DNS Stakeholders and Protocol Stability

"Initial Comments, As Requested"

David Dagon

May 10, 2019

Introduction

Atlanta Traffic Analysis

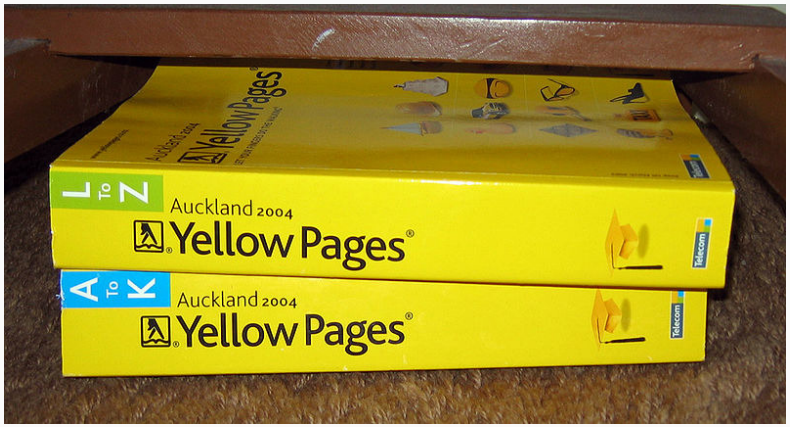
Motivating Question

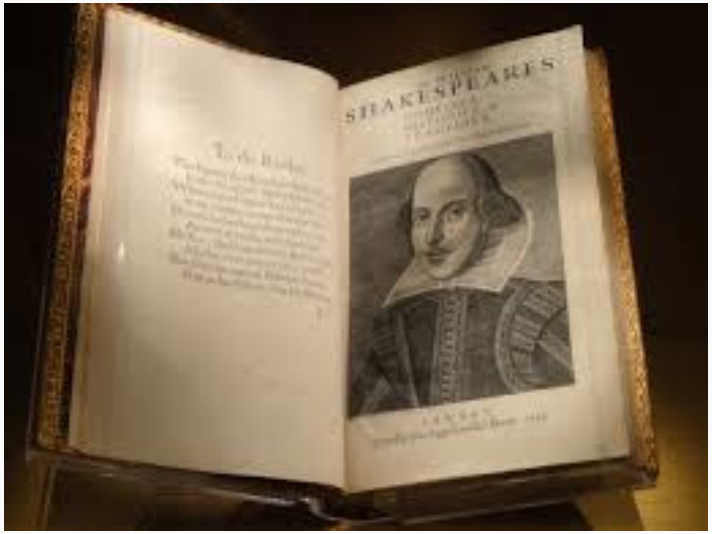
Left: Beveled Rim Bowl (Univ. of Mainz, Germany)

Right: Akkadian Deluge tablet of Gilgamesh epic (British Museum, London)

Question: Which tells us more about Uruk, ca. 4000 BCE?

Motivating Question





Left: Yellow Pages (Wikipedia)

Right: Shakespeare First Folio (Wikimedia)

Question: Which tells us more about our era?

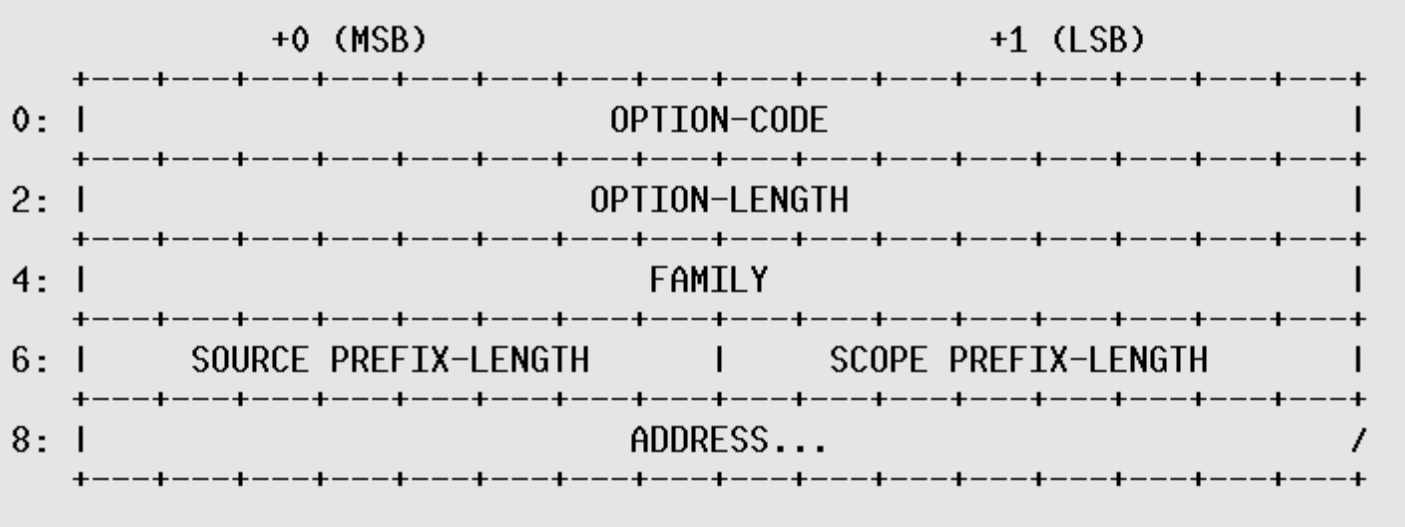
Motivation: Similarly, "discarded" DNS tells us much about our Internet, compared to a single HTML document.

Outline

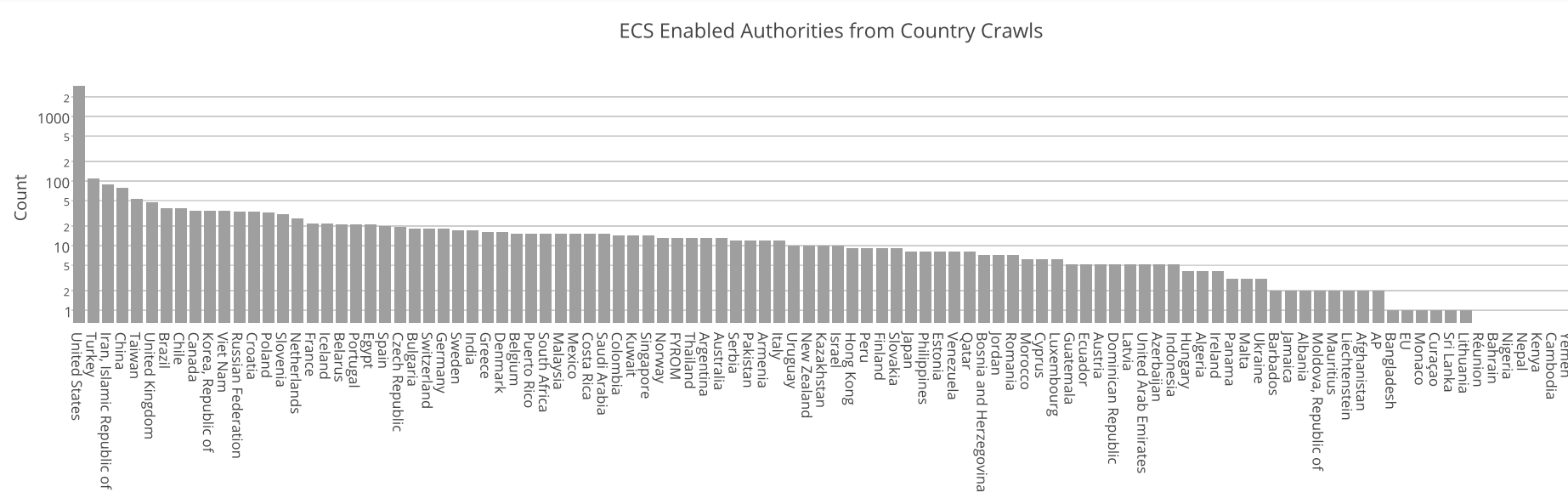
- Argument: DNS is an (i) inherently policy-infused (ii) infrastructure protocol; (iii) providing identity information mappings.
- "DNS Policy" has new currency:
  - Cloud DNS changes the relationship between core resolution speakers: `stub, recursive & authority`.
  - DNS complexity means protocol evolution selects trade-offs among DNS speakers.
    - Limited protocol consideration generates unexpected losers.**Demonstration with i2p ... and also tor**
- Passive & active DNS are near peer collectives of DNS information
  - Privacy focused protocol changes must address both. **Noted with DNS prefetching**
- These lessons may inform DOH adoption

EDNS-Client-Subnet (ECS) and Stakeholder Relationships

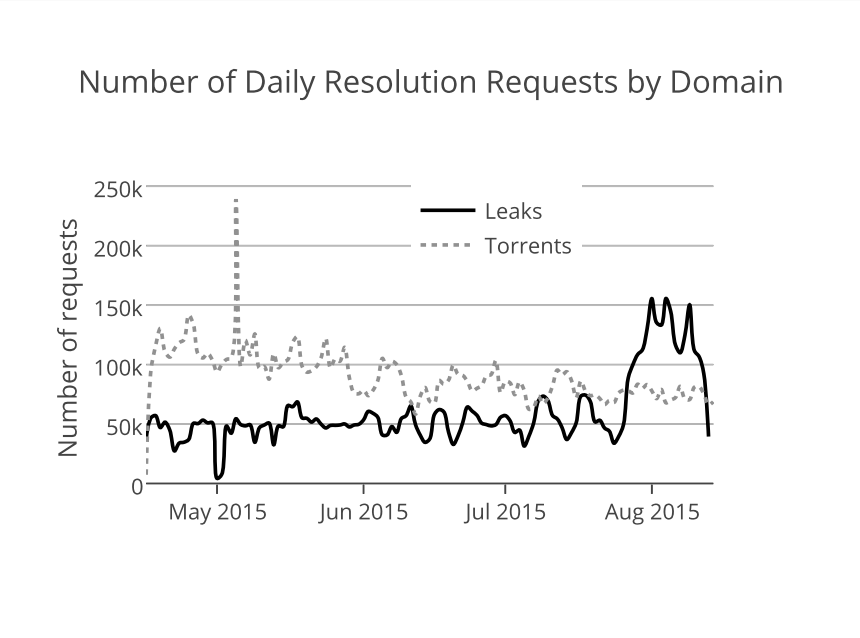
- Client Subnet in DNS Queries, RFC 7871 [4]
- Topologically distant resolvers provide client network octets
- `scope`/`mask` fields for authority/resolver to set extent of answer

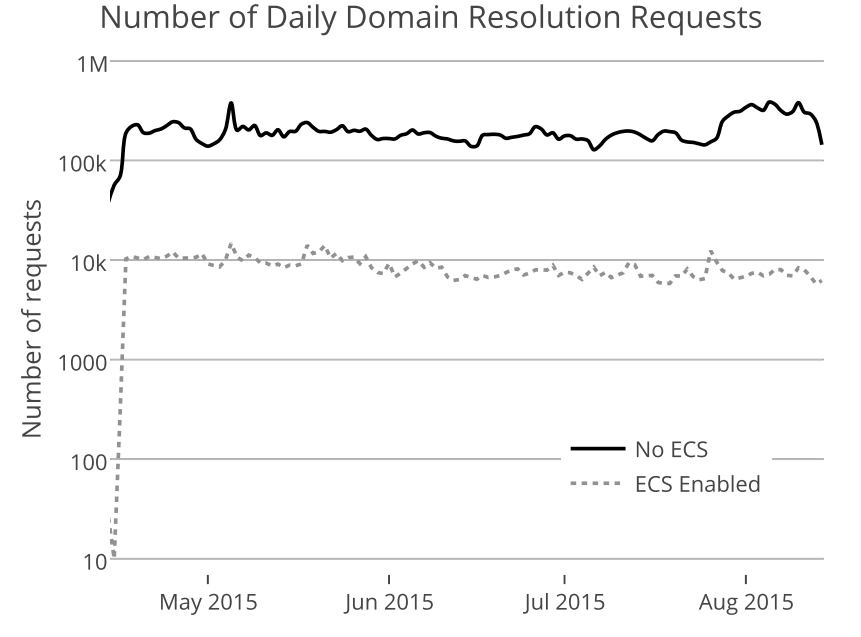


ECS Implementation



ECS Adoption

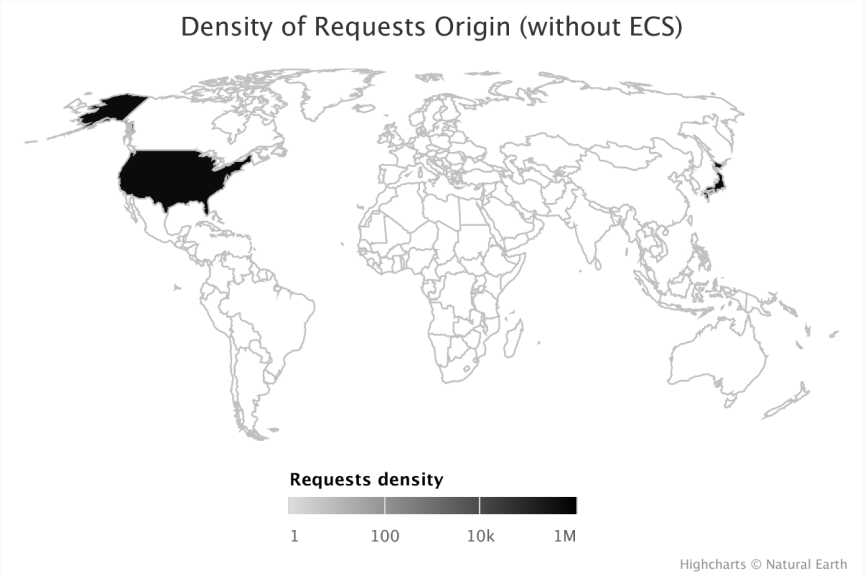


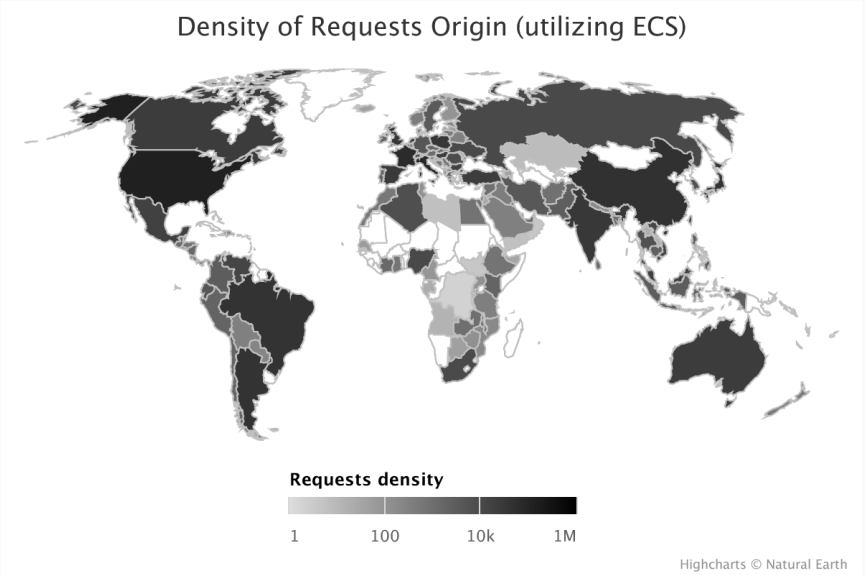


(l) Leak & Torrent authority lookups, daily

(r) Leak & Torrent ECS rates ($<<\approx$ 20% global cloud market share)

ECS Adoption

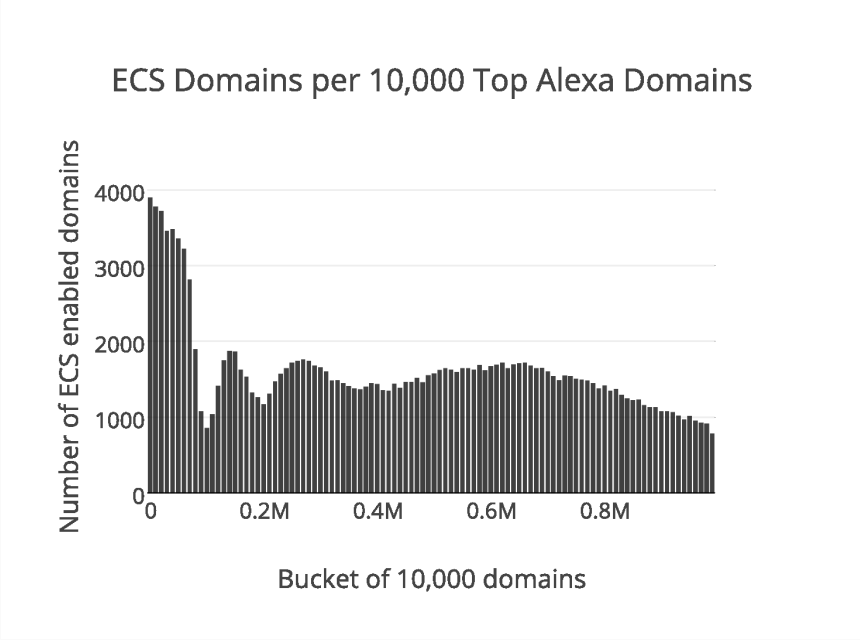


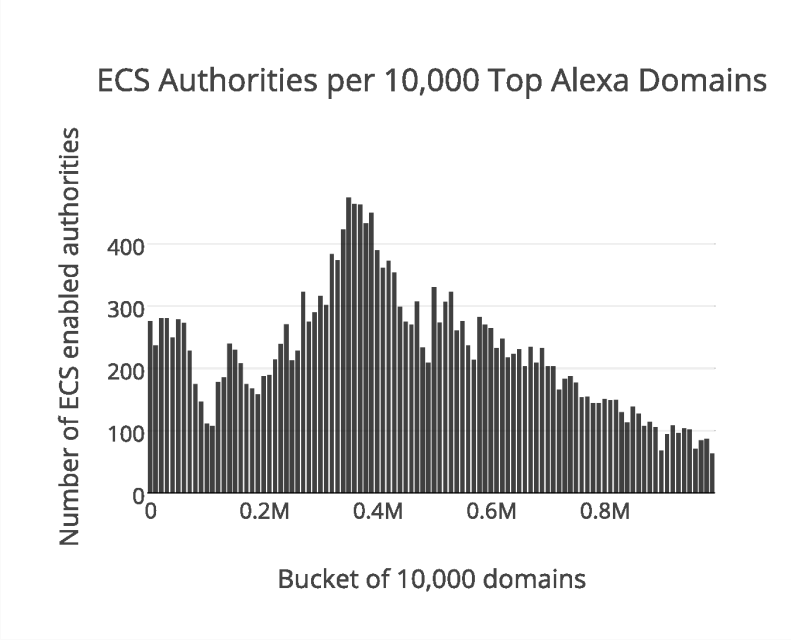


(l) Leak & Torrent queries without ECS

(r) Same, with ECS

ECS Adoption

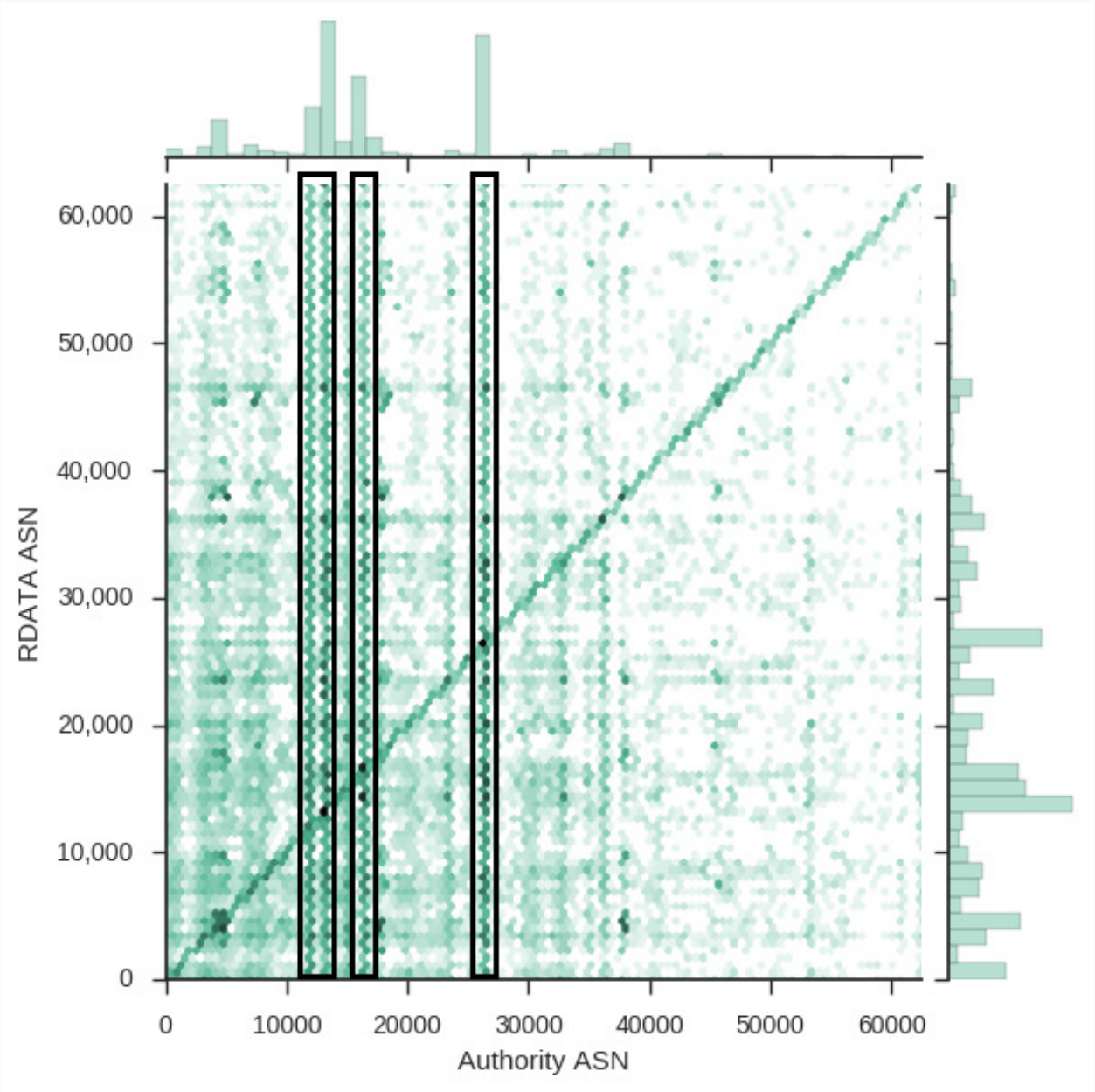




(l) Top 1M Alexa domains, 10K buckets. 189K+ ECS enabled; (r) ECS enabled authorities, from Alexa Top 1M

- Take-away: Even small sites not needing ECS get it anyway. Why?
- Well subscribed secondaries
- A large authority DNS industry spreads ECS to non-CDN zones.

ECS and ASN joint distribution



ECS Implementation Variations

- Google Guidelines [8]
  - Automated whitelisting
- OpenDNS: whitelist by zone (wildcarding allowed) [2]
- Stub tools
  - `scope=0` tools still lacking
  - "Regrettably, support for the opt-out provisions of this specification are currently limited." – `RFC 7871`, May 2016.
  - Noted exception: `getdns`
  - Mozilla: "`network.trr.disable-ECS` $\rightarrow$ `false`", but inheres DOH

ECS Implementation Concerns

- Earliest concerns: [6]
- Did the IETF process identify and avert expected harm?
  - i2p privacy loss, emergency patch, deprecation of all DNS
- Lessons:
  - **Protocol changes should identify changes in DNS stakeholder roles**. (ISP $\rightarrow$ cloud) upset implicit assumptions in existing code, protocols, and communities.
  - **Testing should be off and on-path.** Drop-in testing of users is necessary but not sufficient. This methodology fails to identify secondary instability caused by *changes in inherent assumptions and equities* of DNS, upon which others have relied, built code, and run communities.
  - **Not all prior reliance is reasonable or warrants continued deference.** For instance: reliance on bugs, protocol quirks, or testing behavior elevated to performance criteria (viz qmail, firefox `ANY?`), `0x20`.

i2p and ECS Privacy Impacts

- What is i2p? Reference: [1]
- Essentials:
  - "outproxy" network, messages sent to cryptographic identifier, not an IP address
    - Sites identified via (quasi) pTLD ".i2p"
    - A few, non-default eepproxy peers permit non-i2p browsing
  - Uses inbound/outbound tunnels
  - Kademlia/DHT table of peers
    - Discovers peer's in/out tunnels
  - Peers keep local netDB
    - Flood fill discovery of new peers
    - **Key**: "Warm" tabled work best

i2p Example

THE TIN HAT

Latest Posts

Is Bitcoin Actually Private?

A primer on privacy and Bitcoin, why it matters for fungibility, and what cryptocurrencies are trying to fix it.

Slantwise Action | How WhatsApp, Signal, and Steemit Are Feeding the Resistance

Can people meaningfully resist surveillance without knowing it?

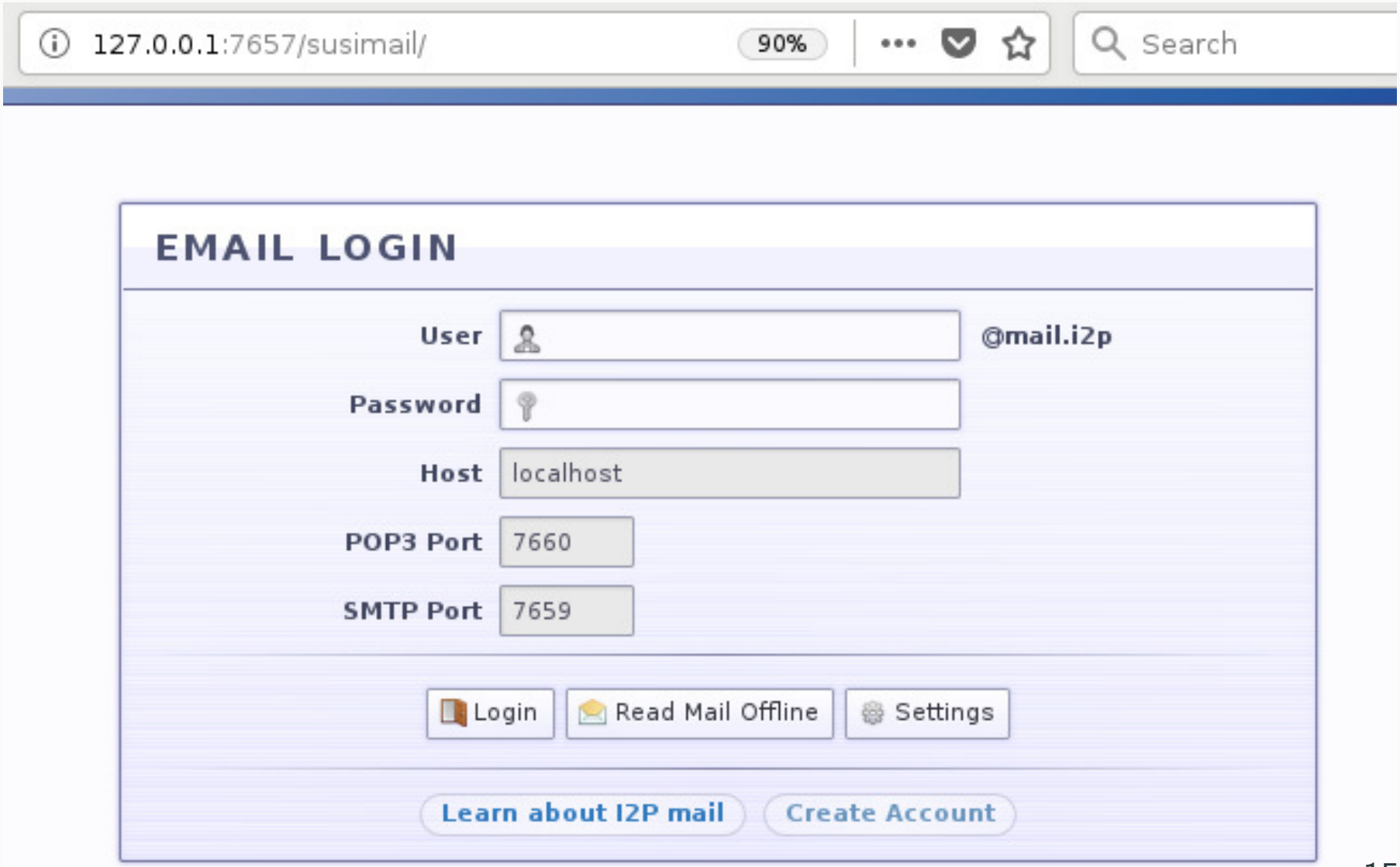
The Internet of Things Isn't Just About Networked Juicers | Privacy, Health, & Technology

The privacy failings of the internet of things get worse when we realize its inevitable health applications

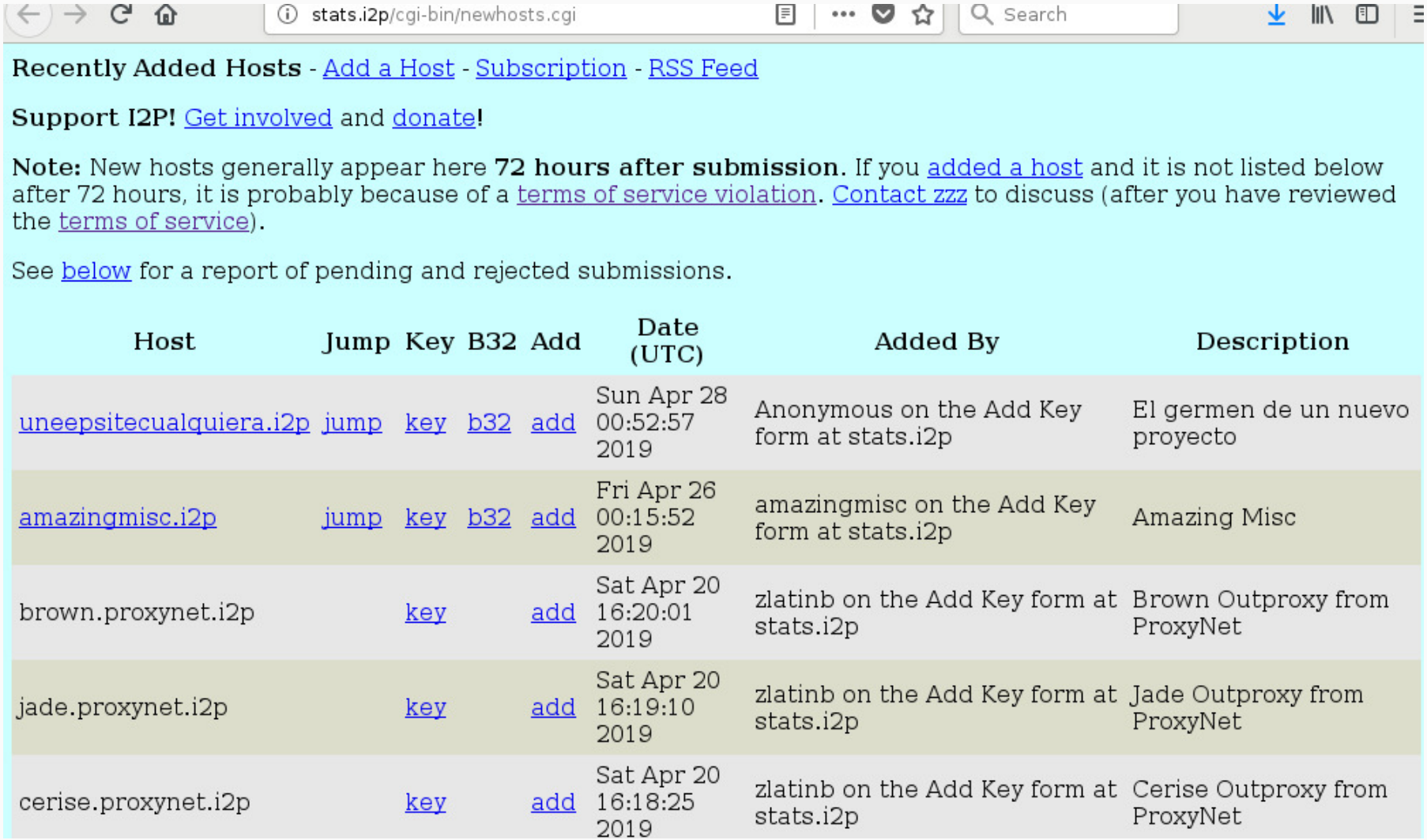
But The Data Says So | Why Data Can't Exist in a Social Vacuum

Some people still don't grasp that data can't be removed from society (and it's racist tendencies)

i2p Example


127.0.0.1:7657/susimail/
90%
Search
EMAIL LOGIN
User
@mail.i2p
Password
Host
localhost
POP3 Port
7660
SMTP Port
7659
Login
Read Mail Offline
Settings
Learn about I2P mail
Create Account

i2p Example



Recently Added Hosts - Add a Host - Subscription - RSS Feed

Support I2P! Get involved and donate!

Note: New hosts generally appear here **72 hours after submission**. If you added a host and it is not listed below after 72 hours, it is probably because of a terms of service violation. Contact zzz to discuss (after you have reviewed the terms of service).

See below for a report of pending and rejected submissions.

Host	Jump	Key	B32	Add	Date (UTC)	Added By	Description
uneepsitecualquiera.i2p	jump	key	b32	add	Sun Apr 28 00:52:57 2019	Anonymous on the Add Key form at stats.i2p	El germen de un nuevo proyecto
amazingmisc.i2p	jump	key	b32	add	Fri Apr 26 00:15:52 2019	amazingmisc on the Add Key form at stats.i2p	Amazing Misc
brown.proxynet.i2p		key		add	Sat Apr 20 16:20:01 2019	zlatinb on the Add Key form at stats.i2p	Brown Outproxy from ProxyNet
jade.proxynet.i2p		key		add	Sat Apr 20 16:19:10 2019	zlatinb on the Add Key form at stats.i2p	Jade Outproxy from ProxyNet
cerise.proxynet.i2p		key		add	Sat Apr 20 16:18:25 2019	zlatinb on the Add Key form at stats.i2p	Cerise Outproxy from ProxyNet

i2p Example

darkness.i2p	jump	key	b32	add	Sun Mar 31 19:38:19 2019	Anonymous on the Add Key form at stats.i2p	
swrd1903.i2p	jump	key	b32	add	Sun Mar 31 10:07:01 2019	Anonymous on the Add Key form at stats.i2p	swwrd1903
freespeech.i2p	jump	key	b32	add	Sat Mar 30 21:32:59 2019	FreeSpeecher on the Add Key form at stats.i2p	Talk about what you want.
latinum.i2p	jump	key	b32	add	Sat Mar 30 18:04:05 2019	Anonymous on the Add Key form at stats.i2p	

Transparency Report

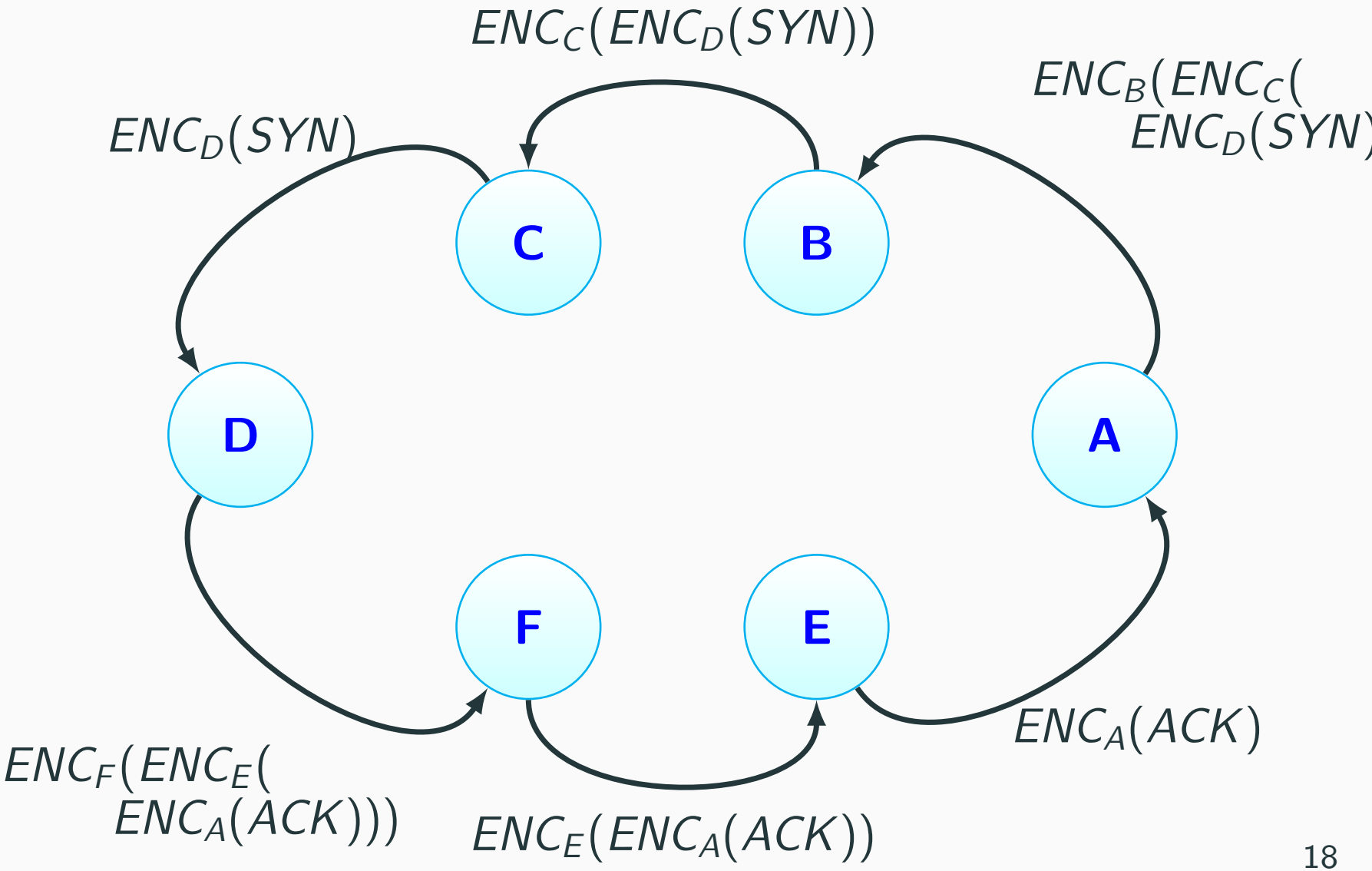
22 hosts submitted in previous 34 days accepted and shown above.

2 hosts hidden: submitted in previous 3 days, or awaiting manual review, or delayed for TOS violations.

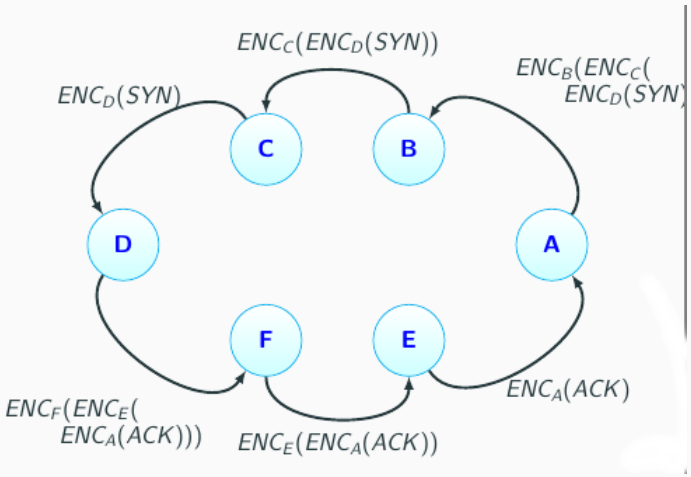
Total hosts rejected for TOS violations:

2019: 1
2018: 8
2017: 36
2016: 38
2015: 32
2014: 58

i2p Conceptual Overview



i2p Conceptual Overview



Key Points

- Separate tunnels for ingress/egress
- `RouterInfo` objects map host keys $\rightarrow$ {ips, domains}
- Variable length, short-lived tunnels

Flood fill

- Efficient discovery of changing paths
- Slow-start period for new/DHCP changes
- DNS **essential** for dynamic hosts

i2p NetDB

Peer info for: -53ZrBvGtVLacaTalqfdAyfMu~KjgO~BvMJLXKkfVEY=

Published: 62 min ago **Signing Key:** EdDSA_SHA512_Ed25519

Addresses:
NTCP: **Host:** 178 **I:** a6wIL027guK2e2xvKmwSuw== **Port:** 24940 **S:** sCdB3ZrcHDuNuJ-KkDqH9Ewypy5UIphnMfXA9rfvNE8= **V:** 2
SSU: **Caps:** BC **Host:** 178 **Key:** -53ZrBvGtVLacaTalqfdAyfMu~KjgO~BvMJLXKkfVEY= **Port:** 24940

Stats:
caps = XfR
netId = 2
netdb.knownLeaseSets = 67
netdb.knownRouters = 3768
router.version = 0.9.39

Peer info for: -fwRgYRbFk6d9QVTWlVWxcdnAw720UrfNgAQEiLpzaw=

Published: 17 min ago **Signing Key:** EdDSA_SHA512_Ed25519

Addresses:
NTCP: **Host:** 78 **Port:** 19251
SSU: **Caps:** BC **Host:** 78 **Key:** -fwRgYRbFk6d9QVTWlVWxcdnAw720UrfNgAQEiLpzaw= **Port:** 19251

Stats:
caps = POfR
netId = 2
netdb.knownLeaseSets = 76
netdb.knownRouters = 3965
router.version = 0.9.25

Peer info for: 0aBSpeQyhwKWxm2YsSuk-pdcVqHDL00I2Vd16KY5CFM=

Published: 97 min ago **Signing Key:** EdDSA_SHA512_Ed25519

Addresses:
NTCP: **Host:** 182 **I:** RTiZSPqvheyMtE7v8Rt~Qw== **Port:** 29021 **S:** cUldN5T5louO8HZ0KI86lbgNmbvexIPORAzNeb7x1wQ= **V:** 2
SSU: **Caps:** BC **Host:** 182. **Key:** 0aBSpeQyhwKWxm2YsSuk-pdcVqHDL00I2Vd16KY5CFM= **Port:** 29021

Stats:
caps = XfR
netId = 2
netdb.knownLeaseSets = 132
netdb.knownRouters = 4257
router.version = 0.9.39

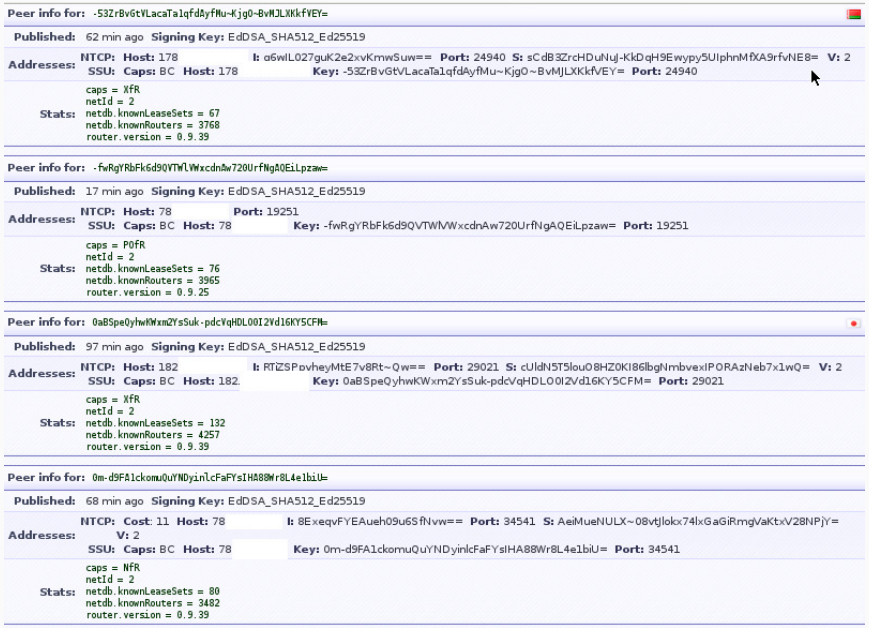
Peer info for: 0m-d9FA1ckomuQuYNDyinlcFaFYsIHA88Wr8L4e1biU=

Published: 68 min ago **Signing Key:** EdDSA_SHA512_Ed25519

Addresses:
NTCP: **Cost:** 11 **Host:** 78 **I:** 8ExeqvFYEAueh09u6SfNvw== **Port:** 34541 **S:** AeiMueNULX~08vtJlokx74lxGaGiRmgVaKtxV28NPjY= **V:** 2
SSU: **Caps:** BC **Host:** 78 **Key:** 0m-d9FA1ckomuQuYNDyinlcFaFYsIHA88Wr8L4e1biU= **Port:** 34541

Stats:
caps = NfR

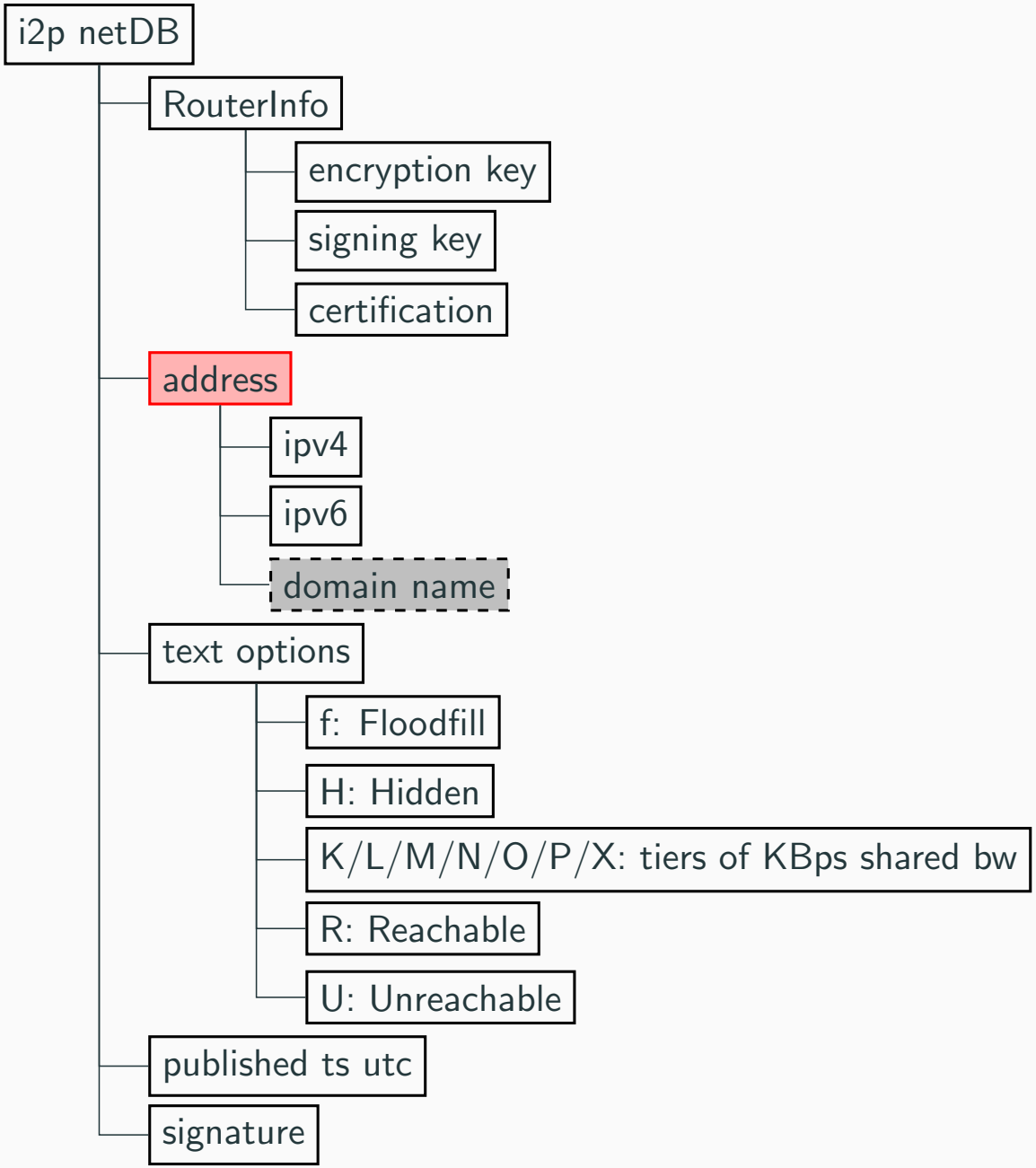
i2p NetDB



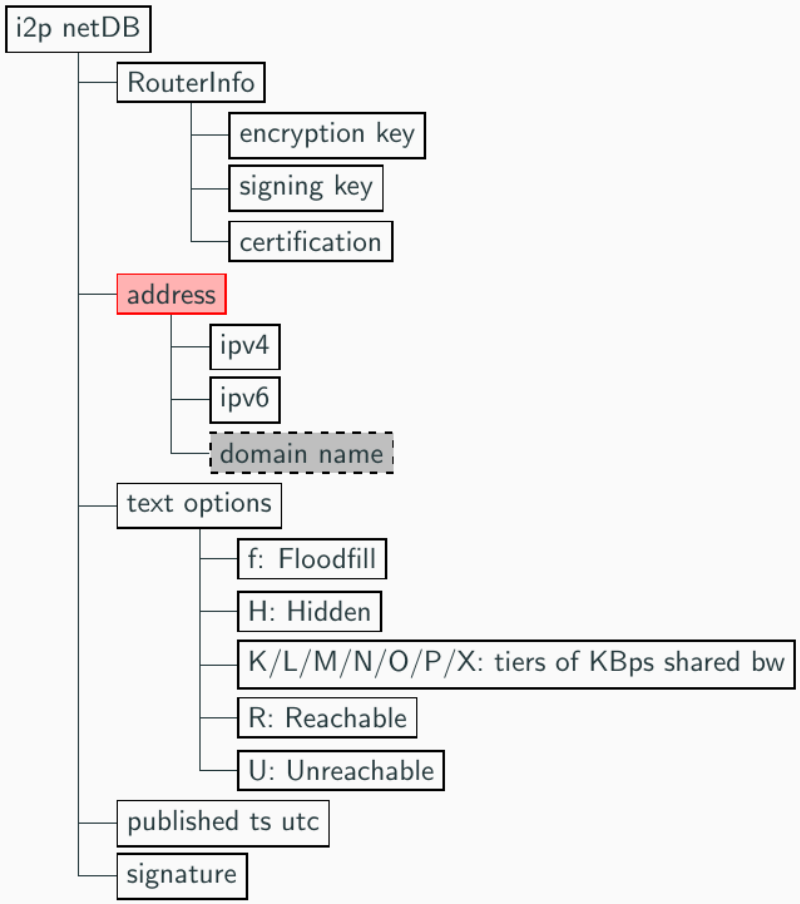
Key Points

- Flood-fill sharing of `RouterInfo` objects
- Tunnels and Lease model, short TTL ($\approx$ 10 min)
- "Warm tables" route better
- Averages peak at $\approx$ 40K users

i2p NetDB Structure



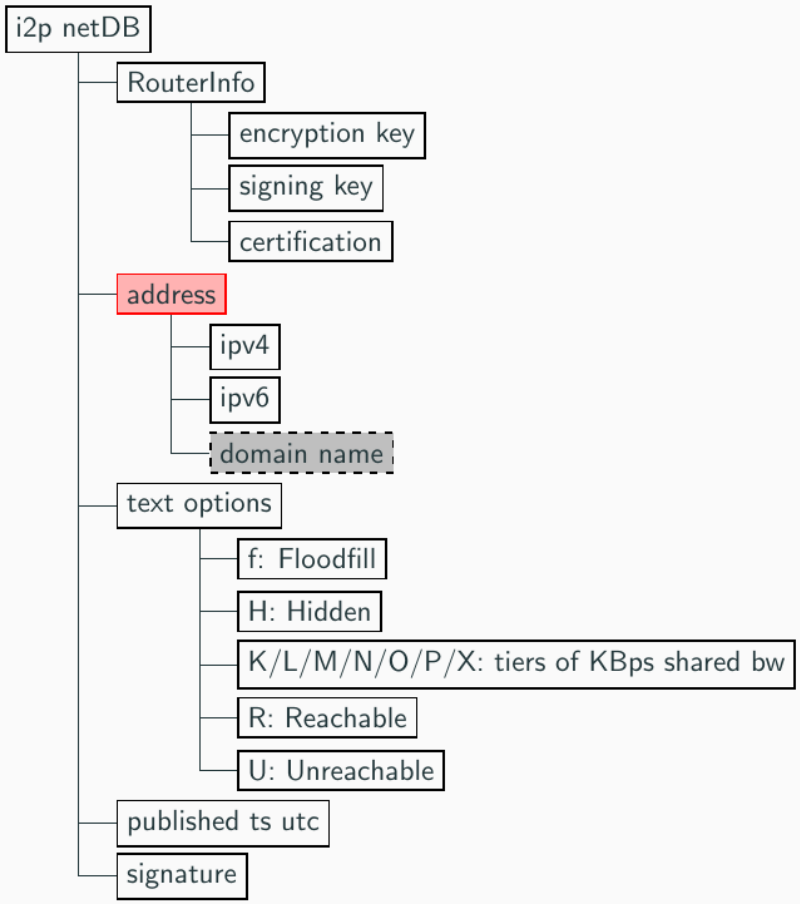
i2p NetDB



Key Points

- i2p-Con panel idea: How to measure size of i2p?
- Create "dye marker" domain in `RouterInfo` (e.g., `$EPOCH.census.example.com`)
- Appropriate low `TTL` ($\approx 10min$) creates census out of authority logs
  - Statistical tools for population estimate
- Nice contrast to Tor Metrics: You don't have to trust the operators

i2p NetDB



Key Points

- Non-intrusive census techniques
- We learn only population, not individuals
- As with modern archaeology, this is often more insightful
- Presumption: k-anonymity analysis not disrupted by technological changes

i2p Attack using EDNS-Client Subnet

Normal FloodFill

$RouterInfo_A$	IP_A
$RouterInfo_B$	IP_B
$RouterInfo_C$	$Domain_C$
...	...

Measurement FloodFill

$RouterInfo_A$	IP_A
$RouterInfo_B$	IP_B
$RouterInfo_D$	$\$COUNTER.example.com$
...	...

Authority logs cannot attribute resolution to specific hosts (haystack) **because of** ISP DNS farms (cf. k-anonymity, e.g., [12]).

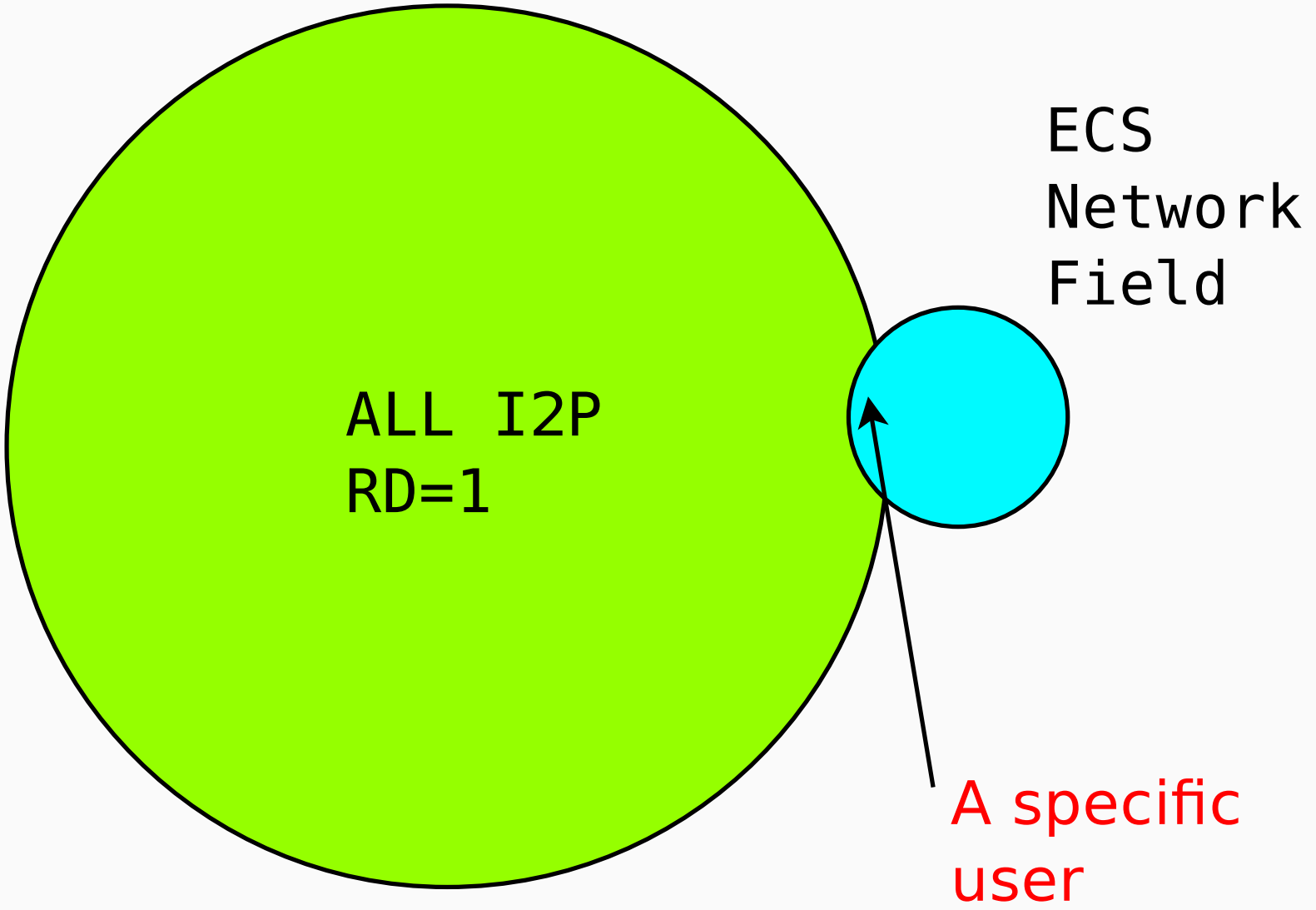
i2p Attack using EDNS-Client Subnet

ECS weaponizes instrumented census flood fill

$RouterInfo_A$	IP_A
$RouterInfo_B$	IP_B
$RouterInfo_D$	$\$COUNTER.example.com$
...	...

- **HOWEVER**, EDNS-Client-Subnet connects queries to **specific** i2p routers
- ECS provides sufficient data to break k-anonymity
- Permits passive, global tracking of route lease creation
- Breaks i2p

i2p and ECS k-anonymity break



i2p Attack Remediation

- Consultation and coordination with i2p operators
- Emergency patch
- "For the router info validation and transport connection code, implementers should ignore router addresses containing hostnames, and use the other published addresses containing IPs, if any. If no addresses in the router info contain IPs, the router should not connect to the published router. In no case should a router do a DNS lookup of a published hostname, either directly or via an underlying library." [13]
- DNS now off-by-default in i2p
- Good news: DNSSEC investigated for supernode bootstrap role

i2p Remediation Plan

For the router info validation and transport connection code, implementers should ignore router addresses containing hostnames, and use the other published addresses containing IPs, if any. If no addresses in the router info contain IPs, the router should not connect to the published router. In no case should a router do a DNS lookup of a published hostname, either directly or via an underlying library.

- Core developers note ECS and "enumeration or attack scenarios"
- Final remediation plan [14]: Deprecate DNS
- Hosts may "opt-in" to DNS (and risk losing anonymity)
- GT has whitelisting algorithm and study

DNS and i2p: Criticisms

- Small community size; smaller developer pool
- Reliance on java/i2p lookup: `java.net.Inet6AddressImpl.lookupAllHostAddr`, often with `ANY`?
  - Possible migration to XBill's `dnsjava` etc
- False assumption: "outproxy" design immunization
- Proponents provide Tor-like view of I2P: `draft-grothoff-iesg-special-use-p2p-i2p-00.txt`
  - `To resolve ‘‘I2P’’ names, the implementation MUST intercept queries for the pTLD to ensure I2P names cannot leak into the DNS.`
- `.i2p` resolution only through local `SusiDNS` (and others).
- Root `.i2p` leaks would be non-routing, non-organic events, since eepnet uses `SusiDNS` (and others) **and** only a few proxies, globally.
  - DITL question: *Any* `.i2p` lookups?

pTLD Motivation

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Leakage of .onion at the DNS Root: Measurements, Causes, and Countermeasures

Aziz Mohaisen, *Senior Member, IEEE, Member, ACM*, and Kui Ren, *Fellow, IEEE, Member, ACM*

***Abstract*—The Tor hidden services, one of the features of the Tor anonymity network, are widely used for providing anonymity to services within the Tor network. Tor uses the .onion pseudo-top-level domain for naming convention and to route requests to these hidden services. The .onion namespace is not delegated to the global domain name system (DNS), and Tor is designed in such a way that all .onion queries are routed within the Tor network. However, and despite the careful design of Tor, numerous .onion requests are still today observed in the global DNS infrastructure, thus calling for further investigation. In this paper, we present the state of .onion requests received at the global DNS and as viewed from two large DNS traces: a continuous period of observation at the A and J DNS root nodes over a longitudinal period of time and a synthesis of Day In The Life of the Internet data repository that gathers a synchronized DNS capture of two days per year over multiple years. We found that .onion leakage in the DNS infrastructure to be both prevalent and persistent. Our characterization of the leakage shows various features, including high volumes of leakage that are diverse, geographically distributed, and targeting various types of hidden services. Furthermore, we found that various spikes in the .onion request volumes can be correlated with various global events, including geopolitical events. We attribute the leakage to various causes that are plausible based on various**

resolved recursively, would require the collaborations of the root of the DNS, the authority server for the top level domain (TLD) of `com`, the authority server for the second level domain (SLD) of `example`, and the authority server of the third level domain `www`. Currently, the root consists of a combination of 13 groups of DNS servers located globally around the world. Each of those servers is named in the form X.root-servers.net, where X is a character in the range of A through M. These roots are responsible for the delegation of top-level-domains (TLDs) such as .com [45].

It is well known within the Internet research and engineering community that many installed systems on the Internet query the DNS root for a wide range of TLDs that are non-delegated and will ultimately result in an error, which is commonly referred to as an NXDomain [57]. Many of these installed systems depend implicitly or explicitly on the indication from the global DNS that the domain name does not exist for their operation. For instance, many internal networks use a domain name suffix list that is not currently delegated in the global DNS, such as .corp and .home [21]. In both of those examples,

pTLD Advocacy and Provable Protections

The Register®
Biting the hand that feeds IT

CENTRE SOFTWARE **SECURITY** DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGE

Security

Monsters defeated in quest to free .onion from clutches of DNS-snooping demons

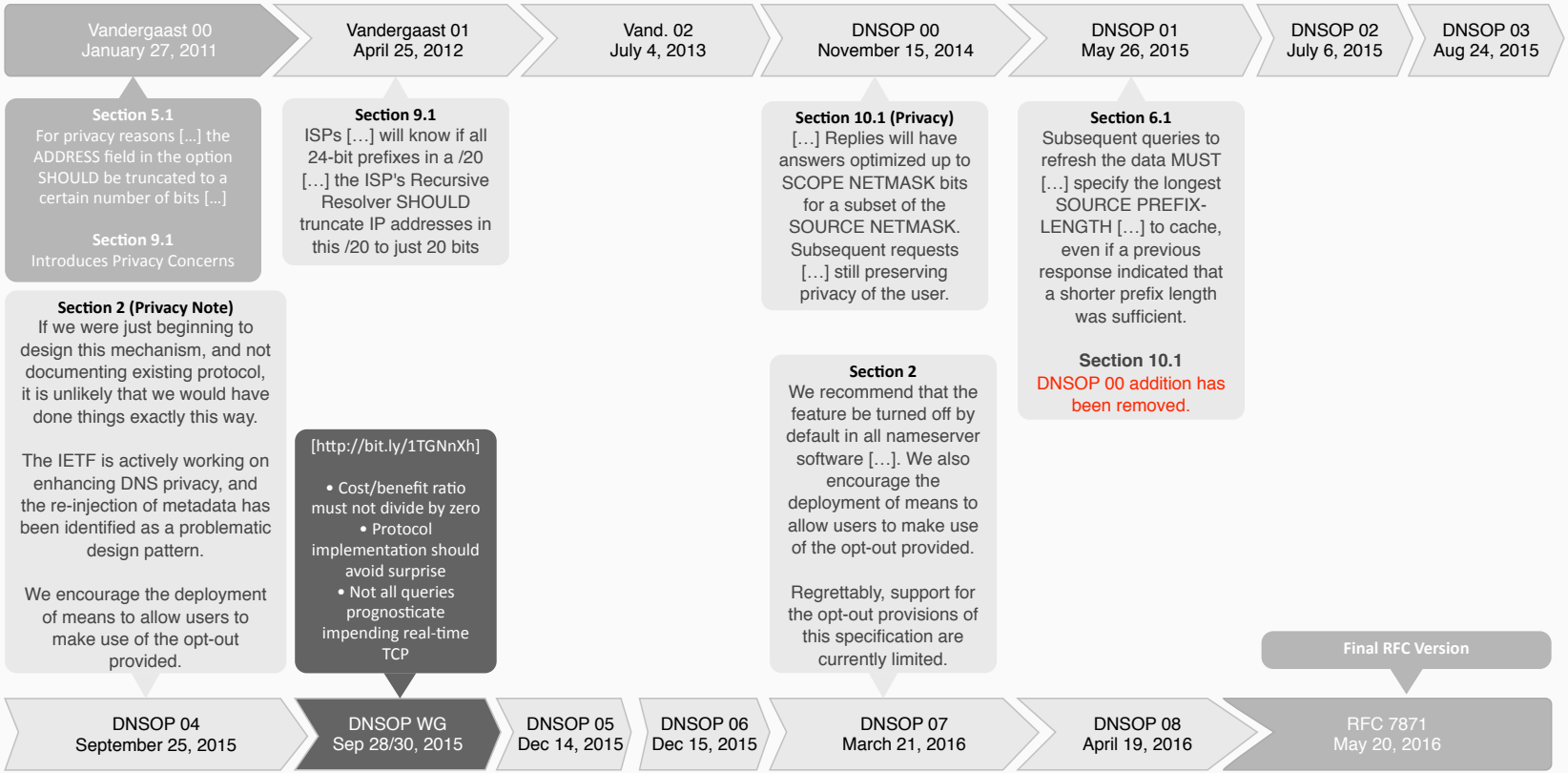
Nice friendly IETF monsters, natch

By Richard Chirgwin 10 Sep 2015 at 03:30 3 SHARE ▼

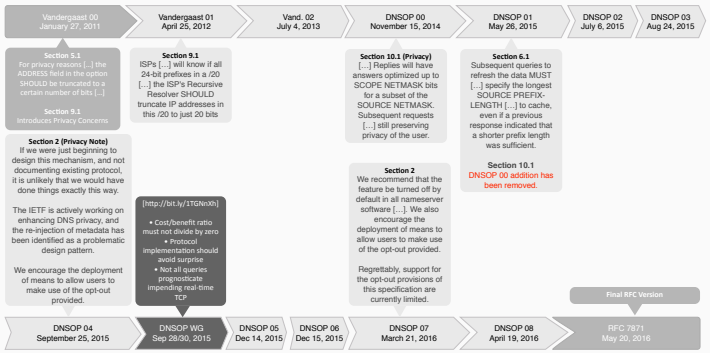
Big steps were taken this week to get The Onion Router (Tor) project's .onion names out of DNS – and away from prying eyes.

Source: [3]

How Was This Missed?



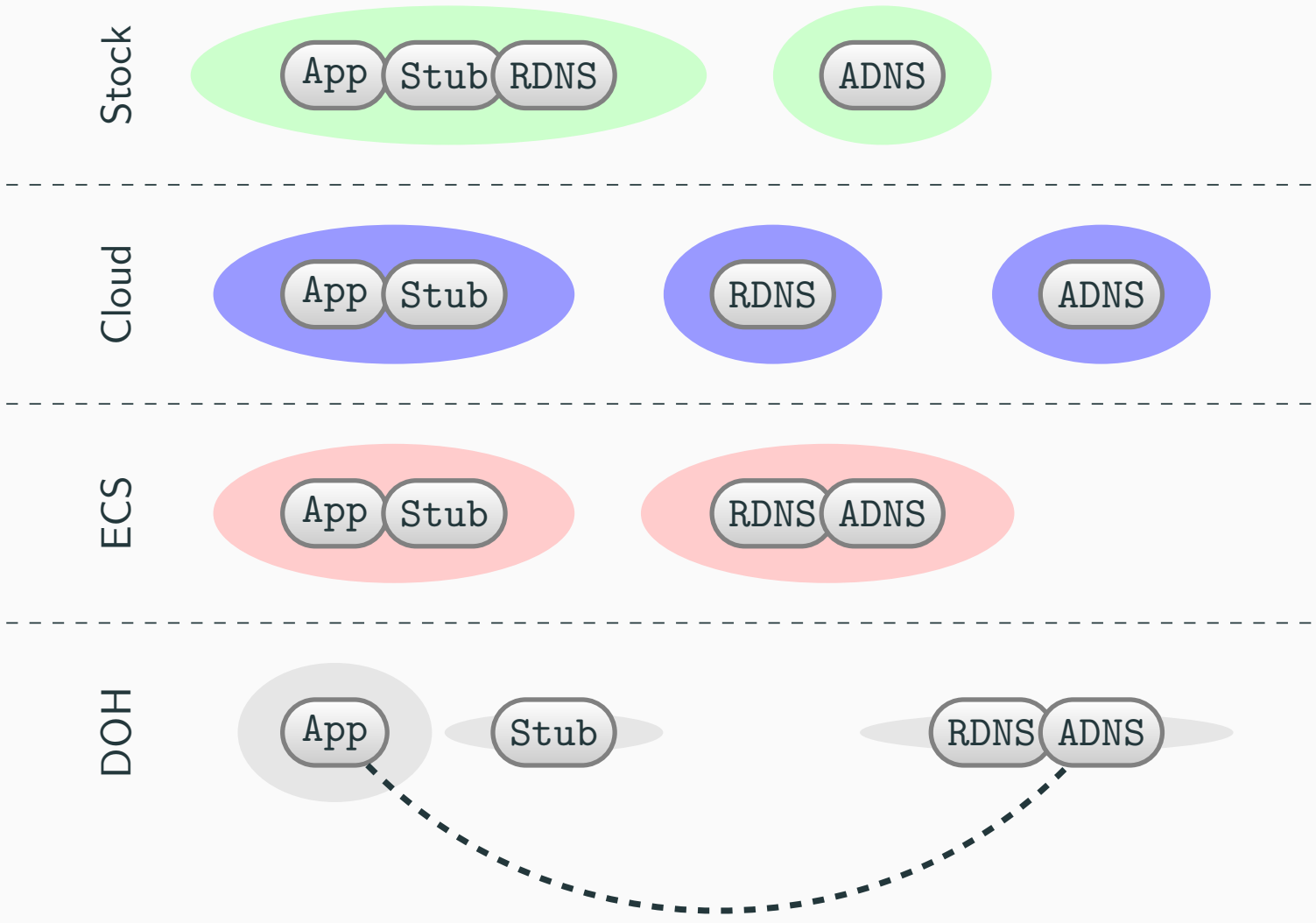
Surprises in Rapid Protocol



Key Points

- Earliest concerns in Frank Denis' blog, 2013: [6] `https://00f.net/2013/08/07/edns-client-subnet`
- Did the IETF process identify and avert expected harm?
  - i2p privacy loss, emergency patch, deprecation of all DNS
- Lesson: Changes in DNS stakeholder roles and information (ISP $\rightarrow$ cloud) upset implicit assumptions in existing code, protocols, and communities.

DNS Stakeholders and Cladistics



Other ECS uses

- DNS significantly improved i2p
  - Needed for for DHCP/mobile users
- ECS changed the fundamental risk profile of DNS.
  - It breaks i2p privacy
- RFC 7258: "In all cases, there will remain some privacy-relevant information that is inevitably disclosed by protocols. As technology advances, techniques that were once only available to extremely well-funded actors become more widely accessible." [9]
- RFC 6973: "Correlation is closely related to identification. Internet protocols can facilitate correlation by allowing individuals' activities to be tracked and combined over time. The use of persistent or infrequently replaced identifiers at any layer of the stack can facilitate correlation" [5]

ECS Leak Magnification

unbound.conf

```
remote-control:
  #control-cert-file: "/etc/unbound/local/unbound_control.pem"
  control-enable: yes
  control-interface: 127.0.0.1
  #control-key-file: "/etc/unbound/local/unbound_control.key"
  control-port: 8953
  #server-cert-file: "/etc/unbound/local/unbound_server.pem"
  #server-key-file: "/etc/unbound/local/unbound_server.key"
  control-use-cert: no

server:
  qname-minimisation: no
  log-servfail: yes
  username: chantra
  do-not-query-localhost: no
  access-control: ::/0 allow
  chroot: ""
  directory: /home/chantra
  cache-min-ttl: 0
  extended-statistics: yes
  hide-identity: yes
  hide-version: yes
  infra-cache-numhosts: 1000000
  infra-cache-slabs: 16
  local-zone: "10.in-addr.arpa." nodefault
  local-zone: "16.172.in-addr.arpa." nodefault
  local-zone: "17.172.in-addr.arpa." nodefault
  local-zone: "18.172.in-addr.arpa." nodefault
  local-zone: "19.172.in-addr.arpa." nodefault
  local-zone: "20.172.in-addr.arpa." nodefault
  local-zone: "21.172.in-addr.arpa." nodefault
  local-zone: "22.172.in-addr.arpa." nodefault
  local-zone: "23.172.in-addr.arpa." nodefault
  local-zone: "24.172.in-addr.arpa." nodefault
  local-zone: "25.172.in-addr.arpa." nodefault
  local-zone: "26.172.in-addr.arpa." nodefault
  local-zone: "27.172.in-addr.arpa." nodefault
  local-zone: "28.172.in-addr.arpa." nodefault
  local-zone: "29.172.in-addr.arpa." nodefault
  local-zone: "30.172.in-addr.arpa." nodefault
  local-zone: "31.172.in-addr.arpa." nodefault
  local-zone: "168.192.in-addr.arpa." nodefault
  max-client-subnet-ipv4: 32
  max-client-subnet-ipv6: 128
  module-config: "subnetcache validator iterator"
  msg-cache-slabs: 16
```

ECS Leak Magnification

unbound.conf

```
remote-control:
  #control-cert-file: "/etc/unbound/local/unbound_control.pem"
  control-enable: yes
  control-interface: 127.0.0.1
  #control-key-file: "/etc/unbound/local/unbound_control.key"
  control-port: 8953
  #server-cert-file: "/etc/unbound/local/unbound_server.pem"
  #server-key-file: "/etc/unbound/local/unbound_server.key"
  control-use-cert: no

server:
  qname-minimisation: no
  log-servfail: yes
  username: chantra
  do-not-query-localhost: no
  access-control: ::/0 allow
  chroot: ""
  directory: /home/chantra
  cache-min-ttl: 0
  extended-statistics: yes
  hide-identity: yes
  hide-version: yes
  infra-cache-numhosts: 1000000
  infra-cache-slabs: 16
  local-zone: "10.in-addr.arpa." nodefault
  local-zone: "16.172.in-addr.arpa." nodefault
  local-zone: "17.172.in-addr.arpa." nodefault
  local-zone: "18.172.in-addr.arpa." nodefault
  local-zone: "19.172.in-addr.arpa." nodefault
  local-zone: "20.172.in-addr.arpa." nodefault
  local-zone: "21.172.in-addr.arpa." nodefault
  local-zone: "22.172.in-addr.arpa." nodefault
  local-zone: "23.172.in-addr.arpa." nodefault
  local-zone: "24.172.in-addr.arpa." nodefault
  local-zone: "25.172.in-addr.arpa." nodefault
  local-zone: "26.172.in-addr.arpa." nodefault
  local-zone: "27.172.in-addr.arpa." nodefault
  local-zone: "28.172.in-addr.arpa." nodefault
  local-zone: "29.172.in-addr.arpa." nodefault
  local-zone: "30.172.in-addr.arpa." nodefault
  local-zone: "31.172.in-addr.arpa." nodefault
  local-zone: "168.192.in-addr.arpa." nodefault
  max-client-subnet-ipv4: 32
  max-client-subnet-ipv6: 128
  module-config: "subnetcache validator iterator"
  msg-cache-slabs: 16
  num-queries-per-thread: 8192
  outgoing-range: 8192
  #pidfile: "/var/run/unbound-local.pid"
```

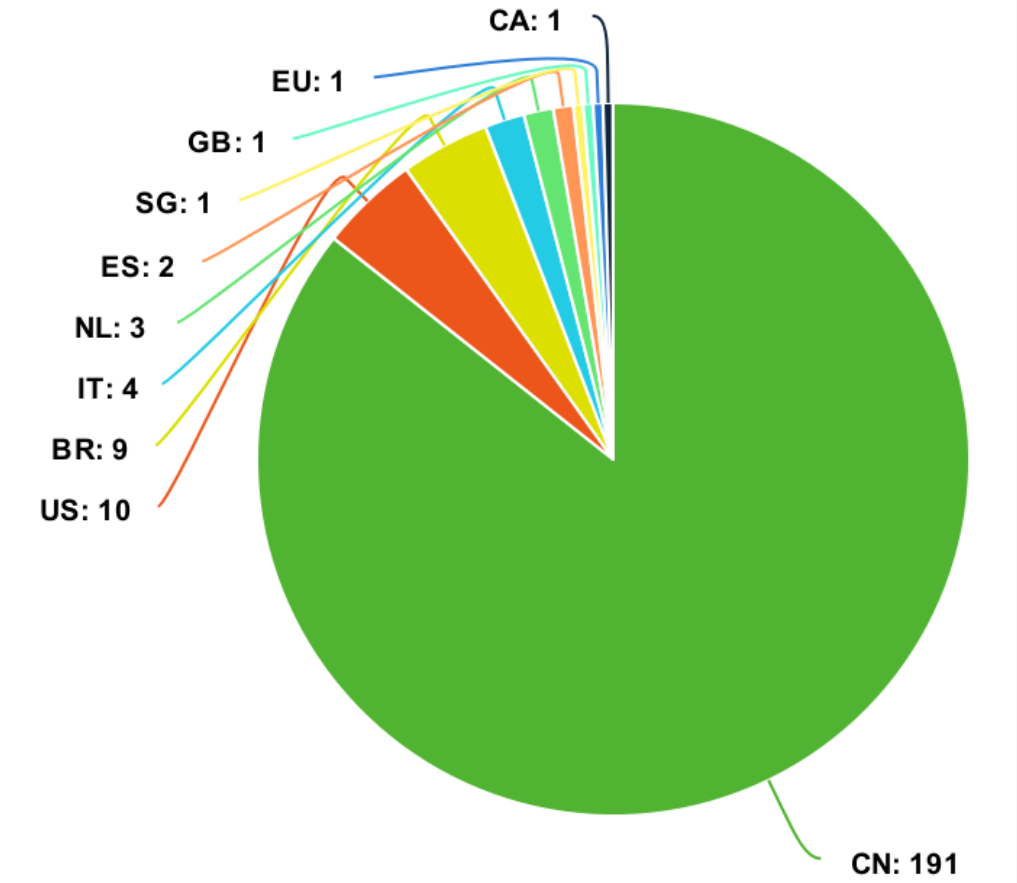
Random Unbound config research result

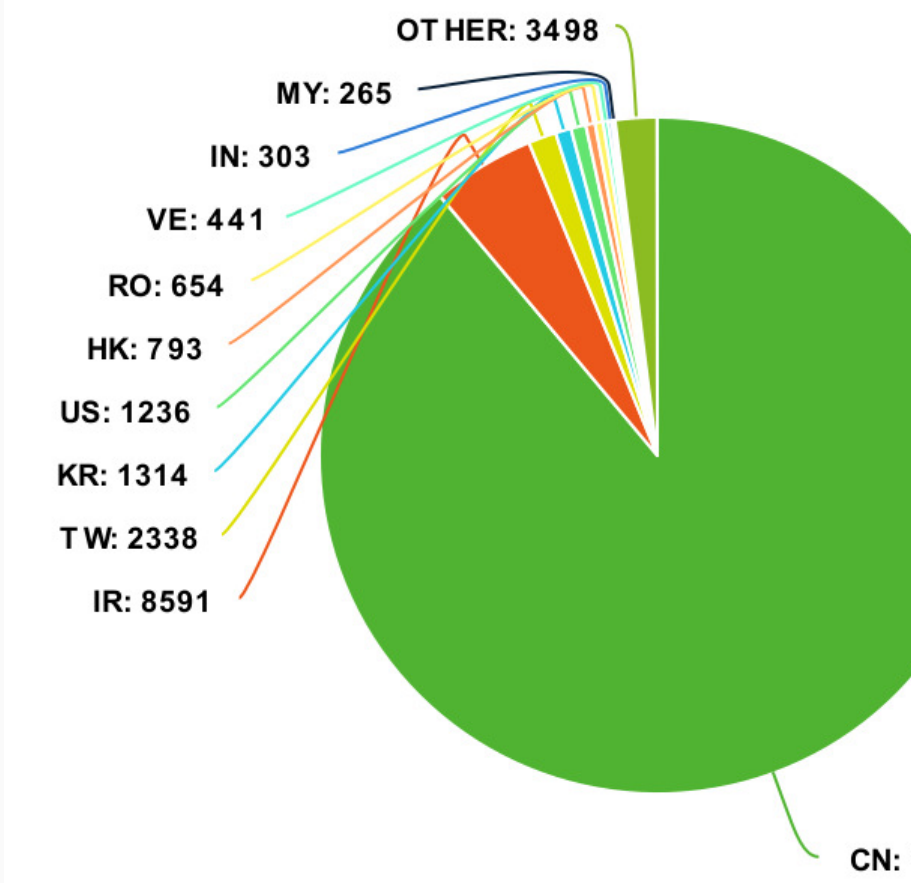
- Advisory values:
- `max-client-subnet-ipv4: 32`
- `max-client-subnet-ipv6: 128`
- `https://gist.github.com/chantra/3cd7d629b16fdd113c3b83239059e74e`

ECS Mask32

- Data: `edns-client-sub.net` (testing), sinkholes, ads, open recursive/forwarding scan
- Numerous hosts (approx 175,000 instances across 200+ hosts) setting family=1, mask=32, and providing 4 octets in network field
  - Started with 2-3 (experimental?) hosts in CN university and ISP
- Major categories
  1. "dot 1" cohort: Mask32 hosts with OPT `network` field portion ends in `.1`
  2. Random network (leak)
  3. Research query (e.g., consistent network of 1.1.1.1 or RFC1918 addr)

ECS Mask32 Resolver Locations

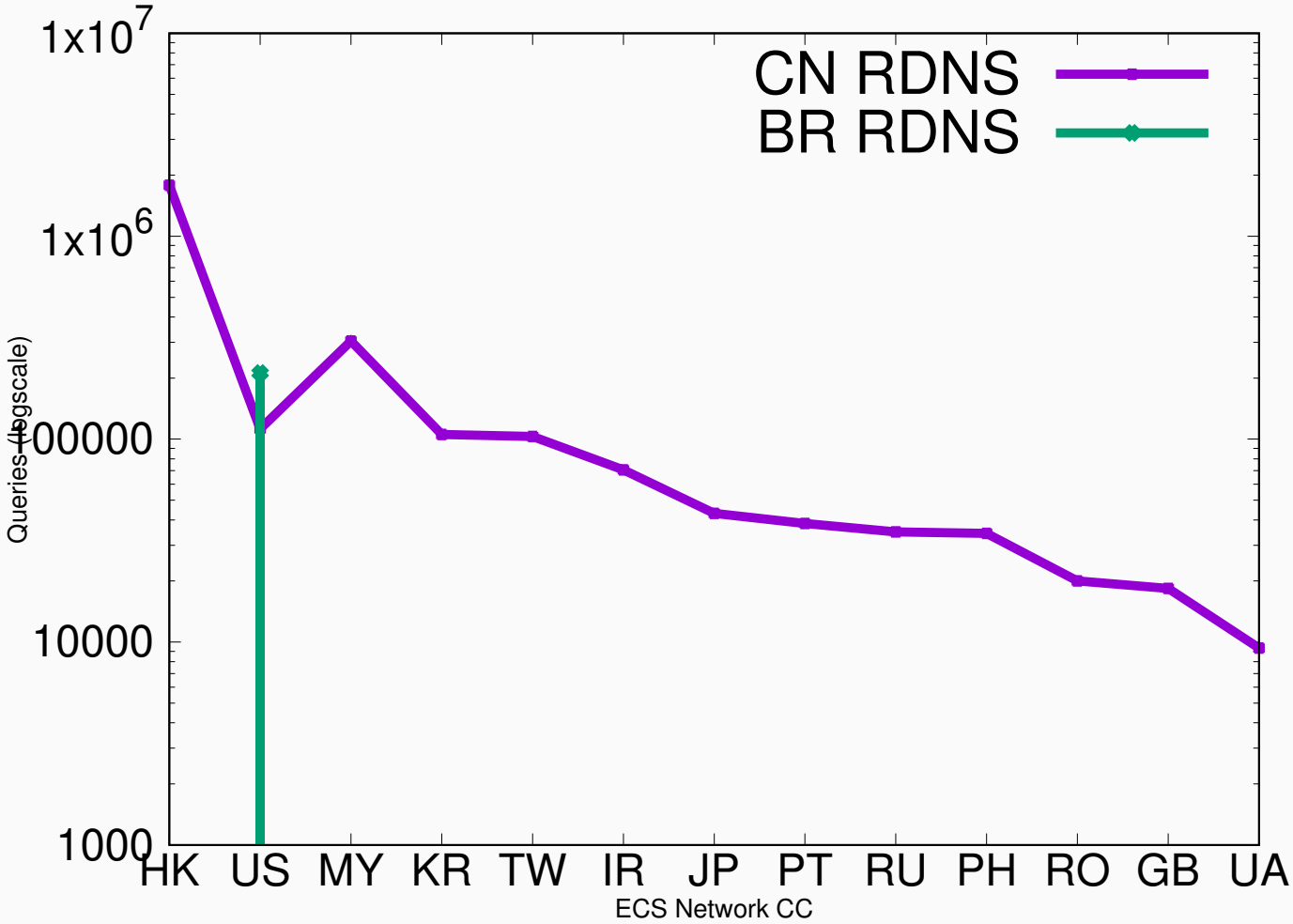




(l) 122 Mask32 RDNS in University, ISP, and VPS/Colo provider networks

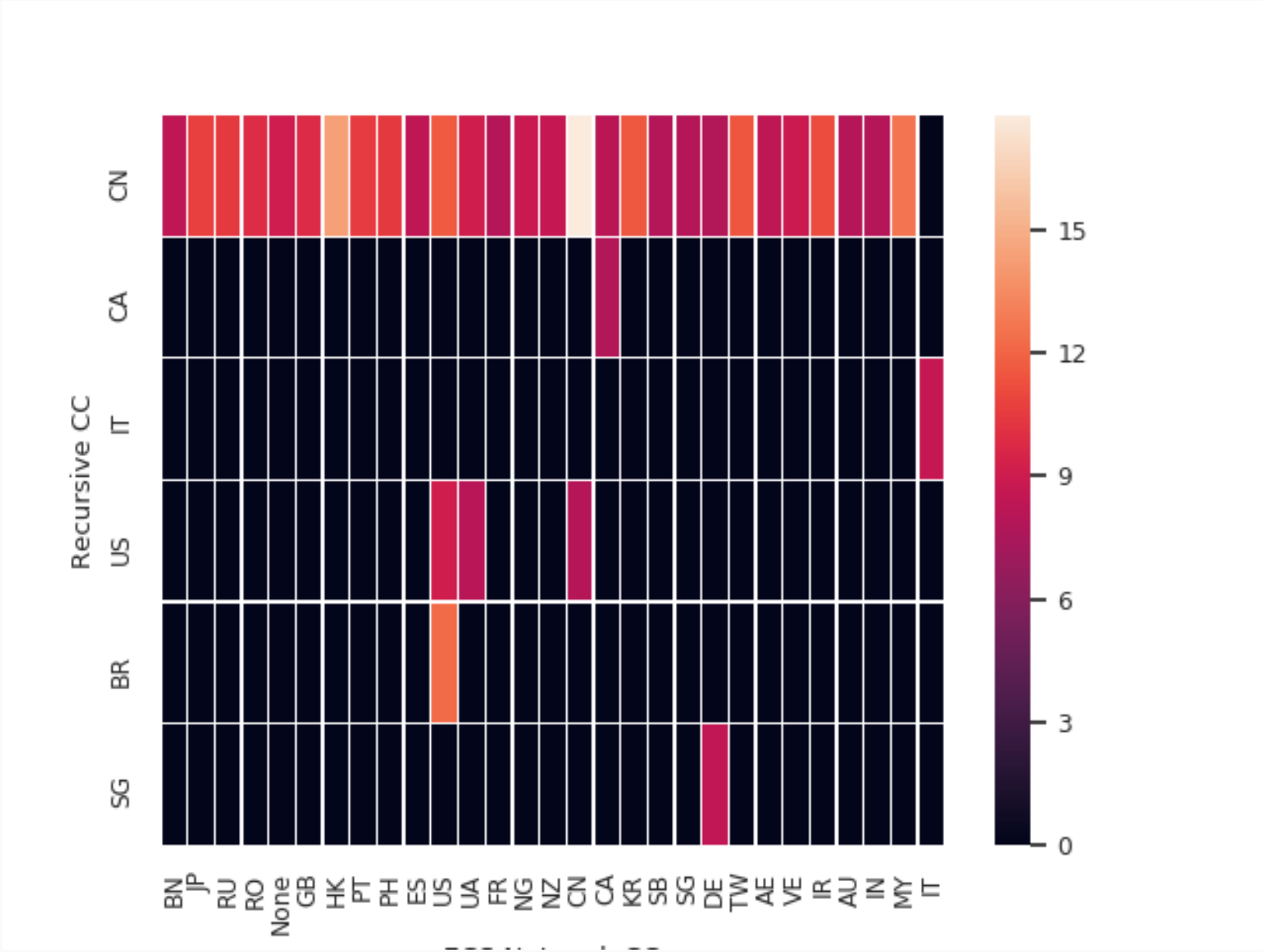
(r) Network field: 136 countries served

ECS Mask32, non-Native Resolutions

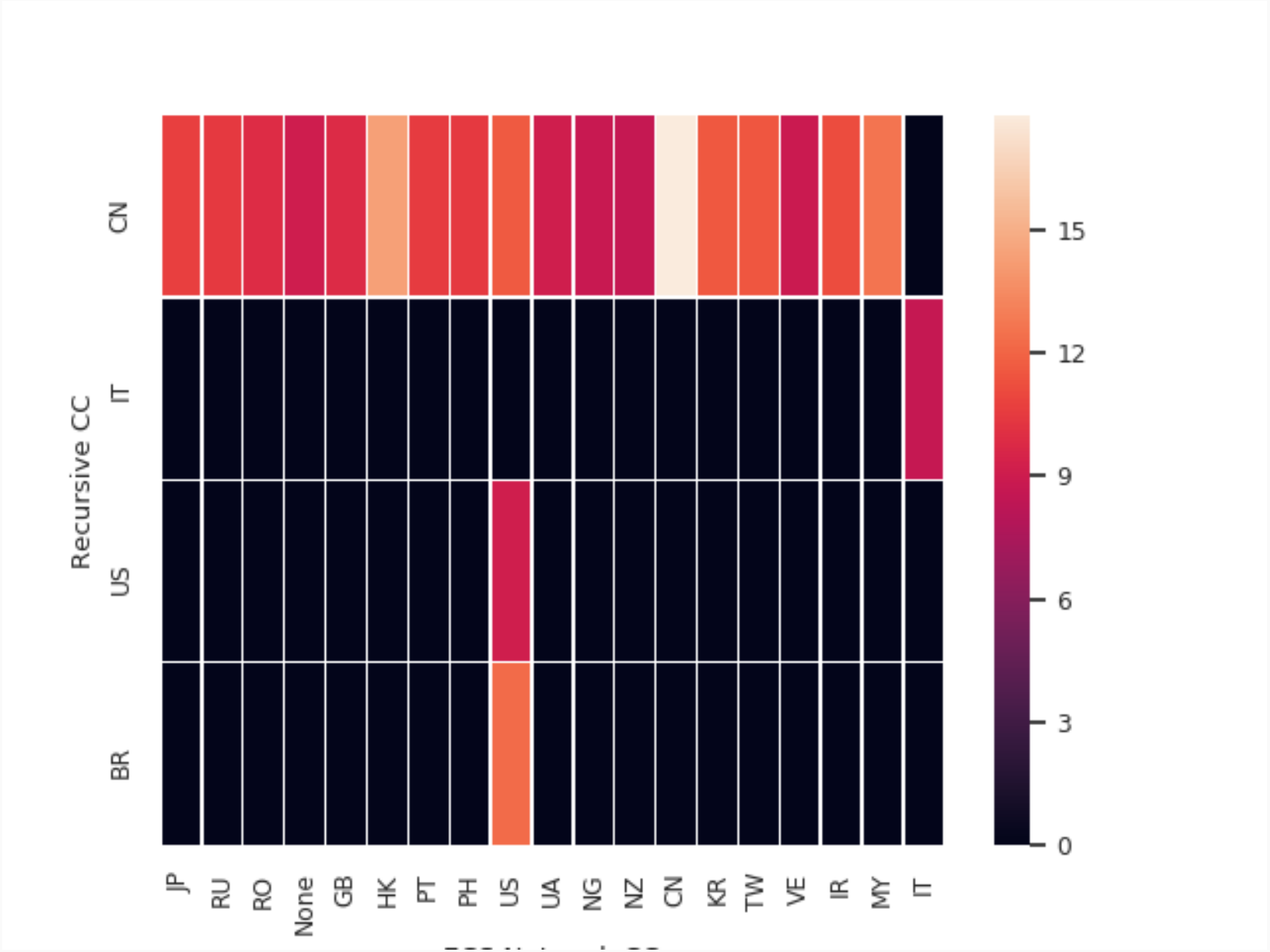


For non-native resolution, CN and BR RDNS, and corresponding ECS network field geolocation.

ECS Mask32 RDNS/Network Heatmap



ECS Mask32 RDNS/Network Heatmap (5k cut)

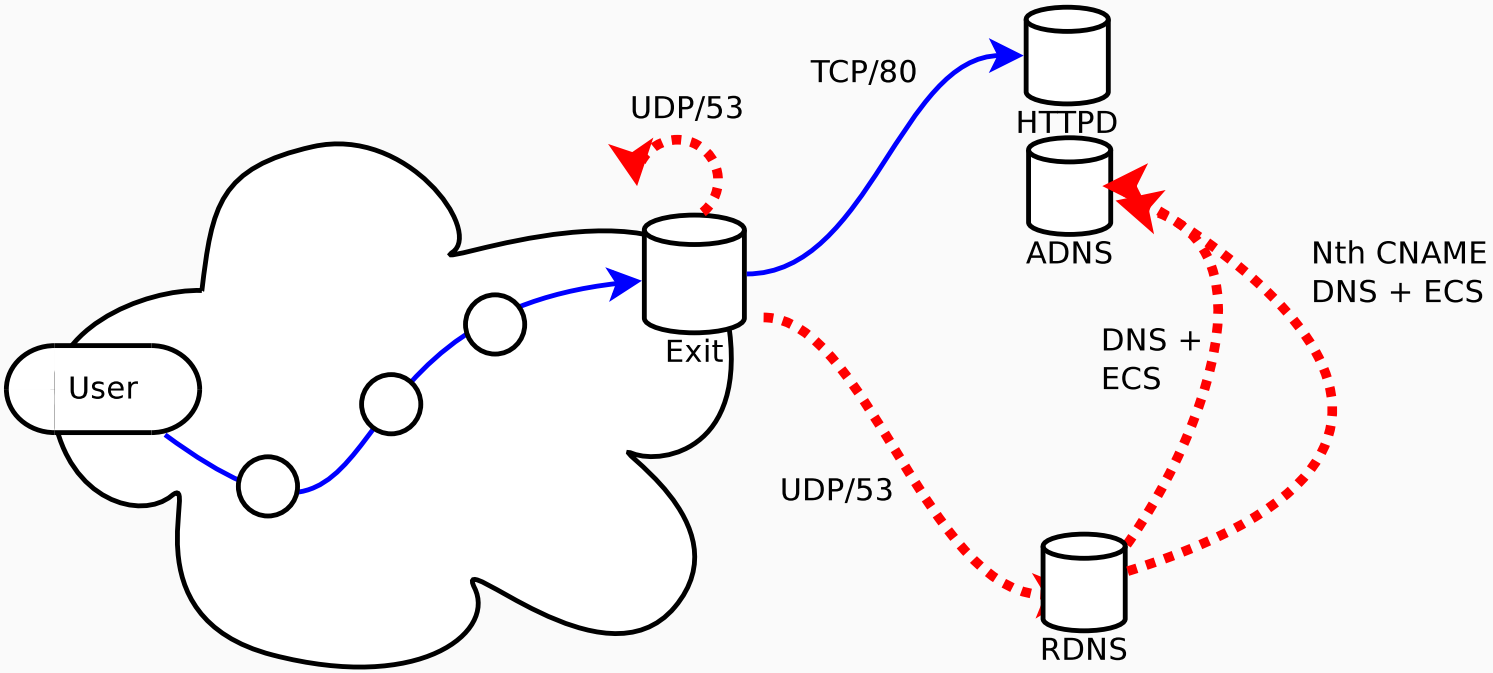


ECS Mask32 Network Prefix Whois

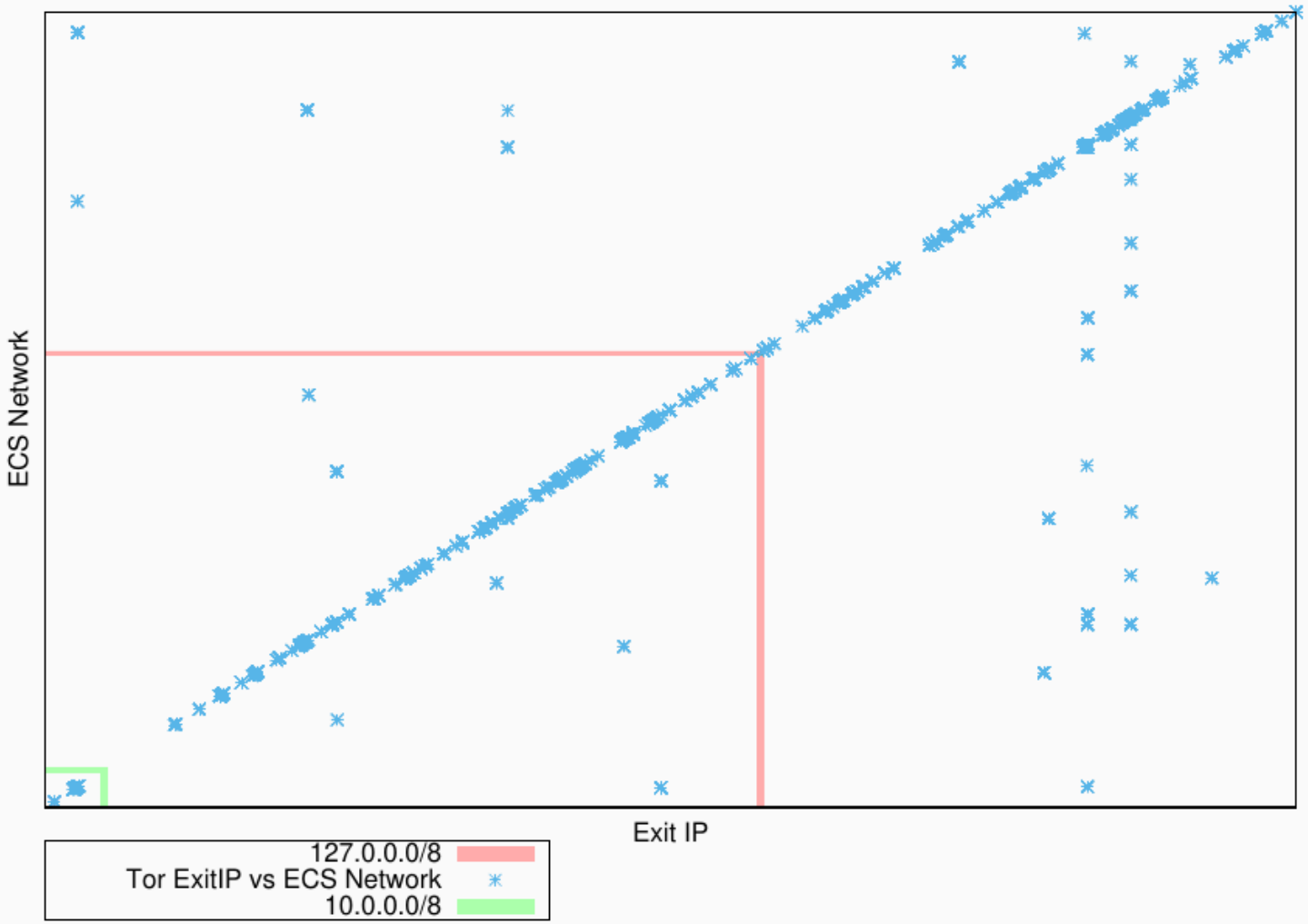
931927	202.165.120.0/22	HK	POWERLINE-AS-AP POWER LINE DATACENTER, HK
345398	112.120.32.0/19	HK	HKTIMS-AP HKT Limited, HK
121486	203.106.192.0/19	MY	TMNET-AS-AP TM Net, Internet Servi
72827	159.138.16.0/22	SG	HWCLOUDS-AS-AP HUAWEI CLOUDS, HK
64747	183.178.0.0/18	HK	HKBN-AS-AP Hong Kong Broadband Net
61724	40.4.0.0/14	US	LILLY-AS - Eli Lilly and Company,
54045	42.200.224.0/19	HK	HKTIMS-AP HKT Limited, HK
47810	67.21.72.0/24	US	ST-BGP - Sharktech, US
45143	219.76.224.0/19	HK	HKTIMS-AP HKT Limited, HK
44023	124.13.0.0/18	MY	TMNET-AS-AP TM Net, Internet Servi
37977	93.108.0.0/16	PT	VODAFONE-PT Vodafone Portugal, PT
33987	175.139.192.0/18	MY	TMNET-AS-AP TM Net, Internet Servi
33638	59.148.128.0/18	HK	HKBN-AS-AP Hong Kong Broadband Net

- Counts and prefix whois for the `network` fields in ECS packets
- Alienated from the recursive's country code
- `family=1, mask=32`
- Resolution context: year+ of network testing, malware, spam delivery

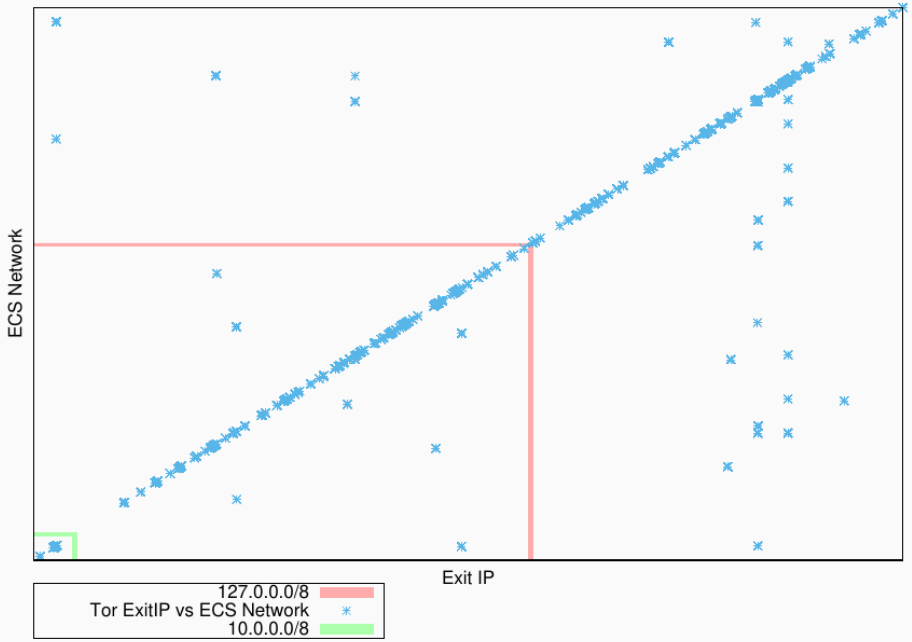
ECS and Tor Data

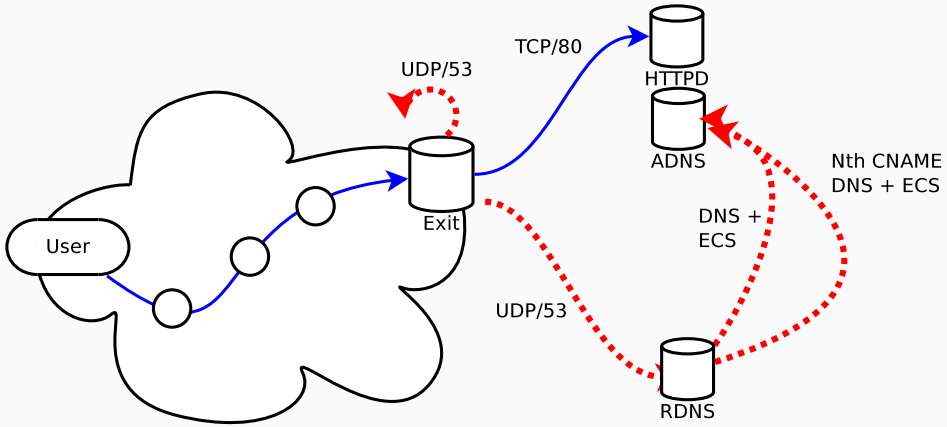


ECS and Tor


ECS Network
Exit IP
127.0.0.0/8
Tor ExitIP vs ECS Network
10.0.0.0/8

ECS and Tor

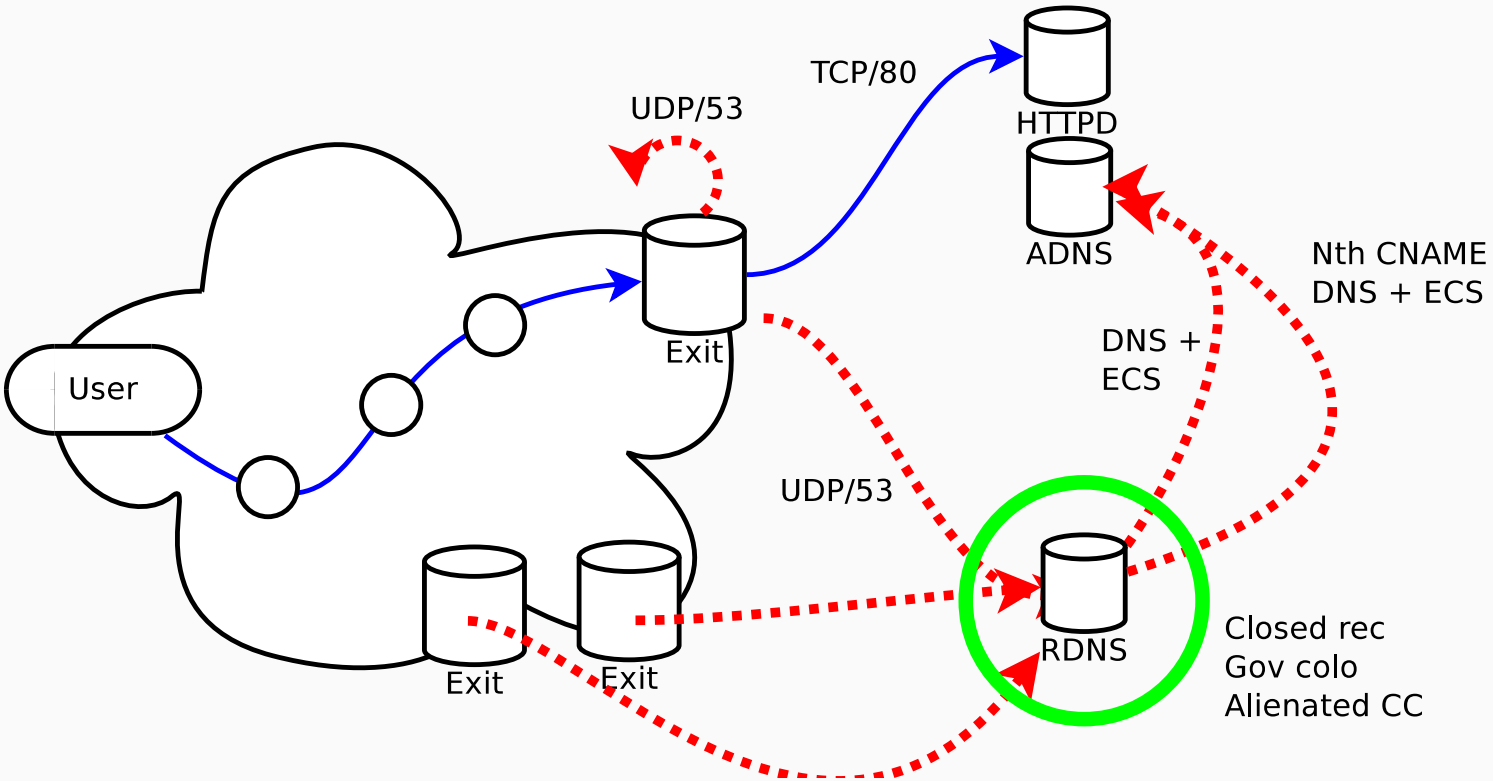




Ideal Tor Network: Exit nodes perform local recursion with cloud backup. Exit nodes set scope 0.

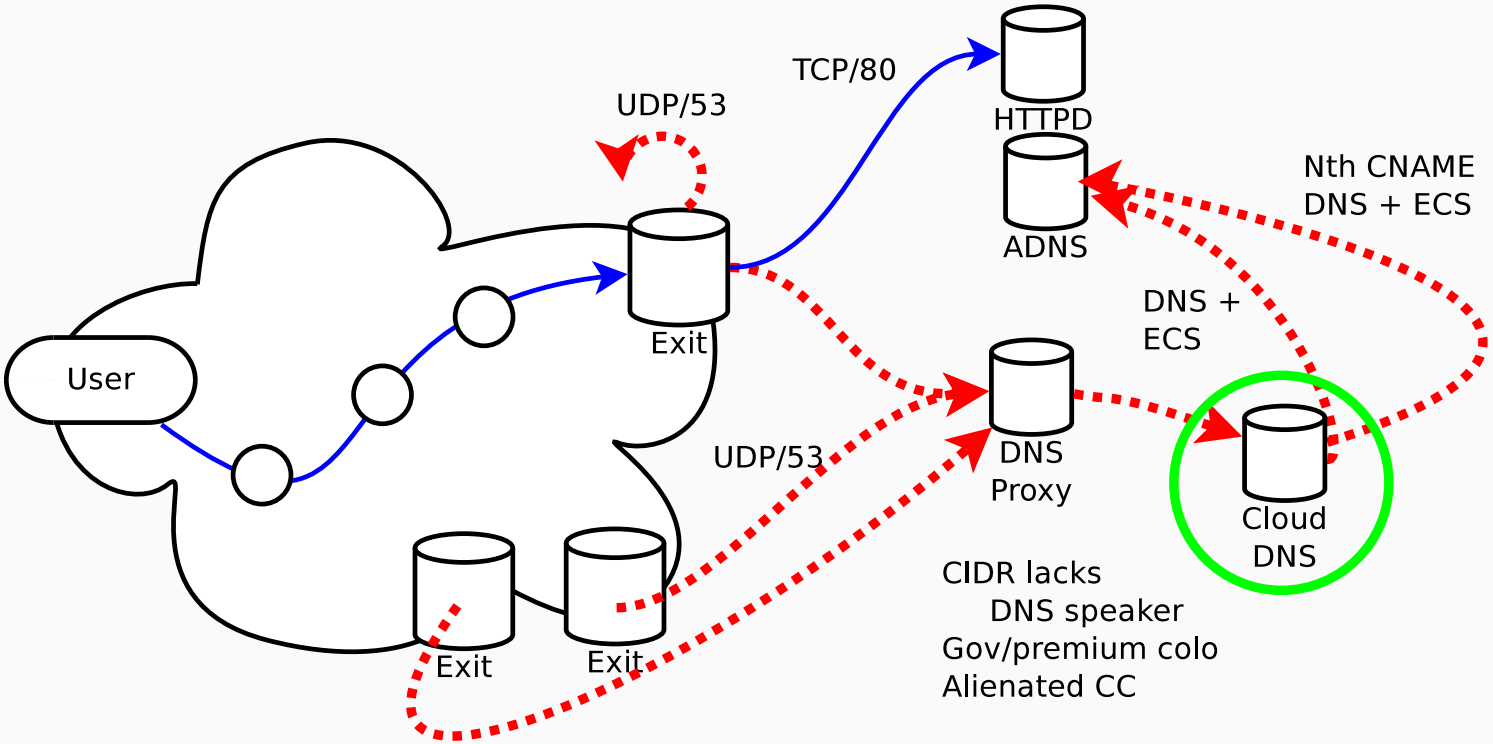
Observed Tor Network: DNS alienation. Exit node alliances inferred from closed rec cluster. *Possible shenanigans*.

ECS-generated Tor graph



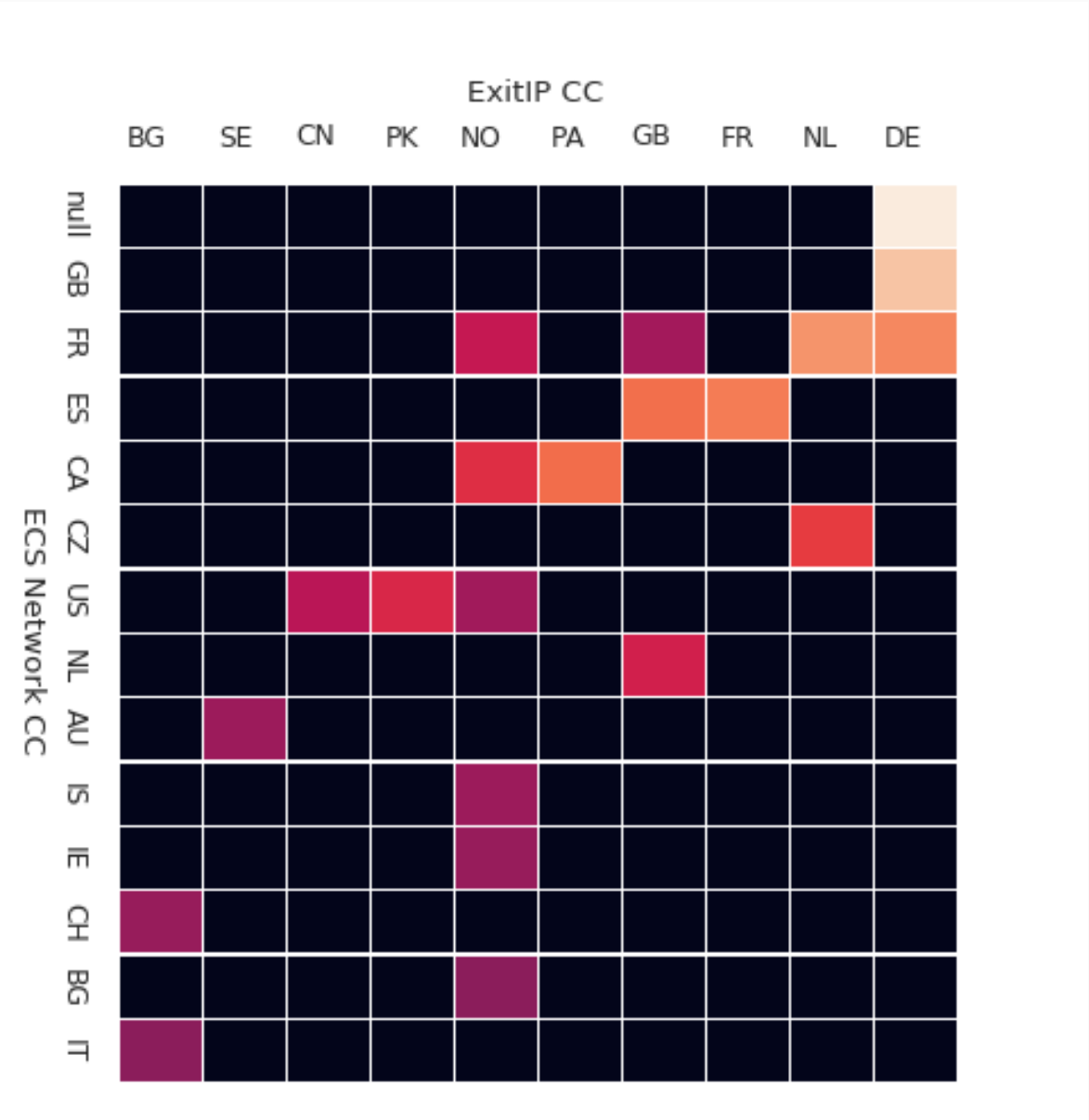
Exporting DNS

ECS Illumination of Tor DNS Forwarder/Proxy



Uhhh...

ECS and Tor: Alienated Queries



Tor and DNS

The Effect of DNS on Tor's Anonymity

Benjamin Greschbach* Tobias Pulls* Laura M. Roberts* Philipp Winter* Nick Feamster
KTH Royal Institute of Technology *Karlstad University* *Princeton University* *Princeton University* *Princeton University*

8187v2 [cs.CR] 11 Oct 2016

***Abstract*—Previous attacks that link the sender and receiver of traffic in the Tor network ("correlation attacks") have generally relied on analyzing traffic from TCP connections. The TCP connections of a typical client application, however, are often accompanied by DNS requests and responses. This additional traffic presents more opportunities for correlation attacks. This paper quantifies how DNS traffic can make Tor users more vulnerable to correlation attacks. We investigate how incorporating DNS traffic can make existing correlation attacks more powerful and how DNS lookups can leak information to third parties about anonymous communication. We (*i*) develop a method to identify the DNS resolvers of Tor exit relays; (*ii*) develop a new set of correlation attacks (DefecTor attacks) that incorporate DNS traffic to improve precision; (*iii*) analyze the Internet-scale effects of these new attacks on Tor users; and (*iv*) develop improved methods to evaluate correlation attacks. First, we find that there exist adversaries who can mount DefecTor attacks: for example, Google's DNS resolver observes almost 40% of all DNS requests exiting the Tor network. We also find that DNS requests often traverse ASes that the corresponding TCP connections do not transit, enabling additional ASes to gain information about Tor users' traffic. We then show that an adversary who can mount a DefecTor attack can often determine the website that a Tor user is visiting with perfect precision, particularly for less popular websites where the set of DNS names associated with that website may be unique to the site. We also use the Tor Path Simulator (TorPS) in combination with traceroute data from vantage points co-located with Tor exit relays to estimate the power of AS-level adversaries who might mount DefecTor attacks in practice.**

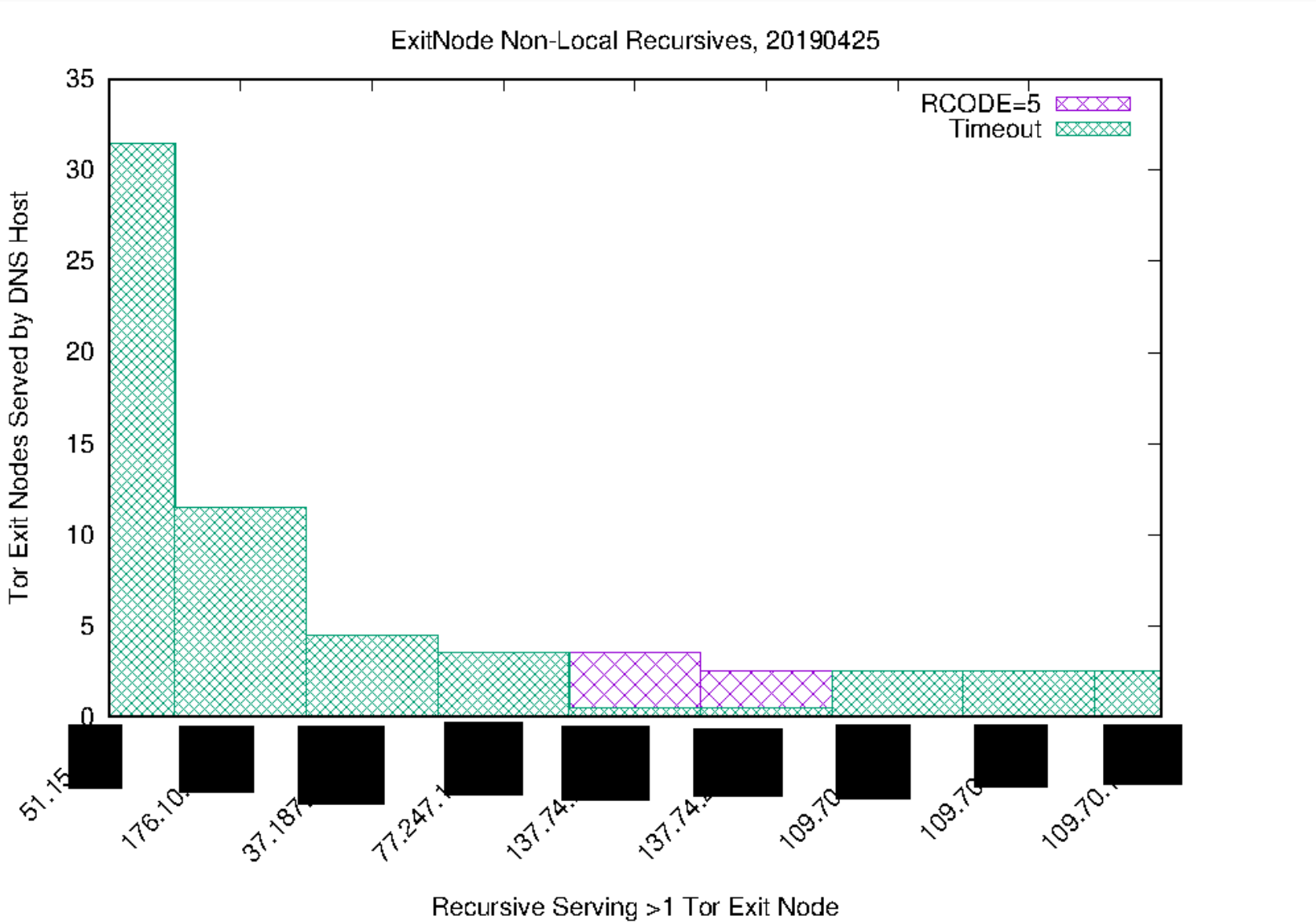
Fig. 1. Past traffic correlation studies have focused on linking the TCP stream entering the Tor network to the one(s) exiting the network. We show that an adversary can also link the associated DNS traffic, which can be exposed to many more ASes than the TCP stream.

correlate these two flows—a so-called *correlation attack*—can link the sender and receiver of a traffic flow, thus compromising the anonymity of both endpoints. Although TCP connections are an important part of communications, the Domain Name System (DNS) traffic is also quite revealing: for example, even loading a single webpage can generate hundreds of DNS requests to many different domains. No previous analysis of correlation attacks has studied how DNS traffic can exacerbate these attacks.

DNS traffic is highly relevant for correlation attacks because it often traverses completely different paths and au-

Source: [10]

Tor and DNS


ExitNode Non-Local Recursives, 20190425
RCODE=5
Timeout
Tor Exit Nodes Served by DNS Host
35
30
25
20
15
10
5
0
51.15
176.10.
37.187.
77.247.1
137.74.
137.74.5
109.70
109.70
109.70.1
Recursive Serving >1 Tor Exit Node

Summary of DNS and Privacy Networks

- ECS leaks, and breaks some anonymity networks
- Leaks go both ways: Dodgy Tor exit nodes flagged by ECS
- Testing/IETF debate did not reveal these specific impacts
  - The generic privacy concerns did not persuade
  - Drop-in testing only addresses on-path injuries

Looking Ahead to DOH

- DOH will reveal private network information
- Can we better estimate what this looks like?
- Sample data run of netbios leaks

Local Leaks via DOH

- Anticipated scenario: Enterprise DOH (E-DOH)
  - Motivation: Corporate audit criticism of cloud DNS use and BYOD
  - Implementation by PAC files, enterprise browser mgmt tools, etc
- Policy challenge for E-DOH
  - Determining true origin of query
  - Organic vs crafted js/uXSS-induced lookup, etc

Local Leaks via DOH

- `IN A? 255.in-addr.arpa`, check for aa bit set (credit to `fpdns`)
- Used to uniquely fingerprint Windows, now some Linux/RH
- Therefore follow up with `IN A? 1.0.0.127.in-addr.arpa` and `CH?` queries
- Summary of crawl:
  - 28,173,188 DNS speakers reached in IPv4
  - 234,061 edge leaked from Windows resolver
  - FQDNs nearly all internal

Local Leaks via DOH

Impacts of DOH

- Do not underestimate the need of local administrators to comply with laws and company policies: 443 MiTM returns
  - Eg. banning Mozilla in organizations (school moz removal)
  - Stretches RFC 7258 " Thus, we cannot defend against the most nefarious actors while allowing monitoring by other actors no matter how benevolent some might consider them to be, since the actions required of the attacker are indistinguishable from other attacks. The motivation for PM is, therefore, not relevant for how PM is mitigated in IETF protocols."
- Stock 1034: queries stay in ISP's data centers. Post DOH: queries now traverse multiple networks
- Unclear threat model
  - TRR opportunistic discovery, to avoid traffic analysis? (Reinvention of Kashpureff poisoning/"same-origin/bailiwick" issues for "serverless" TRR)
- Fails to protect against chosen authority monitoring

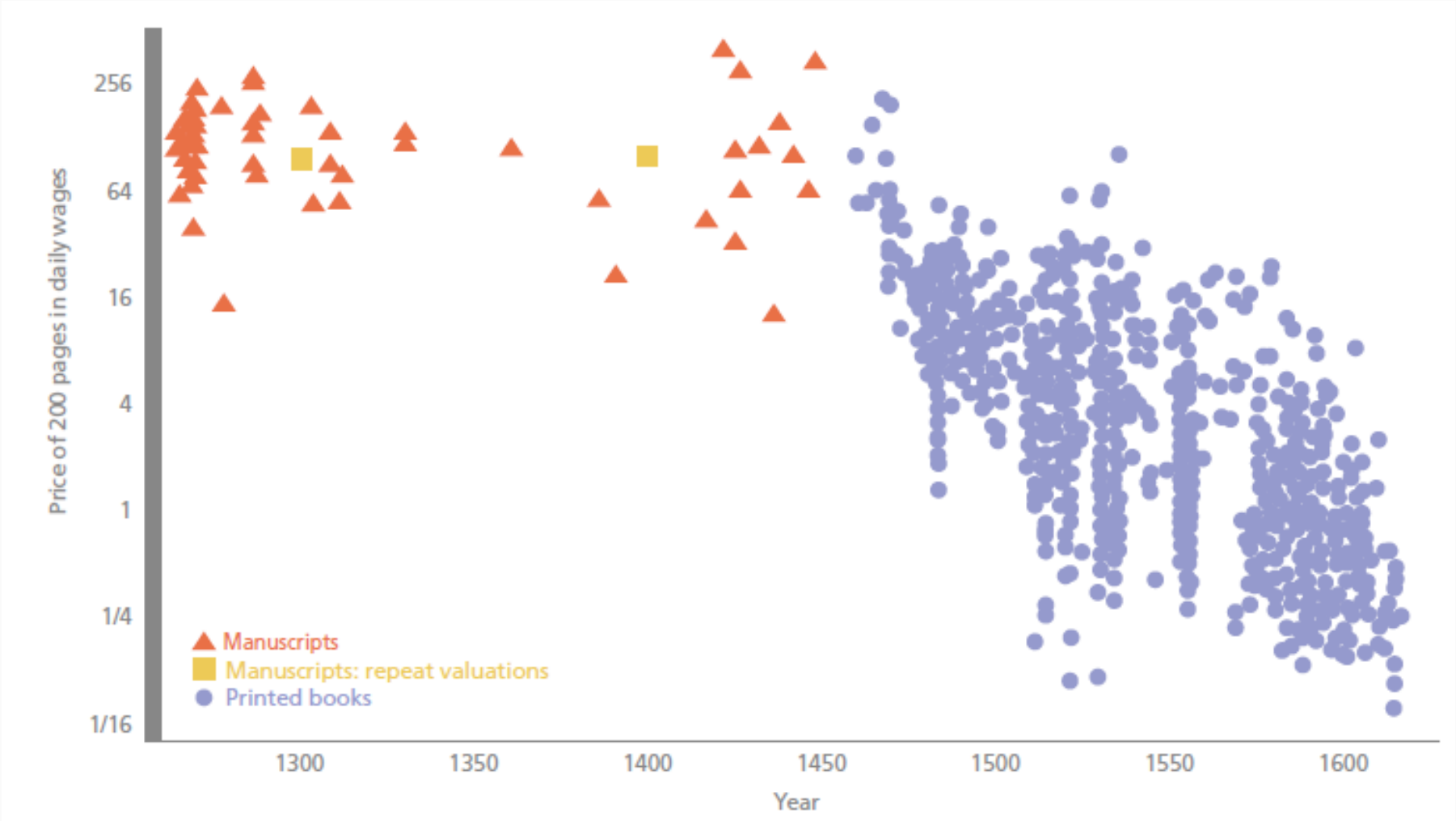
Observations

- Small changes to DNS protocols have *significant* unexpected impacts on privacy
- DNS-based filtration represents **user affirmative choice**
- Any policy reacting to passive DNS must, to prove effective, also address active DNS/chosen qname attacks
    - DOH claims such motivation, but fails
- Key DNS objectives
    - **Universality**. There is but one global DNS, modulo CDN
    - **Locality**. DNS as a whole exists to facilitate local user choice and truthful discovery of mappings.
    - **Drop-in Testing Hides Impact**.

DOH Predictions

- Children will lead; malware then follows
  - Schools removing Mozilla due to DOH DNS filter evasion
  - Malware will turn on/select TRR
- Enormous covert channel opportunity
- DOH will drive split horizon leaks
- First wave: malicious DOH proxies, forwarding to TRRs
- Splitting the stub into app vs OS resolution paths creates surprise and misaligned incentives
- Litigation potential for app vs stub

A Perspective on This Moment in History



Source: [7]

References I

Anon.

The invisible internet project.

https://geti2p.net/en/, May 2019.

S. Boten.

EDNS Client Subnet FAQ.

https://support.opendns.com/hc/en-us/articles/227987647-EDNS-Client-Subnet-FAQ, 2018.

References II

R. Chirgwin.
Monsters defeated in quest to free .onion from clutches of dns-snooping demons.
https://www.theregister.co.uk/2015/09/10/tors_onion_domain_gets_privacyconscious_users_off_the_dns/, September 2015.

C. Contavalli, W. van der Gaast, D. Lawrence, and W. Kumari.
Client subnet in dns queries.
https://www.rfc-editor.org/rfc/rfc7871.txt, May 2016.

References III

A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, and R. Smith.
Privacy considerations for internet protocols.
https://tools.ietf.org/html/rfc6973, July 2013.

F. Denis.
Frank DENIS random thoughts.
https://00f.net/2013/08/07/edns-client-subnet/, 08 2013.

References IV

J. Dittmar and S. Seabold.
Gutenbergs moving type propelled europe towards the scientific revolution.
https://blogs.lse.ac.uk/businessreview/2019/03/19/gutenbergs-moving-type-propelled-europe-towards-the-sci
March 2019.

G. P. DNS.
Edns client subnet (ecs) guidelines.
https://developers.google.com/speed/public-dns/docs/ecs,
August 2018.

References V

S. Farrell and H. Tschofenig.
Pervasive monitoring is an attack.
https://tools.ietf.org/html/rfc7258, May 2014.

B. Greschbach, T. Pulls, L. M. Roberts, P. Winter, and N. Feamster.
The effect of dns on tor's anonymity.
https://arxiv.org/pdf/1609.08187, October 2016.

A. Mohaisen and K. Ren.
Leakage of .onion at the dns root: Measurement, causes and countermeasures.
https://dl.acm.org/citation.cfm?id=3179948, October 2017.

References VI

P. Samarati and L. Sweeney.

Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression.

https://dataprivacylab.org/dataprivacy/projects/kanonymity/paper3.pdf, 1998.

zzz.

urlhttp://zzz.i2p/topics/2363.

zzz.

Develpment discussions: Proposal: Deprecate hostnames in routerinfo.

http://zzz.i2p/topics/2363, August 2017.