If you cite this paper, please use the WTMC reference: J. Zirngibl, P. Sattler, G. Carle. 2023. A First Look at SVCB and HTTPS DNS Resource Records in the Wild. *International Workshop on Traffic Measurements for Cybersecurity 2022*. WTMC.

A First Look at SVCB and HTTPS DNS Resource Records in the Wild

Johannes Zirngibl, Patrick Sattler, Georg Carle
Technical University of Munich, Germany
{*zirngibl, sattler, carle*}*@net.in.tum.de*

***Abstract*—The Internet Engineering Task Force is standardizing new DNS resource records, namely `SVCB` and `HTTPS`. Both records inform clients about endpoint and service properties such as supported application layer protocols, IP address hints or Encrypted Client Hello (ECH) information. Therefore, they allow clients to reduce required DNS queries and potential retries during connection establishment and thus help to improve the quality of experience and privacy of the client. The latter is achieved by reducing visible meta-data, which is further improved with encrypted DNS and ECH.**

The standardization is in its final stages and companies announced support, *e.g.*, Cloudflare and Apple. Therefore, we provide the first large-scale overview of actual record deployment by analyzing more than 400 M domains. We find 3.96 k `SVCB` and 10.5 M `HTTPS` records. As of March 2023, Cloudflare hosts and serves most domains, and most records only contain Application-Layer Protocol Negotiation (ALPN) and IP address hints. Besides Cloudflare, we see adoption by a variety of authoritative name servers and hosting providers indicating increased adoption in the near future. Lastly, we can verify the correctness of records for more than 93 % of domains based on three application layer scans.

1. Introduction

With the ongoing development of the Internet, available protocols and versions, a general requirement is getting more important, namely *information about supported application layer protocols, versions and properties by individual endpoints*. The latter information can be exchanged during a handshake or first communication (*e.g.*, Alternative Service (ALT-SVC) Headers in Hypertext Transfer Protocol (HTTP)). However, missing knowledge increases the handshake duration and information from existing solutions can only be used in subsequent connections. Each connection attempt and the potential use of insecure protocols reveals further meta-data related to a client and its desired connection, thus impacting its privacy and security.

To circumvent this problem, the Internet Engineering Task Force (IETF) works on a new general Domain Name System Resource Record (DNS RR) named `SVCB` ("SerViCe Binding") that provides service bindings for a domain [23]. This record accomplishes two major goals, directing a client *(i)* to another alias or *(ii)* to an endpoint including service information. As a first subtype, the `HTTPS` DNS RR is specified with a focus on Hypertext Transfer Protocol Secure (HTTPS) endpoints. The records allow a client to receive all required information, namely supported protocols, used ports and IP addresses, using a *single*, recursive DNS query. Provided information can be used to directly establish a secure communication channel using a protocol both endpoints support. Information about available application protocols and their explicit version can also reduce the risk of on-path or downgrade attacks, *e.g.*, make HTTP Strict Transport Security (HSTS) obsolete. Furthermore, the new `HTTPS` record is supposed to be extended to provide ECH information to the client in the future. Once specified and deployed, ECH [21] further reduces the visibility of connection-related meta-data, *e.g.*, the Server Name Indication (SNI).

Quick and widespread deployment of these new records can drastically improve the privacy of clients on the Internet. Different operators including Cloudflare [3] and Akamai [2] but also client software, *e.g.*, Apple iOS [25] and Google Chromium [8] have already announced support for the new records.

Therefore, we set out to evaluate actual deployments and availability of the new records based on a large-scale measurement. Our contributions in this paper are:

(i) We evaluate the support of new records for more than 400 M domains. We show that the deployment is mostly driven by Cloudflare. However, other operators show initial deployment as well.

(ii) We evaluate the properties of received records and their implication for a client and established connections. We show that most domains have records with service information, mainly Application-Layer Protocol Negotiation (ALPN) values and *ipv4-* and *ipv6hints*. Further parameters are rarely visible.

(iii) We verify the correctness of received information with application layer scans. We were able to connect to 96 % of targets extracted from `HTTPS` records.

2. Background

The `SVCB` DNS RR represents a more general record to be used with different service types, while the `HTTPS` DNS RR is specifically designed to be used with HTTPS. These DNS RRs allow clients to select the correct service properties directly. To indicate the desired service, domains for `SVCB` records should be prefixed with Attrleaf labels [10] (*e.g.*, *_dns*). Using `HTTPS` records implies HTTP as service. Table 1 shows two example records. IETF designs both records to be flexible and expandable. The first `SVCB` record is in alias mode, indicated by the priority of *0*, and redirects the domain to another target name. In comparison to canonical name (CNAME) records, this is also possible at the apex of a zone [23].

The second `HTTPS` record is in service mode and provides further information about the endpoint. In service

TABLE 1. EXAMPLE SVCB AND HTTPS DNS RRS

Domain	TTL	CLASS	TYPE	Priority	Target Name	SvcParams
coffebike.no.	3600	IN	SVCB	0	barmobile.no.	
cloudflare.com.	30	IN	HTTPS	1	.	alpn="h3,h2" ipv4hint=104.16.132.229,104.16.133.229

mode, a target name can be set to indicate another name. The target name is "." if the actual domain should be used. Additional record data is organized as key-value data, so-called *SvcParams*. Each parameter has to have a specified format to allow interoperability. As of March 2023, the draft specifies six different parameter keys and their value format. By default, an HTTPS record indicates HTTP/1.1 support. The *alpn* parameter can indicate additional protocols. If an endpoint does not support HTTP/1.1 but other ALPNs the *no-default-alpn* parameter has to be added. The *port* parameter allows indicating alternative ports, while *ipv4-* and *ipv6hint* allow informing about IP addresses. Finally, the *mandatory* parameter can be used to indicate a set of parameters that must be used for the service to function correctly.

The initially drafted but now reserved *ech* parameter relies on a different draft [21]. However, it lacks deployment (see Section 4) and its final publication is delayed. Therefore, after a discussion [28], the parameter and references were removed from the SVCB and HTTPS draft [23] to allow an RFC publication. We evaluate the presence of this parameter in Section 4.

For SVCB records prefixed with *_dns*, the respective draft additionally adds the *dohpath* parameter that allows to specify a Uniform Resource Identifier (URI) template for DNS over HTTPS [22].

3. Data Collection

This work relies on active measurements to collect DNS data and verify the usefulness of collected records using HTTP scans. This section explains all scans conducted between February 22nd and March 9th, 2023, and covers ethical considerations.

DNS Scans: We used MassDNS[1] with a local Unbound resolver to resolve more than 400 M domains to their SVCB and HTTPS, but also A and NS records. We further resolved the name server domains from the latter NS records to their respective A records. This allows us to analyze who serves the new record and which operators are involved. We combined domains from the following sources as input for our measurement:
(i) Names on the Majestic [17], Alexa[2] [4], and Umbrella [9] Top 1M lists;
(ii) More than 1 k available zone files from the Centralized Zone Data Service, *e.g.*, *.com*, *.net* and *.org*;
(iii) A static collection of 98 M domains from 52 country-code TLDs (partial zones, *e.g.*, 13 M *.de* domains);
(iv) www. domains extracted from Certificate Transparency logs between August 2022 and January 2023.

We additionally prefixed domains with the Attrleaf label *_dns* [10]. As of March 2023, it was the only available label based on an IETF draft [22]. We exclude www. domains for this measurement but included domains from NS record names.

Protocol Scans: We used the QScanner introduced by Zirngibl *et al.* [29] and the Goscanner [13] to test whether received ALPN information is valid for the given domain. The QScanner supports QUIC handshakes and HTTP/3 requests while the Goscanner supports Transport Layer Security (TLS)/TCP handshakes and HTTP/1.1 and HTTP/2 requests.

For each domain with an HTTPS record in service mode, we extracted the supported ALPNs, port and IP addresses from the *ipv4hint* in the records. If no *ipv4hint* is available, we rely on each domain's additionally requested A records. We use these tuples of domain, IP address, port, and ALPN to seed our protocol scans.

Ethics: During all our scans, we strictly followed a set of ethical measures, *i.e.*, informed consent [11] and community best practices [19]. Our scans are conducted with a limited rate and use a request-based blocklist. Furthermore, our measurement vantage point is clearly identified based on reverse DNS, WHOIS information, and a hosted website. We did not receive any inquiries related to our scans during this work.

4. Analysis

We analyze the current deployment of SVCB and HTTPS records based on our measurements described in Section 3. Resolving more than 400 M domains, we received SVCB records for 3.96 k domains but HTTPS records for 10.56 M domains. SVCB should be available for domains with Attrleaf labels [10]. Therefore, we additionally resolved domains prefixed with the first specified label (*_dns*) but only received records for 27 domains.

4.1. General Record Analysis

Table 2 shows which modes (alias vs service) are used and which keys are commonly present in available records. Regarding SVCB records, 3.9 k (98.4 %) domains use the record for alias mode, aliasing the service to a different domain. Only 62 domains use the service mode and mostly advertise ALPN values or IPv4 and IPv6 addresses as hints. 27 domains prefixed with *_dns* result in SVCB records. All records are in service mode advertising different ALPN values (4× *h2* for DNS over HTTPS and 26× *dot* for DNS over TLS). The DoH path advertised by a single domain is /dns-query?dns. The SVCB record in both scenarios is only deployed by few domains and we focus on HTTPS records for the remainder of this paper.

Regarding HTTPS records, only 2.6 k (0.02 %) domains use the alias mode, while a majority advertises endpoint information using the service mode. Similarly, most domains advertise ALPN values and IPv4 and IPv6

1. https://github.com/blechschmidt/massdns
2. We use the last published list before deprecation from February 1st, 2023. https://toplists.net.in.tum.de/archive/alexa/

TABLE 2. NUMBER OF DOMAINS WITH EACH PROPERTY AND PARAMETER IN THEIR SVCB AND HTTPS DNS RESOURCE RECORDS.

		Mode		Keys							
Record	Total	Alias	Service	Mandatory	ALPN	No Default	Port	ECH	IPv4 Hint	IPv6 Hint	DoH Path
SVCB	3.96 k	3.9 k	62	0	53	0	2	0	25	15	-
HTTPS	10.56 M	2.6 k	10.55 M	0	10.55 M	0	13	20	10.55 M	10.23 M	-
SVCB + *_dns*	27	0	27	0	26	0	12	0	1	1	1

TABLE 3. TOP 5 ADVERTISED ALPN SETS/VALUES IN HTTPS DNS RESOURCE RECORDS. NOTE THAT HTTPS RECORDS IMPLY THE SUPPORT OF HTTP/1.1 BY DEFAULT [23].

ALPN sets	Domains	ALPN values	Domains
h3, h3-29, h2	9.72 M	h2	10.55 M
h2	0.83 M	h3	9.72 M
	3.23 k	h3-29	9.72 M
h3, h3-29	866	http/1.1	15
h2, h3	242	h2c	10

addresses as hints. The HTTPS record implies support of HTTP/1.1 by default if the *no-default-alpn* parameter is not present. In our results, no domain with an HTTPS record in service mode has the flag set. Table 3 shows the Top-5 advertised ALPN parameters. A majority of domains advertise HTTP version 2 but also 3 indicating QUIC support, while 834.4 k only advertise HTTP/2. 3.2 k domains do not advertise additional ALPN values but only rely on the default. A client can still use record information and only establish a connection if it supports HTTP/1.1.

While for 10.55 M (99.9 %) domains IPv4 hints are available, 10.23 M (96.9 %) additionally advertise IPv6 addresses. Most hints contain two addresses respectively but up to eight different addresses are visible as shown in Figure 1. This allows a client to select from a set of different addresses and fallback to alternatives if necessary. All other keys are only visible with a few domains. The advertised ports in HTTPS records are 80 (2×), 443 (10×) and 8920 (1×). Furthermore, we only receive 20 ECH configurations. This supports the discussion that the respective ECH draft [21] still lacks deployment while the DNS RRs are already deployed for many domains and both drafts should be decoupled. [28] 146.5 k domains from the Alexa [4], 169 k from Majestic [17] and 80.8 k domains from the Umbrella [9] Top 1M lists have an HTTPS record. The most prominent candidates are `google.com` with a service mode record and an ALPN parameter *h2,h3* and `youtube.com` with a service mode record without additional data.

Key take-away: *The SVCB record in both scenarios are only deployed by few domains. In contrast, more than 10 M domains make use of HTTPS records, mostly serving address hints and ALPN values. The alias mode or remaining parameters are rarely used and should be reevaluated in the future.*

4.2. Involved Operators

For the following analysis, we focus on domains with HTTPS records in service mode (10.55 M) due to their advanced deployment. To get a better understanding of involved operators, we analyze where domains are hosted

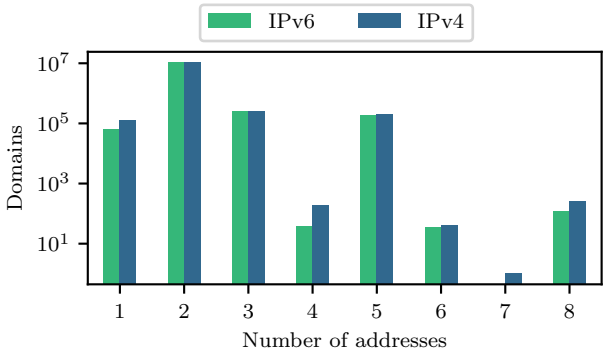

Figure 1. Addresses in *ipv4-* and *ipv6hints*. Note the logarithmic y-axis.

and which name servers are used. If available, we use *ipv4hints* and map addresses to the Autonomous System (AS) announcing the respective prefix. For all domains without this parameter, we use queried A records for IPv4 addresses.

Domains with HTTPS records are hosted in 2.3 k ASes. However, Table 4 shows that a majority of domains (98.8 %) resolves to ASes operated by Cloudflare (AS13335 and AS209242). Domenshop, a Norwegian web hoster, hosts the second-highest number of domains and accounts for a large share of domains indicating support for HTTP/2 but not HTTP/3. Following the Top 3 a more even distribution of the remaining 72 k domains across 2.3 k ASes is visible.

To analyze responsible name servers, we rely on NS records for domains exactly matching domains in our input. We do not follow CNAME records or extract information from SOA records. During our scan, we received NS records for 7.8 M domains with an HTTPS record. Domains without NS records in our data are either resulting in SOAs only (mostly *www.* domains) or resolve to canonical names and would require further resolution steps. In general, we are able to identify name servers supporting HTTPS records hosted in 661 different ASes. This shows a widespread deployment of name servers that support the new record in general.

Similar to web hosting, most HTTPS records are served by name servers hosted within Cloudflare followed by Domenshop. The latter appears as three different ASes (AS1921, AS12996, AS208045). Each AS hosts a name server authoritative for a similar amount of domains respectively. Most domains have one NS record for each of the three name servers for resilience.

Key take-away: *Domains with HTTPS records are hosted in more than 2.3 k ASes and name servers serving the records are in more than 1.6 k ASes. However, most records are hosted in and served by Cloudflare (98 %).*

TABLE 4. TOP 5 WEB HOSTERS (OUT OF 2.3 K) AND NAME SERVER PROVIDERS (OUT OF 661) OF DOMAINS WITH HTTPS RECORDS.

Hosting			Name server		
ASN	Name	#Doms	ASN	Name	#Doms
13335	Cloudflare	10.4 M	13335	Cloudflare	7.7 M
12996	Domenshop	61.6 k	12996[1]	Domenshop	24.0 k
209242	Cloudflare	49.7 k	16509	Amazon	3.2 k
397273	Render	4.9 k	397226	Neustar	3.1 k
14061	Digitalocean	4.6 k	44273	GoDaddy	2.5 k

[1] Domenshop uses three different name servers for most domains located in three different ASes (AS1921, AS12996, AS208045)

TABLE 5. PROTOCOL SCAN RESULTS BASED ON HTTPS RECORDS. TARGETS ARE A COMBINATION OF DOMAIN AND IP ADDRESS PAIRS.

		Successful			
HTTP	Targets	TLS Handshake		HTTP Requests	
1.1	21.44 M	20.72 M	96.63 %	19.48 M	90.84 %
2	21.43 M	20.73 M	96.69 %	19.47 M	90.84 %
3	19.59 M	18.34 M	93.64 %	17.04 M	87.01 %

4.3. Validity of Records

We conducted HTTP scans to check the validity of collected records and whether clients can use the received information for an HTTP request. The general scan approach is described in Section 3. We focus on HTTP/1.1, HTTP/2 and HTTP/3, and select targets for each scan based on the ALPN and IP address hints. Table 5 provides an overview about results. TLS/TCP handshakes are successful for more than 96.6 % of evaluated targets for each HTTP version respectively while QUIC handshakes are successful for more than 93.6 % of HTTP/3 targets. For 90 %, we are further able to conduct an HTTP HEAD request. Most unsuccessful connection attempts either result in a time out (1.1: 6.4 k, 2: 9.1 k, 3: 50.8 k) or a generic TLS handshake failure (1.1: 708.9 k, 2: 692.1 k. 3: 1.2 M).

Successful scans for HTTP/1.1 and HTTP/2 still cover 1.8 k ASes while HTTP/3 and thus QUIC scans only cover 416 ASes out of 2.3 k candidates. Analyzing failed scans reveals that a major origin of errors during QUIC scans and for timeouts during the HTTP request is an attack prevention mechanism by Cloudflare [18]. It is an automated challenge mechanism that delays the page load which results in errors with both the Goscanner and QScanner.

Furthermore, we find 23.0 k domains with HTTPS records served by Cloudflare name servers but hosted in different ASes that only result in timeouts at least during QUIC scans. For those domains, scan results (timeouts) are reproducible. Interestingly, those domains are hosted in more than 1.3 k ASes and no relation is visible besides the Cloudflare name servers. Furthermore, all HTTPS contain the same ALPN set (*h3, h3-29, h2*). We assume a misconfiguration and informed Cloudflare.

Key take-away: *A majority of available HTTPS records contains valid, usable information especially if used by clients able to pass Cloudflare's attack prevention. However, we identify a set of records with incorrect ALPN values. For those domains requests for some announced ALPN values time out consistently (mostly HTTP/3).*

5. Related Work

SVCB and HTTPS records have seen little attention by other research so far. In 2021, Zirngibl *et al.* [29] used HTTPS records to identify QUIC deployments. They found records for 2.9 M domains indicating QUIC support hosted in 1.2 k ASes. However, they do not analyze records further. In contrast, they find HTTP ALT-SVC Headers for more than 20 M domains. While the latter is an alternative approach to distribute endpoint information, it requires a previous HTTP communication. Two years later, we find 4× more HTTPS records hosted in twice as many ASes. Similarly, Trevisan *et al.* [26] use alternative service information to identify QUIC deployments but only HTTP ALT-SVC Header headers from additional HTTP requests. Both, Zirngibl *et al.* and Trevisan *et al.* implied that HTTP ALT-SVC Headers are widely deployed. We show that still fewer HTTPS records are deployed, but growth is visible.

In 2019, Chai *et al.* [7] evaluated Encrypted SNI, an older version of ECH that relied on TXT DNS RR to distribute key information. They identified more than 100 k domains within the Alexa Top 1M. Similar results have been reported by Tsiatsikas *et al.* [27] in 2022. In 2022, Hoang *et al.* [14] find 1.5 % to 2.25 % domains with a respective TXT record out of 300 M domains from TLD zone files. We show that no transition to ECH and HTTPS records is visible yet. Weber [20] reported about the visibility of HTTPS queries from a network (Akamai) perspective. While many queries failed with incorrect behavior initially, the correctness of seen responses changes quickly. Additionally, they only observed records for 126.4 k domains and no alias mode. Aguilar-Melchor *et al.* [1] evaluate a potential positive effect of HTTPS records but do not evaluate its current deployment state.

Furthermore, the security and impact of ECH has been analyzed [5], [24] and related work has evaluated the state of DNS over TCP, HTTP or QUIC [6], [12], [15], [16], and shows increased deployment and in general good performance. Thus, the fundamentals for a successful deployment of SVCB and HTTPS records are given.

6. Conclusion

In this work, we provide the first large-scale overview of the deployment of new SVCB and HTTPS DNS resource records. While we find only very few domains with SVCB records (3.96 k without and 26 with an Attrleaf label), we show that more than 10 M domains already resolve to HTTPS records. These records mainly provide ALPN values and *ipv4-* and *ipv6hints*. We find only 20 domains with an ECH parameter which indicates lacking deployment. However, we show that most domains are hosted within Cloudflare, and Cloudflare operated name servers are authoritative.

Nevertheless, information contained in most available records is correct, and handshakes followed by HTTP requests with indicated versions are possible. Therefore, clients already querying the records (e.g., Apple devices [25]) can effectively make use of HTTPS records for more than 10 M domains and reduce, DNS requests and visible meta-data during connections establishments while reducing handshake cost.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable feedback. This work was partially funded by the German Federal Ministry of Education and Research under the project PRIMEnet (16KIS1370), 6G-life (16KISK002) and 6G-ANNA (16KISK107) as well as the German Research Foundation (HyperNIC, grant no. CA595/13-1). Additionally, we received funding by the Bavarian Ministry of Economic Affairs, Regional Development and Energy as part of the project 6G Future Lab Bavaria and the European Union's Horizon 2020 research and innovation program (grant agreement no. 101008468 and 101079774).

References

[1] Carlos Aguilar-Melchor, Thomas Bailleux, Jason Goertzen, David Joseph, and Douglas Stebila. TurboTLS: TLS connection establishment with 1 less round trip, 2023. https://arxiv.org/abs/2302.05311.

[2] Akamai. New SVCB & HTTPS Resource Records in the wild, 2020. https://community.akamai.com/customers/s/article/NetworkOperatorCommunityNewSVCBHTTPSResourceRecordsinthewild20201128135350 (Accessed: 2023-03-08).

[3] Alessandro Ghedini. Speeding up HTTPS and HTTP/3 negotiation with... DNS, 2020. https://blog.cloudflare.com/speeding-up-https-and-http-3-negotiation-with-dns/ (Accessed: 2023-03-08).

[4] Alexa. Top 1M sites, 2022. https://web.archive.org/web/20220501101403/https://www.alexa.com/topsites (Accessed: 2023-03-08).

[5] Karthikeyan Bhargavan, Vincent Cheval, and Christopher Wood. A Symbolic Analysis of Privacy for TLS 1.3 with Encrypted Client Hello. In *Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS)*, CCS '22, page 365–379, New York, NY, USA, 2022. Association for Computing Machinery.

[6] Timm Böttger, Felix Cuadrado, Gianni Antichi, Eder Leão Fernandes, Gareth Tyson, Ignacio Castro, and Steve Uhlig. An Empirical Study of the Cost of DNS-over-HTTPS. In *Proc. ACM Int. Measurement Conference (IMC)*, New York, NY, USA, 2019. Association for Computing Machinery.

[7] Zimo Chai, Amirhossein Ghafari, and Amir Houmansadr. On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention. In *9th USENIX Workshop on Free and Open Communications on the Internet, FOCI*. USENIX Association, 2019.

[8] Chrome Platform Status. Feature: HTTP -> HTTPS redirect for HTTPS DNS records, 2021. https://chromestatus.com/feature/5485544526053376 (Accessed: 2023-03-08).

[9] Cisco. Umbrella Top 1M List, 2022. https://s3-us-west-1.amazonaws.com/umbrella-static/index.html (Accessed: 2023-05-18).

[10] Dave Crocker. Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves. RFC 8552, March 2019.

[11] David Dittrich, Erin Kenneally, et al. The Menlo Report: Ethical principles guiding information and communication technology research. *US Department of Homeland Security*, 2012.

[12] Trinh Viet Doan, Irina Tsareva, and Vaibhav Bajpai. Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times. In *Proc. Passive and Active Measurement (PAM)*. Springer International Publishing, 2021.

[13] Oliver Gasser, Markus Sosnowski, Patrick Sattler, and Johannes Zirngibl. Goscanner, 2023. https://github.com/tumi8/goscanner.

[14] Nguyen Phong Hoang, Michalis Polychronakis, and Phillipa Gill. Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering. In *Proc. Passive and Active Measurement (PAM)*. Springer International Publishing, 2022.

[15] Mike Kosek, Trinh Viet Doan, Simon Huber, and Vaibhav Bajpai. Measuring DNS over TCP in the Era of Increasing DNS Response Sizes: A View from the Edge. *ACM SIGCOMM Computer Communication Review*, 52(2), June 2022.

[16] Mike Kosek, Luca Schumann, Robin Marx, Trinh Viet Doan, and Vaibhav Bajpai. DNS Privacy with Speed? Evaluating DNS over QUIC and Its Impact on Web Performance. In *Proc. ACM Int. Measurement Conference (IMC)*, New York, NY, USA, 2022. Association for Computing Machinery.

[17] Majestic. The Majestic Million, 2022. https://majestic.com/reports/majestic-million/ (Accessed: 2023-03-08).

[18] Matthew Prince. Introducing: I'm Under Attack Mode, 2012. https://blog.cloudflare.com/introducing-im-under-attack-mode/ (Accessed: 2023-03-08).

[19] Craig Partridge and Mark Allman. Addressing Ethical Considerations in Network Measurement Papers. *Communications of the ACM*, 59(10), October 2016.

[20] Ralf Weber. DNS HTTP RR: a bright new future?, 2021. https://indico.dns-oarc.net/event/37/contributions/810/attachments/784/1413/dns-https-rr-final.pdf (Accessed: 2023-03-08).

[21] Eric Rescorla, Kazuho Oku, Nick Sullivan, and Christopher A. Wood. TLS Encrypted Client Hello. Internet-Draft draft-ietf-tls-esni-16, Internet Engineering Task Force, April 2023. Work in Progress.

[22] Benjamin M. Schwartz. Service Binding Mapping for DNS Servers. Internet-Draft draft-ietf-add-svcb-dns-08, Internet Engineering Task Force, March 2023. Work in Progress.

[23] Benjamin M. Schwartz, Mike Bishop, and Erik Nygren. Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs). Internet-Draft draft-ietf-dnsop-svcb-https-12, Internet Engineering Task Force, March 2023. Work in Progress.

[24] Danil Shamsimukhametov, Anton Kurapov, Mikhail Liubogoshchev, and Evgeny Khorov. Is Encrypted ClientHello a Challenge for Traffic Classification? *IEEE Access*, 10:77883–77897, 2022.

[25] Tommy Pauly. DNS HTTPS/SVCB record type support in iOS 14, 2020. https://mailarchive.ietf.org/arch/msg/dnsop/ldaCto09yaOuSXM92HgJhGqmPJw/ (Accessed: 2023-03-22).

[26] Martino Trevisan, Danilo Giordano, Idilio Drago, and Ali Safari Khatouni. Measuring HTTP/3: Adoption and Performance. In *19th Mediterranean Communication and Computer Networking Conference (MedComNet)*, 2021.

[27] Zisis Tsiatsikas, Georgios Karopoulos, and Georgios Kambourakis. Measuring the Adoption of TLS Encrypted Client Hello Extension and Its Forebear in the Wild. In *Computer Security. ESORICS 2022 International Workshops*, 2023.

[28] Warren Kumari. Breaking the logjam that is draft-ietf-dnsop-svcb-https, 2023. https://mailarchive.ietf.org/arch/msg/dnsop/5aiWtJbmAoqj7-5oD03Rgw1PEoo/ (Accessed: 2023-03-08).

[29] Johannes Zirngibl, Philippe Buschmann, Patrick Sattler, Benedikt Jaeger, Juliane Aulbach, and Georg Carle. It's over 9000: Analyzing early QUIC Deployments with the Standardization on the Horizon. In *Proc. ACM Int. Measurement Conference (IMC)*, 2021.