

Experiences with DoH Server Software

DNSheads Vienna Meetup

June 2019



Foundation for
Applied Privacy

Foundation for Applied Privacy

- Non-profit Privacy Infrastructure Provider
- We run privacy services for the public
- founded in 2018
- ISPA member



Foundation for
Applied Privacy

Agenda

- Why encrypt DNS traffic
- Our experiences with:
 - doh-httpproxy
 - knot-resolver
 - rust-doh
 - dnsdist
- Summary and Recommendations



Motivation



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver



Foundation for
Applied Privacy

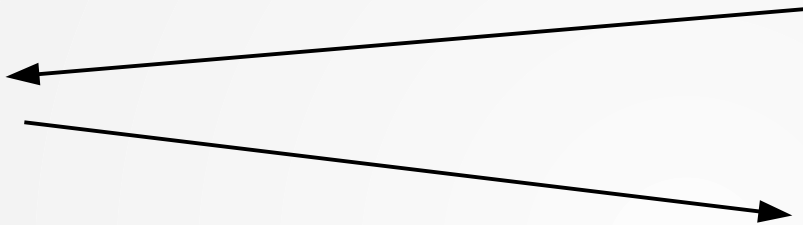


User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org



Foundation for
Applied Privacy



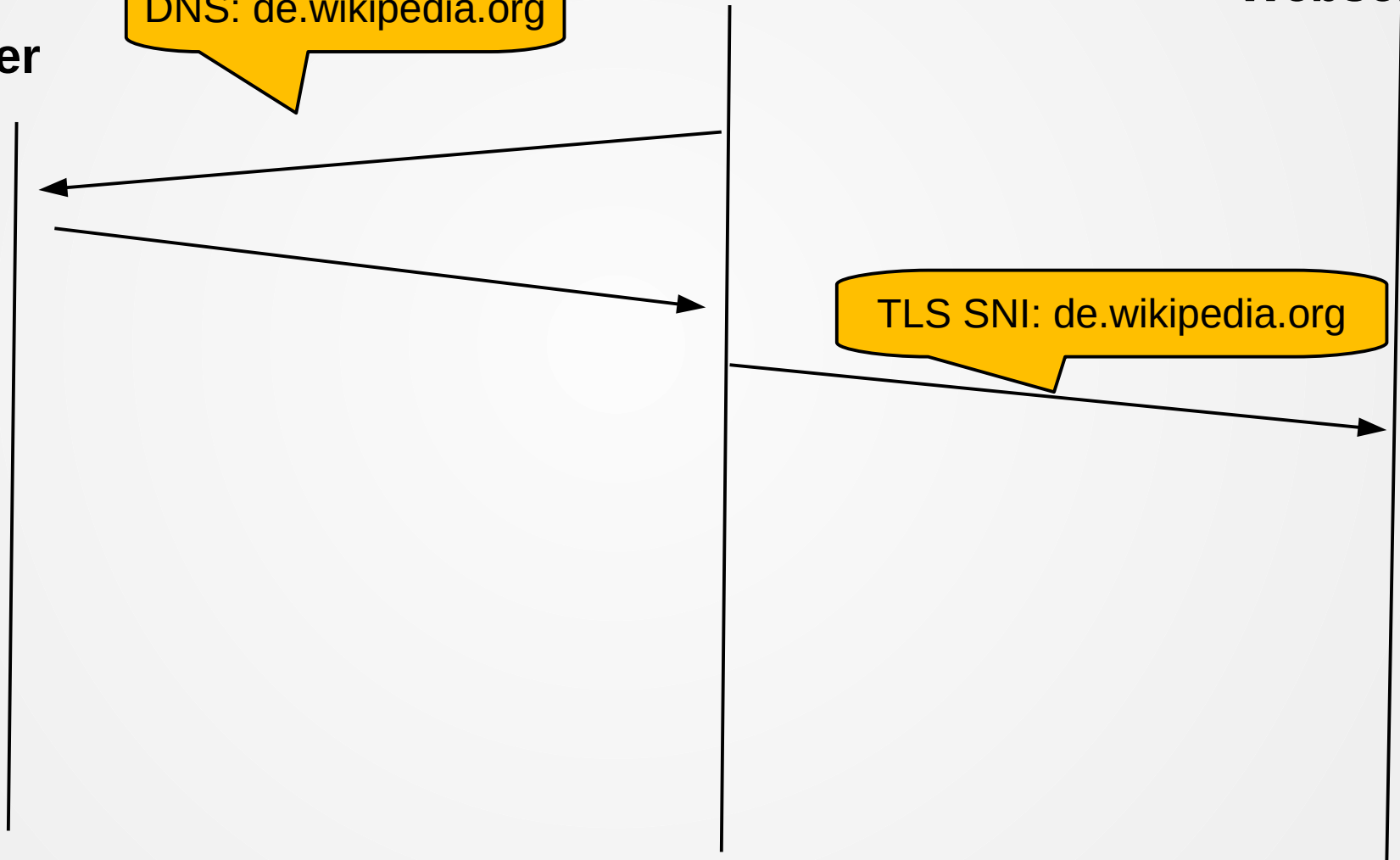
User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org

TLS Connection



Foundation for
Applied Privacy



User/Browser

de.wikipedia.org
Webserver

DNS
Resolver

DNS: de.wikipedia.org

TLS SNI: de.wikipedia.org

TLS cert: *.wikipedia.org

**metadata
in plaintext**

TLS Connection



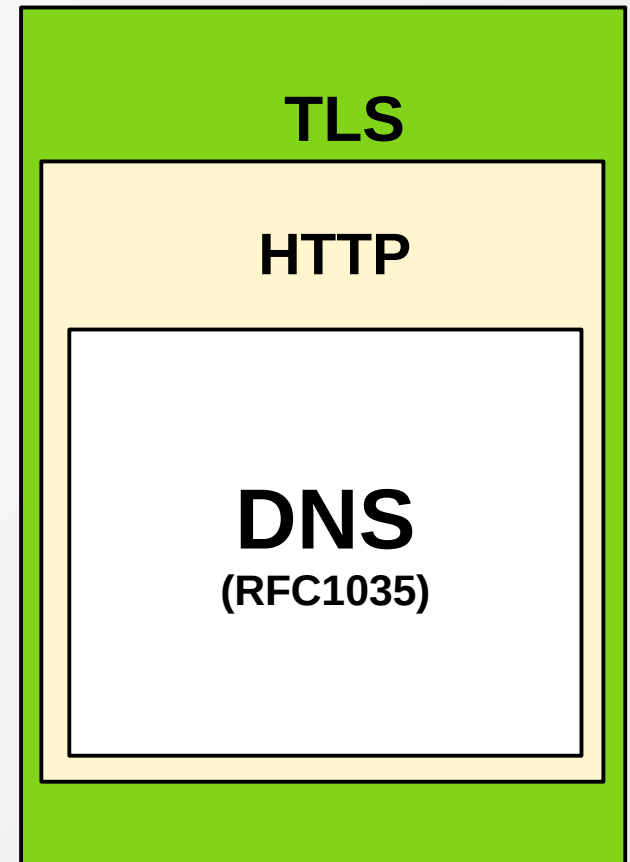
Foundation for
Applied Privacy

Leak	Solution	Effort for website operator
IP address	CDN/vHosts	~
TLS SNI	Work in Progress: Encrypted SNI (ESNI)	Big effort (Webserver + DNS)
TLS certificate	TLS 1.3	deploy TLS 1.3
OCSP	OCSP Stapling	Minor configuration effort
DNS	DoH/DoT/...	No effort (owner not involved)



DoH (RFC8484)

- HTTPS (TCP/443)
- **POST**
- or GET (base64url)
- HTTP/2 (recommended)
- Content Type:
application/dns-message



Encrypt all the things, DNS included!

Foundation for Applied Privacy — 2019-03-29 20:52

tldr; Today we are launching our new [DNS Privacy Services](#) supporting the DNS-over-TLS and DNS-over-HTTPS protocols.

<https://appliedprivacy.net/posts/dns-privacy-services-launch/>



Foundation for
Applied Privacy

doh-(http)proxy

facebookexperimental / doh-proxy

Watch 22

Star 271

Fork 34

Code

Issues 8

Pull requests 0

Projects 0

Security

Insights

A proof of concept DNS-Over-HTTPS proxy implementing <https://datatracker.ietf.org/doc/draft-ietf-doh-dns-over-https/>
<https://facebookexperimental.github.io/>

117 commits

1 branch

8 releases

9 contributors

View license

Branch: master

New pull request

Find File

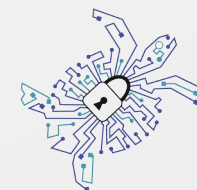
Clone or download



prajay and chantra Removes support for NPN in doh-proxy (#64) ...

Latest commit 09313bb on May 10

<https://github.com/facebookexperimental/doh-proxy>



Foundation for
Applied Privacy

doh-http-proxy

nginx → doh-http-proxy → unbound



Foundation for
Applied Privacy

doh-httpproxy

- easy setup (+)
- IETF hackaton proof-of-concept (-)
- no metrics (-)
- single DNS backend only (-)



knot-resolver 4.0.0

CZ-NIC / knot-resolver

Watch 25 Star 132 Fork 32

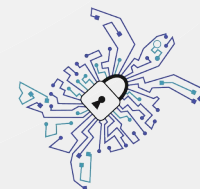
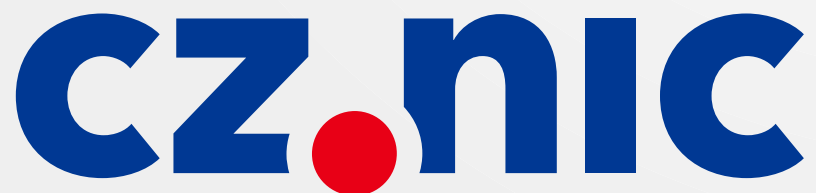
Code Issues 2 Pull requests 0 Security Insights

Knot Resolver - resolve DNS names like it's 2019 <https://www.knot-resolver.cz/>

dns resolver-library dnssec resolver daemon cache

4,937 commits 67 branches 38 releases 32 contributors GPL-3.0

<https://www.knot-resolver.cz/>



Foundation for
Applied Privacy

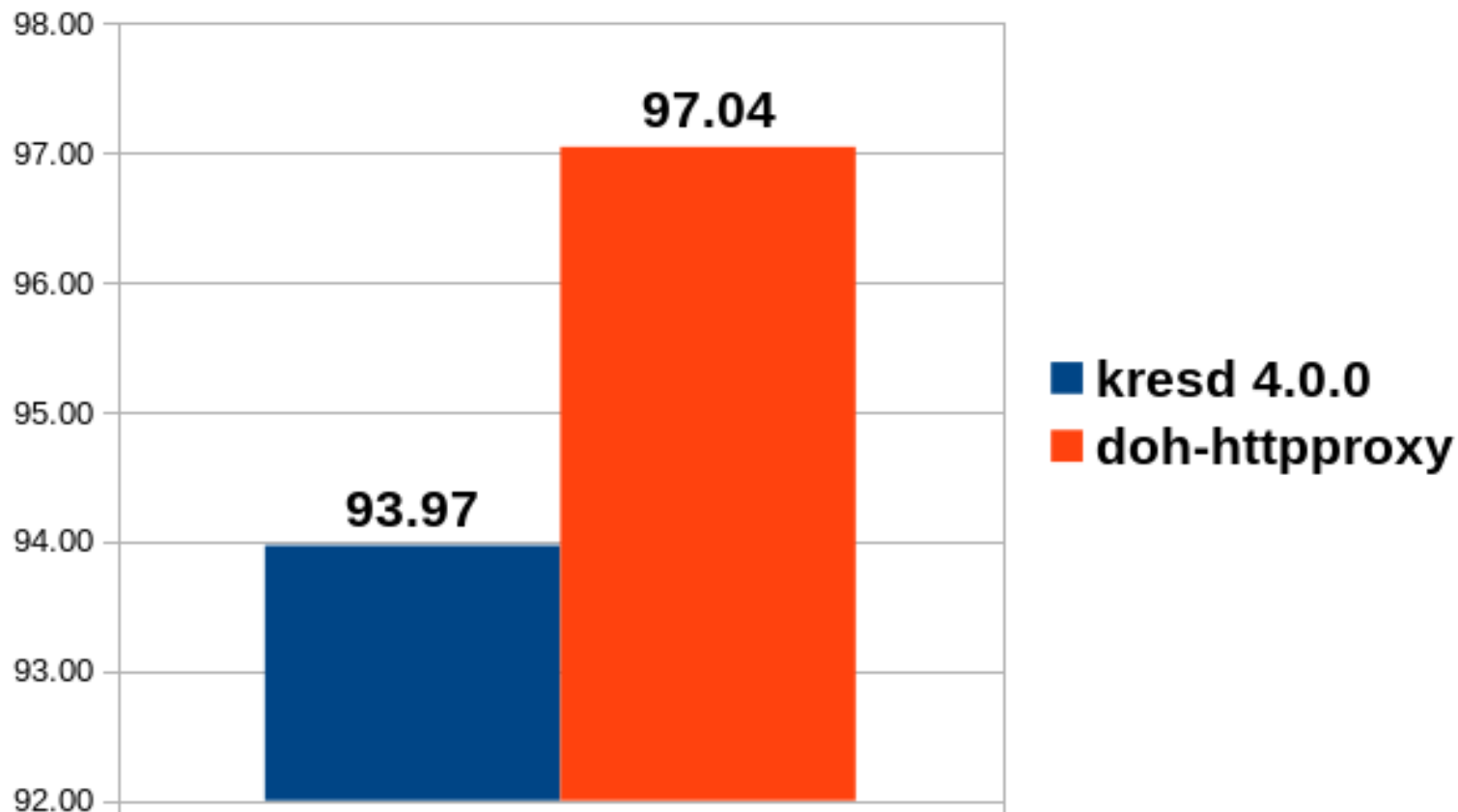
knot-resolver 4.0.0

- released on 2019-04-18
- DoH client → nginx → knot-resolver



kresd vs. doh-httpproxy

What percentage of HTTP requests are answered with '200 OK'? (more = better)



knot-resolver 4.0.0

HTTP parameter handling

<https://odvr.nic.cz/doh?dns=l1sBAAABAAAAAAAAAAAA3d3dw1rbm90LXJlc29sdmVyAmN6AAAcAAE>

200 OK

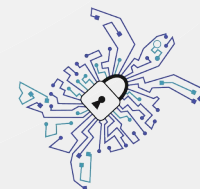
<https://odvr.nic.cz/doh?>

[dns=l1sBAAABAAAAAAAAAAAA3d3dw1rbm90LXJlc29sdmVyAmN6AAAcAAE](https://odvr.nic.cz/doh?dns=l1sBAAABAAAAAAAAAAAA3d3dw1rbm90LXJlc29sdmVyAmN6AAAcAAE&ct)**&ct**

400 Bad Request

Thread about HTTP parameter checking on the DoH working group mailing list:

<https://mailarchive.ietf.org/arch/msg/doh/naLd8rVW1HWmghlCs6qmtNq-5RE>



Foundation for
Applied Privacy

knot-resolver 4.0.0

Quote from knot-resolver developer Petr Špaček (cz.nic) from RIPE78 (2019-05-23):

“[...] we hate DoH implementation so please don't use it.”

<https://ripe78.ripe.net/archives/video/127/> (@ 18:13sec)



Foundation for
Applied Privacy

dnsdist

 PowerDNS / [pdns](#)

 Watch

125

 Star

1,735

 Fork

512

 Code

 Issues **622**

 Pull requests **59**

 Projects **0**

 Wiki

 Security

 Insights

PowerDNS

[powerdns](#)

[recursor](#)

[dns](#)

[dns-server](#)

[dnsdist](#)

[authoritative](#)

[powerdns-authoritative-server](#)

 **16,947** commits

 **13** branches

 **169** releases

 **165** contributors

 GPL-2.0

<https://dnsdist.org>

POWERDNS



Foundation for
Applied Privacy

dnsdist 1.4.0-alpha2

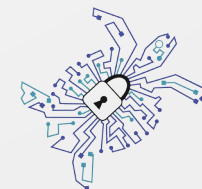
- released on 2019-04-26
- DoH client → dnsdist → unbound



dnssdist 1.4.0-alpha2

```
May 12 21:12:08 kernel: dnssdist/doh[11118]: segfault at 7fe0440af5a8 ip 0000560e7c0f1d98 sp
May 12 21:12:08 kernel: Code: de 97 cf ff e9 a1 00 d7 ff 48 89 c5 e9 af 00 d7 ff 48 89 c5 e9
May 12 21:12:08 systemd[1]: dnssdist.service: Main process exited, code=killed, status=11/SEGV
May 12 21:12:08 systemd[1]: dnssdist.service: Failed with result 'signal'.
May 12 21:12:10 systemd[1]: dnssdist.service: Service RestartSec=2s expired, scheduling restart
May 12 21:12:10 systemd[1]: dnssdist.service: Scheduled restart job, restart counter is at 1.
May 12 21:12:10 systemd[1]: Stopped DNS Loadbalancer.
May 12 21:12:10 systemd[1]: Starting DNS Loadbalancer...
May 12 21:12:10 dnssdist[18854]: Configuration '/etc/dnssdist/dnssdist.conf' OK!
[...]
```

Fixed in <24 hours after submitting issue



Foundation for
Applied Privacy

rust-doh

jedisct1 / rust-doh

Watch

11

Star

138

Fork

10

Code

Issues 5

Pull requests 0

Projects 0

Security

Insights

A DNS-over-HTTP server proxy

doh

dns

dnscrypt-proxy

http

proxy

97 commits

1 branch

14 releases

3 contributors

MIT

Branch: master

New pull request

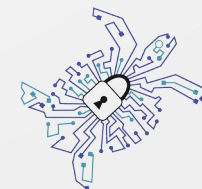
Find File

Clone or download

jedisct1 Check content-type instead of accept ...

Latest commit 224609e 5 days ago

<https://github.com/jedisct1/rust-doh>



Foundation for
Applied Privacy

rust-doh

- nginx → rust-doh → unbound
- faster/less CPU usage than doh-httproxy
- no proper HTTP return codes (i.e. connection teardown instead of return code '400 Bad Request')

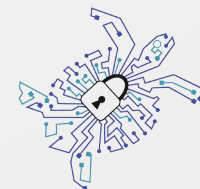
<https://github.com/jedisct1/rust-doh/issues/20>



Foundation for
Applied Privacy

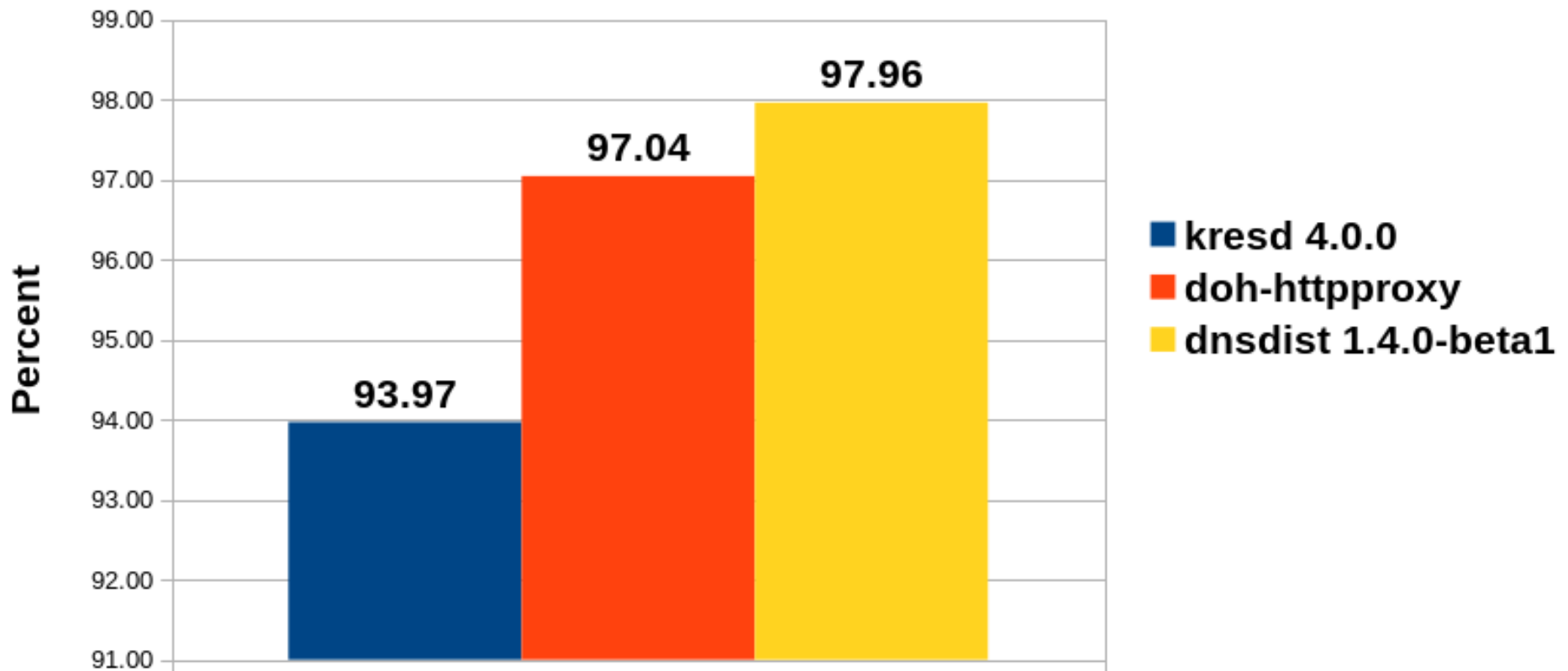
dnsmdist 1.4.0-beta1

- released on 2019-06-06
- includes fix for previously reported crashes (#7810)



kresd vs. doh-httpproxy vs. dnsdist 1.4.0-beta1

Fraction of successful Transactions (HTTP 200 OK)



sample size: 1 000 000 HTTP requests for
each DoH server



**Foundation for
Applied Privacy**

dnscdist

- easy installation: repositories for Debian/CentOS/SUSE...
- libh2o (supports HTTP/1.x and HTTP/2)
- SNI based matching



dnsmdist feature requests

- HTTP header (CORS) (#7900)
- OCSP Stapling (#7812)
- HTTP response code stats (#7898)

https://github.com/PowerDNS/pdns/issues/created_by/appliedprivacy



Foundation for
Applied Privacy



unbound

DoH implementation planned
for second half of 2019



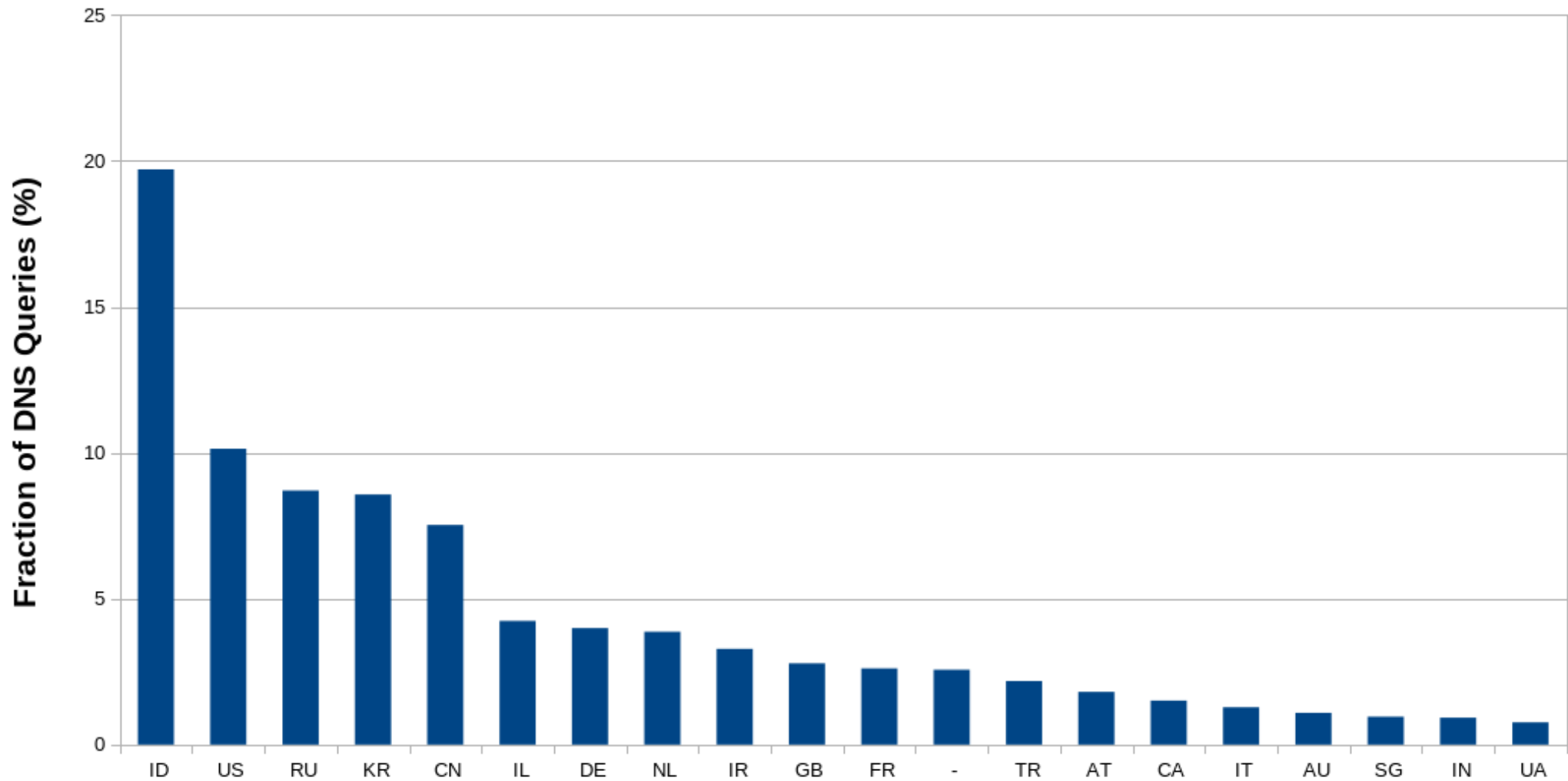
Foundation for
Applied Privacy

Summary

- **dnscast** is (currently) the best option and becoming production ready
- run DoH and DoT services to help prevent centralization



Top 20 Countries using DoH.appliedprivacy.net



Foundation for
Applied Privacy

Using DoH with Firefox

☐ Automatic proxy configuration URL

Reload

No proxy for

localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Do not prompt for authentication if password is saved

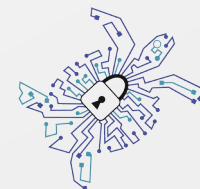
☐ Proxy DNS when using SOCKS v5

☒ Enable DNS over HTTPS

☐ Use default (https://mozilla.cloudflare-dns.com/dns-query)

☒ Custom

Help Cancel OK



Our DoH/DoT DNS resolvers

<https://doh.appliedprivacy.net/query>

dot1.appliedprivacy.net



Foundation for
Applied Privacy

Questions?

contact@appliedprivacy.net

Twitter: @applied_privacy

<https://appliedprivacy.net>



Foundation for
Applied Privacy