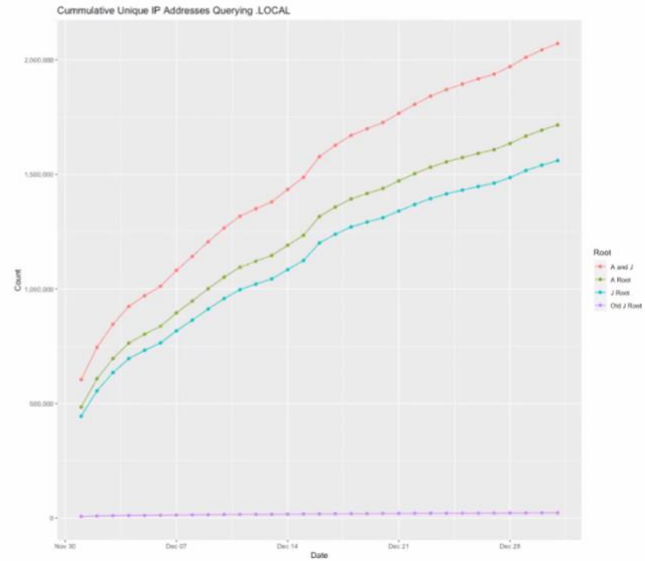
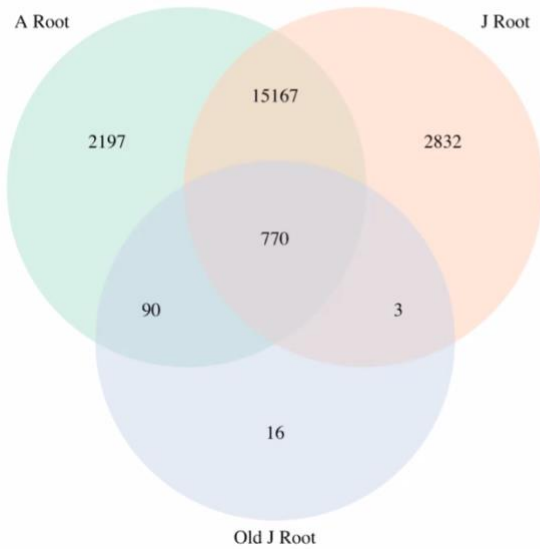
Top ASNs for .LOCAL to A and J Root Servers



Scale of X axis: other studies dropped at 900 ASNs, but .LOCAL is over 22000 different ASNs- wider spread than other case studies but 50% of traffic comes from top 10 (mostly US/China ISPs)

Slide 6: Root ASN Overlap and IP Growth

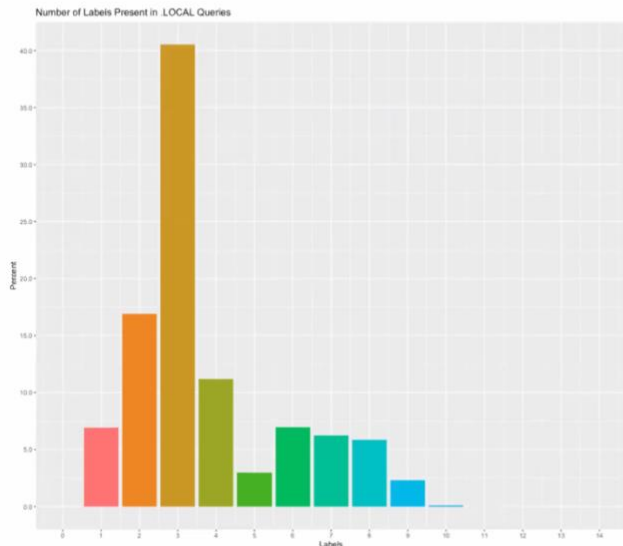
.LOCAL Analysis :: Root ASN Overlap and IP growth



J root always has much larger collection of catchment than A root

Slide 7: Label Analysis

.LOCAL Analysis :: Label Analysis



SLD	Percent	ThirdLabel	Percent
1: cluster	5.21249852	1: svc.cluster	3.51330249
2: _tcp	1.49889226	2: com.cluster	1.64049344
3: rsyslogd	1.33485913	3: .rsyslogd	1.33485913
4: com	0.91223693	4: _ipp._tcp	0.91939797
5: corp	0.59915487	5: _ipps._tcp	0.49808035
6: _	0.59818977	6: .constructif	0.22731603
7: navigon	0.58851840	7: ad.usfood	0.19233000
8: demo	0.34343977	8: com.meintelbras	0.15422826
9: group	0.25521015	9: .retracker	0.11704026
10: meintelbras	0.24681727	10: onelondon.tfl	0.08225368
11: constructif	0.22731762	11: americas.ppd	0.08144675
12: usfood	0.19251837	12: ld.corp	0.06288812
13: mcint	0.18398142	13: uk.group	0.06220033
14: net	0.18000130	14: asia1.group	0.05934020
15: ppdi	0.17633557	15: europe.ppd	0.05106923
16: root	0.15693040	16: areal.eurofins	0.05032565
17: domain	0.15608579	17: googleapis.com	0.04940997
18: retracker	0.11704026	18: .wpad	0.04735098
19: ad	0.11596449	19: google.com	0.04543337
20: hkvisionwifi	0.09515900	20: com.group	0.04444318
21: eurofins	0.09451535	21: com.jltbrnet	0.04383821
22: lord	0.09421412	22: prant.prantl	0.04310520
23: fujitsu	0.09260529	23: _msdcs.corp	0.04241632
24: tfl	0.09206417	24: lat.tyc	0.04116376
25: experian	0.09123802	25: _msdcs.domain	0.03913942
26: samsungdemo	0.08891397	26: kt.group	0.03877845
27: pregis	0.08764093	27: tiktokv.com	0.03711911
28: tes	0.07830863	28: us.experian	0.03687628
29: hidalgocounty	0.07609835	29: .ntp	0.03675101
30: kriton	0.07327312	30: com.hkvisionwifi	0.03673716

Left: 40% have 3 labels, only 7% had 1 label (.mail had 50% with 1 label) int

Like .corp – some are anchored under delegated tlds, so you wonder if this is by-product of suffix search list appendage

Right: associated with DNS service discovery protocols

Slide 8: Data Attributes

Data Attributes When Evaluating Collision Strings

Traffic Properties:

- Network diversity
 - Number of unique ASNs, /24s, etc.
 - Distribution of traffic (e.g. heavily weighted in a few ASNs)
- Geographical diversity
- Qtype distribution
- Query volume
- Longitudinal trends

Qname and Labels:

- Distinct SLDs
 - Distribution of traffic over SLDs
- Amount of “noise” (e.g. Chromium)
- SLDs appear to be delegated TLDs
- First label features
 - DNS-SD
 - Common protocols
- Qname Minimization effect

Other Attributes:

- The string's context
- OSINT of string being used
- Data sensitivity and catchment of data collector

.LAN

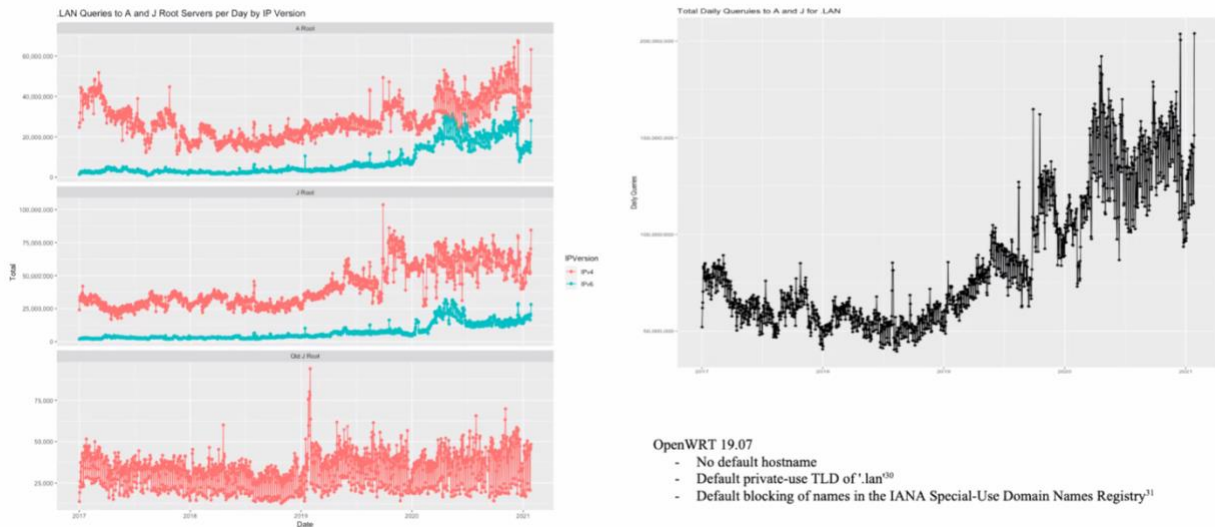
Name Collision Analysis

.LAN

Used in open wrt- open source for home routers with wide variety of software features. Uses private use .tld .lan

Slide 1: Daily Query Volume

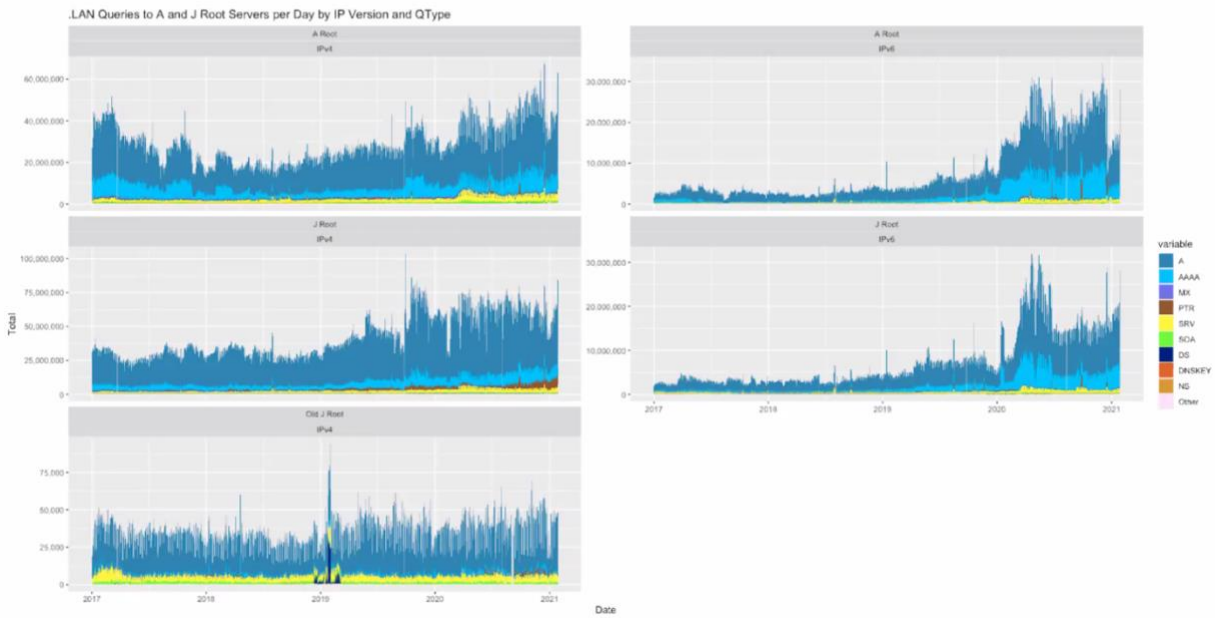
.LAN Analysis :: Daily Query Volume



See mar 2020 shift. Decrease at end of 2020 - patch of chromium

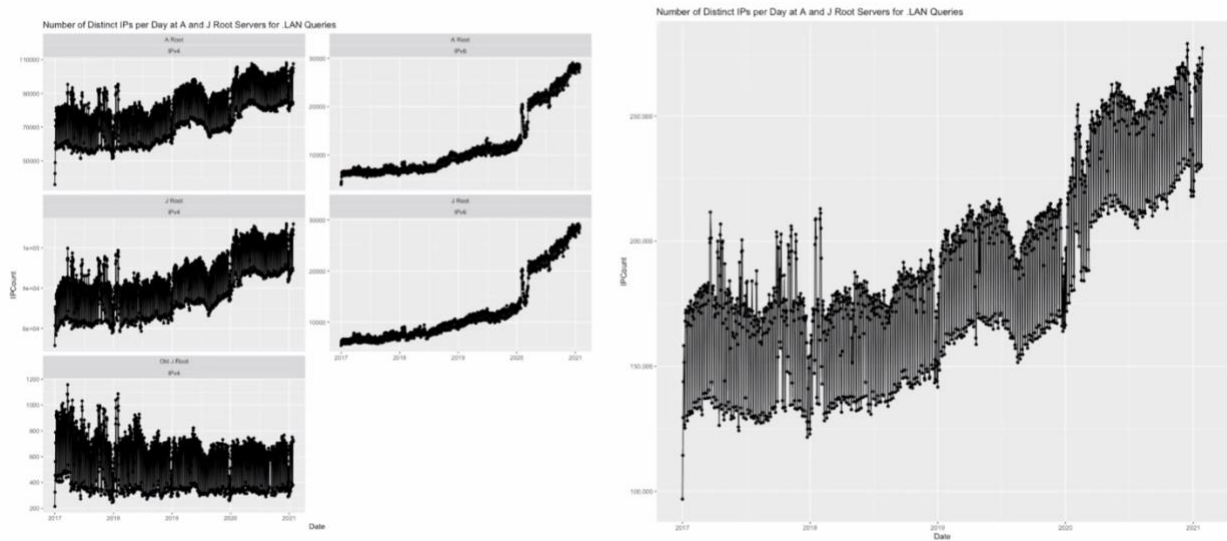
Slide 2: Qtype Distribution

.LAN Analysis :: Qtype Distribution



Slide 3: Unique Daily Source IPs

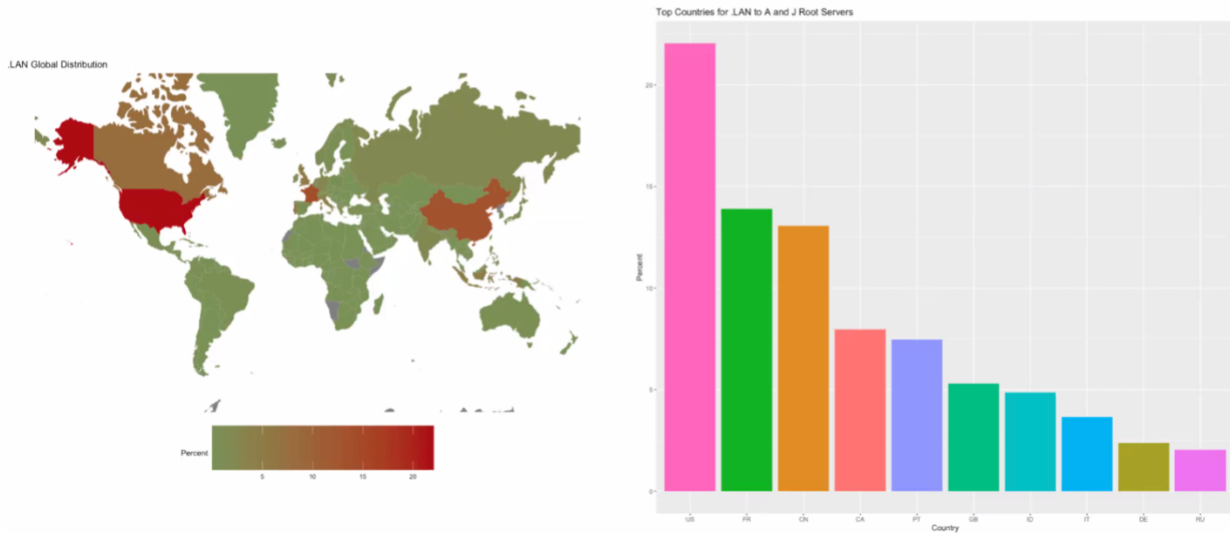
.LAN Analysis :: Unique Daily Source IPs



Not as pronounced covid bump

Slide 4: Geographical Distribution

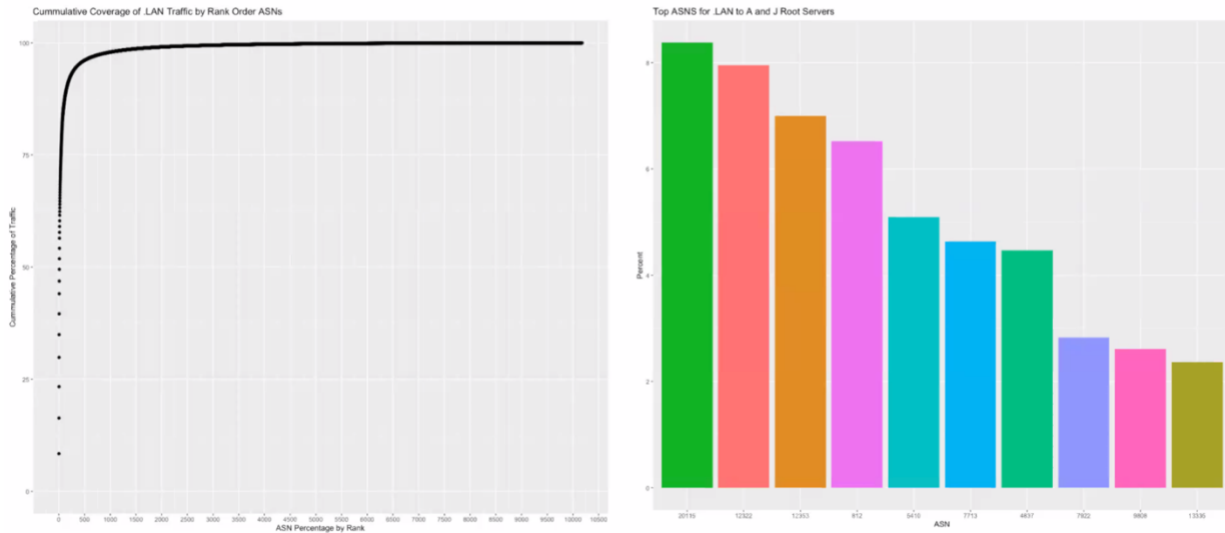
.LAN Analysis :: Geographical Distribution



More spread out than others

Slide 5: ASN Distribution

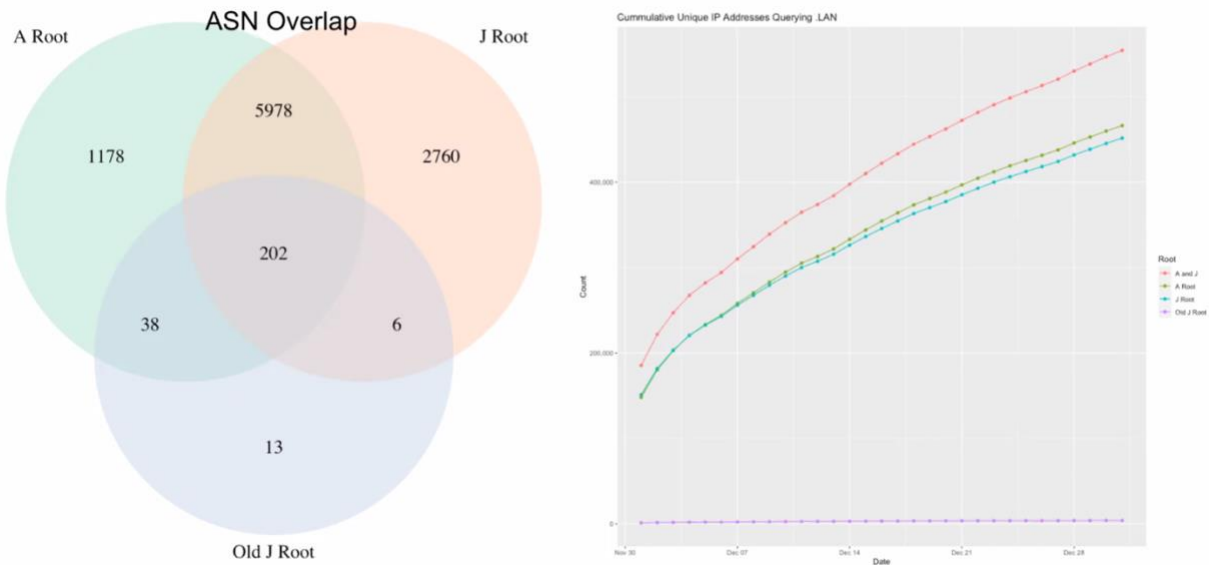
.LAN Analysis :: ASN Distribution



10000 different ASNs sending queires for .lan Q names, top 10 ASNs

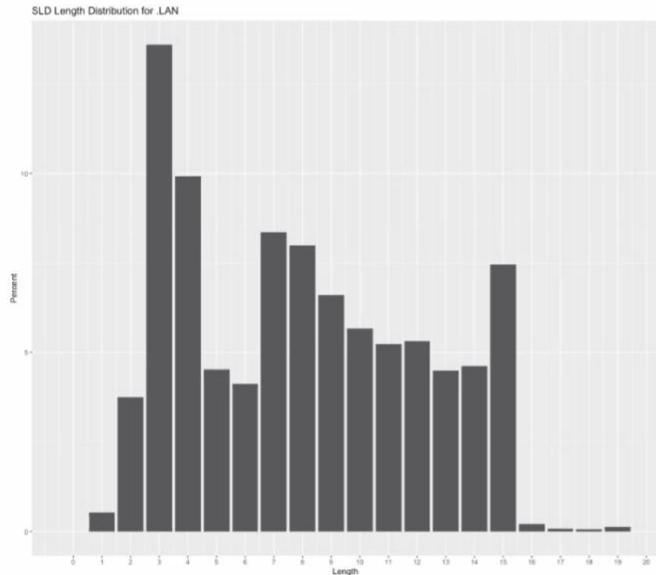
Slide 6: Root ASN Overlap and IP Growth

.LAN Analysis :: Root ASN Overlap and IP growth



Slide 7: SLD Overlap analysis

.LAN Analysis :: SLD Overlap Analysis



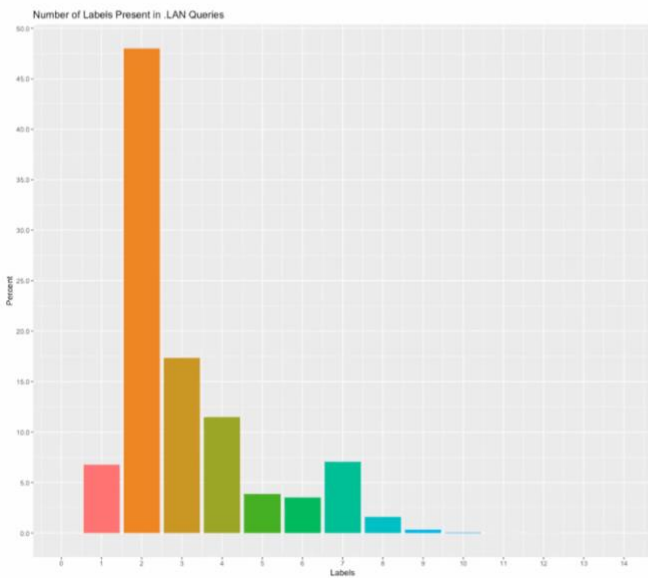
.LAN Names for 12/31/2020

- Unique Qnames: 46,117,456
- Unique SLDs: 37,440,698

Drops off at 15 chars so good portion of traffic probably chromium queries

Slide 8: SLD Analysis

.LAN Analysis :: SLD Analysis



SLD	Percent	ThirdLabel	Percent
1: com	7.12973991	1: in-addr.arpa	5.15606803
2: arpa	5.18317203	2: .wpad	0.75620481
3: net	0.84312410	3: qq.com	0.47754414
4: wpad	0.75697182	4: avl01.avlcorp	0.31909082
5: cn	0.63376531	5: _dns-sd._udp	0.31551641
6: _tcp	0.46920957	6: ww.hl	0.30687549
7: _	0.41307506	7: google.com	0.25032900
8: hl	0.38232998	8: com.cn	0.24325432
9: local	0.37466281	9: googleapis.com	0.24286857
10: avlcorp	0.37420665	10: facebook.com	0.19768126
11: org	0.35474061	11: corp.zodiac	0.15541521
12: _udp	0.33067472	12: .isatap	0.15135092
13: basis	0.30296325	13: snssdk.com	0.14456837
14: vhgroup	0.29140558	14: hicloud.com	0.14448897
15: asm	0.22288120	15: tiktokcdn.com	0.14359312
16: zodiac	0.22274337	16: ntp.org	0.13207514
17: sercol	0.19536148	17: baidu.com	0.13203020
18: alliance	0.19518921	18: vgeu.vhgroup	0.13126917
19: zebra	0.17299217	19: tiktokv.com	0.12444467
20: isatap	0.15135092	20: vaillant.vhgroup	0.12275184
21: c3connect	0.13618587	21: _msdcs.workgroup	0.10863245
22: workgroup	0.11708910	22: ksmobile.com	0.10593366
23: lan	0.11662245	23: fbcnd.net	0.09152888
24: corp	0.11101439	24: yximgs.com	0.09115886
25: tsi	0.10818003	25: corp.alliance	0.07994349
26: lixil	0.10498463	26: amemv.com	0.07836976
27: emergent	0.09072142	27: _aaplcache3._tcp	0.07742597
28: galaxy	0.08977388	28: _aaplcache._tcp	0.07724320
29: enivest	0.08697547	29: _aaplcache1._tcp	0.07712785
30: mobily	0.08560098	30: _aaplcache2._tcp	0.07681325

```

> sum(x$Percent)
[1] 20.04771
    
```

2 labels is average for .lan

.LAN Analysis :: Label Analysis

.LAN

Column1	Column2
lan	9071680
_ldap	7016308
wpad	4442042
_kerberos	850354
msoid	752678
_	655521
www	470657
isatap	355617
tracker	326938
api	311709
lb	298665
_tcp	277524
1	251172
_msdcs	225903
_gc	160900
dc	152028
_sites	116483
_aaplcache3	111750
_aaplcache	111421
_aaplcache1	111266
_aaplcache2	110761
_aaplcache4	110480
_vmcs	109290
b	105420
2	100823
3	97680
connectivitycheck	95719
db	94965
server-test	91574
android	90751

.HOME

	SLD	Percent
1:	hitronhub.home.	9.75412714
2:	com.home.	6.61782804
3:	home.	3.03802436
4:	_.home.	2.68200505
5:	net.home.	1.19227441
6:	ht.home.	0.57062557
7:	fios-router.home.	0.52528746
8:	_tcp.home.	0.30401179
9:	wpad.home.	0.29160084
10:	org.home.	0.28520555
11:	cn.home.	0.26442140
12:	_udp.home.	0.23789951
13:	ch.home.	0.21296067
14:	ru.home.	0.19720468
15:	arpa.home.	0.08625248
16:	io.home.	0.08591727
17:	tv.home.	0.08381899
18:	isatap.home.	0.07388558
19:	me.home.	0.06444656
20:	biz.home.	0.05839011
21:	unifi.home.	0.05735203
22:	workgroup.home.	0.05627388
23:	in.home.	0.05361050
24:	home.home.	0.05328508
25:	info.home.	0.04995074
26:	uk.home.	0.04905044
27:	co.home.	0.04637510
28:	xyz.home.	0.04604986
29:	jpg.home.	0.03915547
30:	local.home.	0.03533617

```

> sum(x$Percent)
[1] 27.11263
    
```

.LAN

	SLD	Percent
1:	com	7.12973991
2:	arpa	5.18317203
3:	net	0.84312410
4:	wpad	0.75697182
5:	cn	0.63376531
6:	_tcp	0.46920957
7:	_	0.41307506
8:	hl	0.38232998
9:	local	0.37466281
10:	avllcorp	0.37420665
11:	org	0.35474061
12:	_udp	0.33067472
13:	basis	0.30296325
14:	vhgroup	0.29140558
15:	asm	0.22288120
16:	zodiac	0.22274337
17:	sercol	0.19536148
18:	alliance	0.19518921
19:	zebra	0.17299217
20:	isatap	0.15135092
21:	c3connect	0.13618587
22:	workgroup	0.11708910
23:	lan	0.11662245
24:	corp	0.11101439
25:	tsi	0.10818003
26:	lixil	0.10498463
27:	emergent	0.09072142
28:	galaxy	0.08977388
29:	enivest	0.08697547
30:	mobily	0.08560098

```

> sum(x$Percent)
[1] 20.04771
    
```

Slide 10:

Data Attributes

Data Attributes When Evaluating Collision Strings

Traffic Properties:

- Network diversity
 - Number of unique ASNs, /24s, etc.
 - Distribution of traffic (e.g. heavily weighted in a few ASNs)
- Geographical diversity
- Qtype distribution
- Query volume
- Longitudinal trends

Qname and Labels:

- Distinct SLDs
 - Distribution of traffic over SLDs
- Amount of "noise" (e.g. Chromium)
- SLDs appear to be delegated TLDs
- First label features
 - DNS-SD
 - Common protocols
- Qname Minimization effect

Other Attributes:

- The string's context
- OSINT of string being used
- Data sensitivity and catchment of data collector

See discussion 48mins into Zoom recording

