Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting

Yevheniya Nosyk, Maciej Korczyński, Andrzej Duda

Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting

Yevheniya Nosyk
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France
yevheniya.nosyk@univ-grenoble-alpes.fr

Maciej Korczyński
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France
maciej.korczynski@univ-grenoble-alpes.fr

Andrzej Duda
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France
andrzej.duda@univ-grenoble-alpes.fr

ABSTRACT

The Domain Name System (DNS) relies on response codes to confirm successful transactions or indicate anomalies. Yet, the codes are not sufficiently fine-grained to pinpoint the root causes of resolution failures. RFC 8914 (Extended DNS Errors or EDE) addresses the problem by defining a new extensible registry of error codes to be served inside the `OPT` resource record. In this paper, we show that four major DNS resolver vendors and three large public DNS resolvers support this standard and correctly narrow down the cause of underlying problems. Yet, they do not agree in 94% of our test cases in terms of the returned EDE codes. We reveal that Cloudflare DNS is the most precise in indicating various DNS misconfigurations via the EDE mechanism, so we use it to perform a large-scale analysis of more than 303M registered domain names. We show that 17.7M of them trigger EDE codes. Lame delegations and DNSSEC validation failures are the most common problems encountered.

CCS CONCEPTS

• **Networks** → **Naming and addressing**; **Network measurement**.

KEYWORDS

DNS, Extended DNS Errors, Troubleshooting, DNSSEC, Misconfigurations

ACM Reference Format:
Yevheniya Nosyk, Maciej Korczyński, and Andrzej Duda. 2023. Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting. In *Proceedings of the 2023 ACM Internet Measurement Conference (IMC '23), October 24–26, 2023, Montreal, QC, Canada.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3618257.3624835

1 INTRODUCTION

The Domain Name System (DNS) was introduced back in 1987 [54, 55] to translate human-readable domain names into IP addresses. It replaced the static centralized `HOSTS.TXT` text file and distributed the domain name space management across different entities. The original standard accounted for cases when DNS resolutions would go wrong and designated a 4-bit response code (`RCODE`) field in the DNS packet header. Six values were defined directly and the remaining ones were reserved for future use.

With the evolution of DNS, new response codes were gradually added to support dynamic DNS updates [79], DNAME Redirection [68], TSIG [30], DNS Stateful Operations [12], EDNS(0) [23], TKEY [1], and DNS Cookies [4]. These new assignments have further complicated the original semantics of response codes—as all newly added `RCODE`s did not fit the 4-bit field in the packet header, some codes had to be served inside `TSIG`, `TKEY`, and `OPT` resource records. Moreover, the `RCODE` value of 9 has two different meanings depending on whether it was found inside the `OPT` or the `TSIG` record, and the value of 16 was assigned twice by mistake [3].

By the year 2023, the complexity of DNS has drastically increased—it is now defined in 297 RFCs [13] making it more than ever prone to various misconfigurations and resolution failures. As observed in a large passive dataset with 1.6 trillion DNS transactions, only 68.1% of them succeed [34]. The remaining requests would fail due to various reasons, such as non-existing domain names, DNSSEC validation failures, unreachable authoritative nameservers, recursive resolver policies, and others. DNS failures were also behind Slack [33], Salesforce [69], NASA [83], and European Commission [71] website outages. Unfortunately, the generic DNS response codes are of little help to precisely pinpoint the underlying causes of such events.

To address this shortcoming, RFC 8914 introduced Extended DNS Errors—a mechanism to define more specific error codes and return them inside the `OPT` resource record along with a verbose explanation of the problem [52]. The proposed standard defined 25 initial extended error codes (`INFO-CODE`s) and encouraged adding new ones to the registry maintained by IANA [40]. EDE can provide a new unique insight into the state of the DNS ecosystem but no prior work systematically analyzed this new standard. To fill this research gap, this paper aims at analyzing whether one can rely on EDE to efficiently identify the most common reasons behind DNS failures. In particular, our contributions are as follows:

- We set up 63 domain names that reflect common misconfigurations and corner cases. We make our infrastructure publicly available at https://extended-dns-errors.com for the community to use.
- We test the implementation of RFC 8914 by four open-source DNS resolvers (BIND9, Unbound, PowerDNS Recursor, Knot

IMC '23, October 24–26, 2023, Montreal, QC, Canada

ACM ISBN 979-8-4007-0382-9/23/10…$15.00
https://doi.org/10.1145/3618257.3624835

Table 1: Registered Extended DNS Error codes.

Code	Description	Code	Description
0.	Other	15.	Blocked
1.	Unsupported DNSKEY Algorithm	16.	Censored
2.	Unsupported DS Digest Type	17.	Filtered
3.	Stale Answer	18.	Prohibited
4.	Forged Answer	19.	Stale NXDOMAIN Answer
5.	DNSSEC Indeterminate	20.	Not Authoritative
6.	DNSSEC Bogus	21.	Not Supported
7.	Signature Expired	22.	No Reachable Authority
8.	Signature Not Yet Valid	23.	Network Error
9.	DNSKEY Missing	24.	Invalid Data
10.	RRSIGs Missing	25.	Signature Expired before Valid
11.	No Zone Key Bit Set	26.	Too Early
12.	NSEC Missing	27.	Unsupported NSEC3 Iter. Value
13.	Cached Error	28.	Unable to conform to policy
14.	Not Ready	29.	Synthesized

Resolver) and three large public DNS resolvers (Quad9, OpenDNS, Cloudflare DNS). We observe that they do not agree in 94% of test cases, but the differences come from response specificity and the support of specific EDE codes rather than correctness. Cloudflare DNS returns the most specific codes when handling our test domains.

- We perform a large-scale measurement study of 303M domain names using Cloudflare DNS. Out of those, 17.7M domains trigger EDE codes, mostly due to lame delegations and DNSSEC failures.

The rest of the paper is organized as follows. Section 2 discusses the Extended DNS Errors standard and its implementation by software vendors. Section 3 shows how open source DNS software and public resolvers handle our misconfigured domains. Section 4 presents the large-scale analysis of common domain name misconfigurations. We discuss the ethical considerations of this study in Section 5 and the related work in Section 6. We conclude the paper in Section 7.

2 BACKGROUND

The original DNS message format was not extensible to support new protocol features. To overcome this limitation, the EDNS(0) [23] standard introduced the new `OPT` pseudo resource record that can serve a variable number of options. The `OPTION-CODE` of 15 was assigned to EDE. The RFC 8914 proposed standard additionally defined the 16-bit `INFO-CODE` field that stores the newly added error codes and the variable-length `EXTRA-TEXT` field to provide a more verbose description of a problem. Importantly, extended error codes exist independently from traditional `RCODE`s and the standard does not prohibit any combination of the two.

Table 1 presents the currently registered EDE codes—the first 25 directly defined in RFC 8914 and the other 5 added to the IANA registry afterwards. These `INFO-CODE`s cover various aspects of the DNS operation: i) DNSSEC validation (1, 2, 5-12, 25, 27), ii) caching (3, 13, 19, 29), iii) DNS resolver policies (4, 15-18, 20), iv) DNS software operation (14, 21-23), and v) others (0, 24, 26, 28). Any DNS system, whether a recursive resolver, a forwarder, or an authoritative nameserver, can generate, forward, and parse the EDE codes.

Despite being recently introduced as a proposed standard, the EDE already provides the basis for other ongoing work at the IETF [44]. Extended error codes were suggested to be returned in case of unauthorized zone transfer requests [76] or HTTP proxy errors [58]. Furthermore, the DNS Error Reporting draft [7] describes a mechanism for recursive resolvers to signal the authoritative nameservers of encountered resolution failures. Spamhaus implemented the EDE on their DNS Firewall for PowerDNS Recursor to indicate the reasons for blocking [73].

As of May 2023, four major vendors of DNS resolver software, namely BIND9 [45], Unbound [57], PowerDNS Recursor [63], and Knot Resolver [22] have implemented a subset of Extended DNS Errors defined in RFC 8914. Introducing such a new feature requires a non-trivial amount of effort from software developers. BIND9 implemented `INFO-CODE`s related to response policy zones (codes 15-18) and serving stale data (codes 3,4,19) [6]. They are next planning to introduce DNSSEC validation errors [65] and the *No Reachable Authority (22)* [64]. Unbound prioritizes the impact of DNSSEC error codes and, therefore, has implemented all of them [75].

3 TRIGGERING EXTENDED DNS ERRORS

In this section, we describe our testing infrastructure composed of 63 domain names designed to trigger EDE codes supported by DNS software. They also represent some of the common misconfigurations and corner cases. Our setup excludes all the codes that result from specific resolver configurations (e.g., *Blocked (15)* is only returned when the queried domain name is on the resolver's blocklist). We then test the EDE support by four DNS software vendors and three large public DNS resolvers. We make our testing infrastructure publicly available at https://extended-dns-errors.com and encourage fellow researchers to use it in the future.

3.1 Domain Names

Our testing infrastructure relies on two levels of DNS zones: the correctly configured `extended-dns-errors.com` domain and its 63 subdomains, grouped by configuration type and presented in Table 2. Table 3 in Appendix provides further configuration details.

The first subdomain, as its name implies, is valid and serves as a baseline for subsequent testing. Group 2 domains imitate problems with the `DS` record [67]. For example, the `no-ds` subdomain is correctly signed but does not have the corresponding `DS` record published in the parent zone—the type of misconfiguration affecting roughly 30% of DNSSEC-signed domains [18]. Another domain contains undefined cryptographic algorithm numbers [41].

The subdomains in group 3 manipulate DNSSEC signature (`RRSIG`) inception and expiration fields either for all the resource records (RRs) in zone files or only for the `A` record. Note that for signed domain names to validate properly, the `RRSIG` signatures must be valid. The next group of misconfigurations concerns `NSEC3` and `NSEC3PARAM` resource records needed to provide the hashed authenticated denial of existence [8]. The `nsec3-iter-200` is configured correctly, but we have used a very high `NSEC3` iteration count (200) to sign the domain, even though the values above `0` must not be used anymore [36]. The largest misconfiguration group `5` deals with `DNSKEY` resource records, whether serving as Key Signing Keys (KSKs) or Zone Signing Keys (ZSKs).

The subdomain group 6 represents the most common misconfigurations of `AAAA` resource records as discussed by Hendriks et al. [38]. All the `AAAA` glue records of corresponding subdomains at

Table 2: Our custom subdomains grouped by (mis)configuration type.

#	Description	Subdomains
1.	Control subdomain	valid
2.	DS misconfigurations	no-ds, ds-bad-tag, ds-bad-key-algo, ds-unassigned-key-algo, ds-reserved-key-algo, ds-unassigned-digest-algo, ds-bogus-digest-value
3.	RRSIG misconfigurations	rrsig-exp-all, rrsig-exp-a, rrsig-not-yet-all, rrsig-not-yet-a, rrsig-no-all, rrsig-exp-before-all, rrsig-no-a, rrsig-exp-before-a
4.	NSEC3 misconfigurations	nsec3-missing, bad-nsec3-hash, bad-nsec3-next, bad-nsec3-rrsig, nsec3-rrsig-missing, nsec3-iter-200, nsec3param-missing, bad-nsec3param-salt, no-nsec3param-nsec3
5.	DNSKEY misconfigurations	no-zsk, bad-zsk, no-ksk, no-rrsig-ksk, bad-rrsig-ksk, bad-ksk, no-rrsig-dnskey, bad-rrsig-dnskey, no-dnskey-256, no-dnskey-257, no-dnskey-256-257, bad-zsk-algo, unassigned-zsk-algo, reserved-zsk-algo
6.	Invalid AAAA glue records	v6-mapped, v6-multicast, v6-unspecified, v4-hex, v6-unique-local, v6-doc, v6-link-local, v6-localhost, v6-mapped-dep, v6-nat64
7.	Invalid A glues records	v4-private-10, v4-doc, v4-private-172, v4-loopback, v4-private-192, v4-reserved, v4-this-host, v4-link-local
8.	Other	unsigned, ed448, rsamd5, dsa, allow-query-none, allow-query-localhost

the parent (extended-dns-errors.com) zone contain invalid IPv6 addresses and thus, do not point to genuine child nameservers. Similarly, subdomains in group 7 have glue records with special-purpose IPv4 addresses [42].

The domains in group 8 are not misconfigured *per se* but represent some of the corner cases. The unsigned subdomain is not DNSSEC-signed as proven at the parent zone. The next three subdomains are either signed with deprecated (RSA/MD5), not recommended (DSA/SHA1) or the newest (Ed448) cryptographic algorithms. Finally, the two remaining entries have ACLs that restrict the allowed DNS clients.

3.2 Tested Systems

We have set up four recursive DNS resolvers that implement the RFC 8914 standard: BIND 9.19.9, Knot Resolver 5.6.0, Unbound 1.16.2, and PowerDNS Recursor 4.8.2. The latter two require adding special configuration options to return EDE when handling client requests. We have additionally requested ten popular public DNS resolvers [29] to resolve one domain per group from Table 2 and kept the three that support EDE as of May 2023, namely, Cloudflare DNS, Quad9, and OpenDNS.

3.3 Results

Only 4 test cases out of 63 triggered the same results across all the seven tested systems: the no-ds, nsec3-iter-200, unsigned, and valid subdomains did not result in any error condition. The remaining 94% of the cases were handled inconsistently. Table 4 in Appendix provides additional information about the EDE codes returned in each case.

DNSSEC Bogus (6) is a generic INFO-CODE indicating that DNSSEC validation resulted in a bogus state. Given that most of our subdomains are not signed correctly, there is no surprise that we encounter this error code the most frequently. In particular, as NSEC3 resource records could not be properly validated when requesting non-existing subdomains of bad-nsec3-next and bad-nsec3-rrsig, both resulted in EDE 6. Fourteen more test cases triggered either *DNSSEC Bogus (6)* or a more specific *DNSKEY Missing (9)* showing that no DNSKEY at the child zone matched the DS record at the parent. For example, the misconfigurations of ds-bad-tag, bad-zsk, and reserved-zsk-algo imply mismatches between the corresponding keys and digest values. Interestingly, Unbound consistently returned *DNSKEY Missing (9)*, while Knot Resolver indicated a more generic *DNSSEC Bogus (6)* code in the 14 aforementioned cases.

As expected, the expired, not yet valid, and missing RRSIGs mostly resulted in *Signature Expired (7)*, *Signature Not Yet Valid (8)*, and *RRSIGs Missing (10)* errors, respectively. When signatures expire before becoming valid (subdomains rrsig- exp-before-all, rrsig-exp-before-a), resolvers return as many as four different EDEs. However, a new dedicated INFO-CODE *Signature Expired before Valid (25)* was introduced in 2022. Once implemented, it will signal mismatches between inception and expiration fields of DNSSEC signatures.

The domain names signed with unsupported algorithms should be treated as DNSSEC unsigned [66] and return the NOERROR response code. Cloudflare DNS and Knot Resolver additionally include *Unsupported DNSKEY Algorithm (1)* and *Other (0)* extended errors, respectively, the latter accompanied by the EXTRA-TEXT field saying "LSLC: unsupported digest/key". Note that Cloudflare DNS is the only tested system that does not yet support the Ed448 cryptographic algorithm.

The glue records of subdomains in groups 6 and 7 contain special-use IP addresses that do not point to valid authoritative nameservers. Cloudflare DNS indicated the problem using the *No Reachable Authority (22)* error. Interestingly, OpenDNS occasionally returned the *Prohibited (18)* error code, unexpected in this context. We have filed a ticket to OpenDNS support explaining the issue. Finally, the nameservers of the last two domains had ACLs that either did not accept any queries at all (allow-query-none) or only allowed queries originating from the localhost IPs (allow- query-localhost). These two domains resulted in *Forbidden (18)* for OpenDNS and *DNSKEY Missing (9)*, *No Reachable Authority (22)*, and *Network Error (23)* for Cloudflare DNS.

Our test cases triggered 12 unique INFO-CODEs, mostly *DNSSEC Bogus (6)*, *DNSKEY Missing (9)*, and *RRSIGs Missing (10)*. Overall, apart from one unexpected *Prohibited (18)* code generated by OpenDNS, all the EDE codes returned by DNS software and public resolvers were correct. Despite an important difference between the generated EDE codes, they were all helpful to narrow down the list of potential issues with queried domains, some being significantly more precise than others. As such, EDE is an efficient

mechanism to troubleshoot DNS failures. The Cloudflare implementation of RFC 8914 provides the richest feedback on DNS misconfigurations and other related issues (e.g., unreachable authoritative nameservers). Therefore, we have chosen it for the full domain scan described in the next section.

4 MISCONFIGURATIONS IN THE WILD

We have seen what kind of DNS (mis)configurations can trigger recursive resolvers to return EDEs. In this section, we enumerate the most common misconfigurations in the wild.

4.1 Internet-wide Scan

Our input list of domain names contains 488M entries gathered from different sources, including the Centralized Zone Data Service (CZDS) [43], the Tranco list [62], passive DNS data from SIE Europe [70], `.se`, `.nu`, `.ch`, `.li` top-level domain (TLD) zone files accessible via AXFR zone transfers, and Google Certificate Transparency logs [15]. We used `zdns` [46] scanner to generate `A` requests at scale and queried Cloudflare DNS in May 2023. We filter out non-existing domains (resulting in the `NXDOMAIN` response code) and keep 303M registered domains across 1,475 TLDs for further analysis.

4.2 Extended DNS Errors

Overall, more than 17.7M domains triggered one or more EDE codes. Below, we discuss the 14 encountered `INFO-CODE`s and the misconfigurations they indicate:

1. No Reachable Authority (13,965,865 domains): the issue that affects the largest number of registered domain names. Lame delegation [59] occurs when some or all nameservers cannot provide responses for domains they are authoritative for (despite referrals being present at the parent zone). When none of the nameservers is responsive, end clients would only receive a generic `SERVFAIL` response code, but Cloudflare DNS adds the *No Reachable Authority (22)* EDE code. It was mostly returned along with other `INFO-CODE`s discussed below such as *Network Error (23)*, *DNSKEY Missing (9)*, and *RRSIGs Missing (10)*.

2. Network Error (11,647,551 domains): indicates that it is not possible to communicate with another DNS server due to an unrecoverable error. Cloudflare DNS uses the `EXTRA-TEXT` field of the DNS packet to specify the nameserver triggering the error (e.g., "1.2.3.4:53 rcode=REFUSED for a.com A"). Overall, Cloudflare DNS identified three types of issues with 293k unique authoritative nameservers when requesting `A`, `AAAA`, `NS`, `DS`, or `DNSKEY` RRs. The majority of nameservers responded to Cloudflare with the `REFUSED` `RCODE` (267k), others with `SERVFAIL` (21k), and the remaining ones timed out (15k). In most cases (97.91%), the nameservers of queried domains were the cause of the problem. Other 2.1k child domains were affected because of 88 parent DNS zones and the remaining 241k cases were, for example, unreachable DNS provider domains. We observe a high concentration of domain names per malfunctioning authoritative nameservers—6 of them responding with the `REFUSED` error code are authoritative for more than 100k domains each. Overall, fixing 20k nameservers would render reachable more than 81% of domain names.

Network Error (23) is another evidence of lame delegations along with the above-mentioned *No Reachable Authority (22)*. In total, more than 14.8M unique domains triggered a combination of these two EDE codes. We note, however, that it is the lower bound estimation of the problem—one would need to test all the domain nameservers to confirm whether all of them are available. In our scanning setup, a recursive resolver would end the DNS resolution process once the response is obtained from any authoritative nameserver.

3. RRSIGs Missing (2,746,604 domains): returned when the recursive resolver cannot obtain all the signatures needed for DNSSEC validation. Most of these errors were triggered by 2.47M domain names under two ccTLDs. Surprisingly, the error did not lead to DNSSEC validation failure. We reached out to one of the TLD operators who explained to us that despite the TLD zone being correctly configured, Cloudflare DNS signaled the problem with a so-called stand-by KSK, i.e., the one published in the zone file in case the emergency key rollover is needed, but not actively used to establish the chain of trust [51]. We identified 22 more public suffixes and TLDs with stand-by DNSSEC keys triggering the same error. We contacted Cloudflare and reported our findings. They, in turn, confirmed that it was an expected behavior and updated their documentation [21] to inform that "key rollover in-progress, stand-by key, and attacker stripping signatures" may trigger the RRSIGs Missing EDEs.

4. DNSKEY Missing (296,643 domains): refers to those cases when the `DS` record found at the parent zone does not match any `DNSKEY` at the child zone. Despite its name, this error condition does not necessarily imply that no public key was found at the child zone. In some cases, when accompanied by the *No Reachable Authority (22)*, it states that nameservers were not reachable, so the resolver could not obtain the `DNSKEY` resource record. More broadly, as defined in the RFC 8914, the *DNSKEY Missing (9)* refers to the cases for which the child `DNSKEY` was not cryptographically verified with respect to the `DS` record. Almost all the affected domains failed the DNSSEC validation due to the same reason—no `RRSIG` RRs covered KSKs in the child zone, even though `DNSKEY`s corresponded to `DS` records found at the parent.

5. DNSSEC Bogus (82,465 domains): DNSSEC validation results in a bogus state when validating resolvers cannot cryptographically establish the chain of trust from the root to the requested zone. More than 80k domain names resulted in the `SERVFAIL` response code because 124 corresponding TLDs did not provide valid proofs of non-existence for the `A` records queried during our Internet-wide scan. Other encountered problems include `RRSIG` records that do not validate corresponding `DNSKEY/A` RRs, `DS` hashes that do not match corresponding KSKs, etc.

6. Invalid Data (12,268 domains): this group of domains contained responses with the "Mismatched question from the authoritative server <ip>" `EXTRA-TEXT`. For example, nameservers that do not implement EDNS0 would not respond with the `FORMERR` response code as specified in RFC 6891 [23] but rather did not include the `OPT` record in the response.

7. Unsupported DNSKEY Algorithm (8,751 domains): validating DNS resolvers ignore `DNSKEY`s with unknown algorithms, as generated signatures cannot be cryptographically verified. Cloudflare DNS signaled that it does not support GOST R 34.10-2001 and

Ed448 algorithms. Additionally, we received the "unsupported key size" EXTRA-TEXT for the domains that have 512-bit keys of types RSA/SHA-1, RSASHA1-NSEC3-SHA1, and RSA/SHA-256. Despite the fact that the key length is explicitly allowed in the corresponding specifications [2, 47], the keys are now considered weak. Finally, we received the "no supported DNSKEY algorithm" EXTRA-TEXT in two cases: i) when using prohibited DNSSEC algorithms (e.g., DSA-NSEC3-SHA1 or DSA) and ii) when the DS record at the parent corresponds to the key tag of the DNSKEY record in the child zone, but the algorithm numbers do not match. In particular, one domain name deliberately misconfigured by fellow researchers had a reserved DNSKEY algorithm number.

8. Signature Expired (2,877 domains): validating resolvers examine the Signature Expiration field of RRSIG RRs to check whether they can still be used to build the chain of trust. Cloudflare DNS revealed that certain signatures expired sometime between 2009 and our measurement (2019 for one research domain name deliberately misconfigured). Interestingly, in some cases, the domain name of the authoritative nameserver contains expired RRSIG resource records, rather than the queried domain name itself. For example, the resolution of 377 domains resulted in SERVFAIL because the domain name of the DNS provider contained expired signatures.

9. NSEC Missing (1,980 domains): signifies that no valid proof of non-existence was returned in the response. For example, the domains in this category had missing NSEC/NSEC3 records to validate the absence of DS records at the parent zone or the absence of the A record at the child zone. The message stating "failed to verify an insecure referral proof for <domain>" was added to all the errors.

10. Unsupported DS Digest Type (62 domains): IANA allows two mandatory and two optional algorithms to compute DS digest values [39]. As Cloudflare DNS does not support the optional GOST R 34.11-94 algorithm yet, we received this extended error code when resolving 54 domains. As for the remaining 8 domains with the nameservers managed by one DNS provider, their corresponding DS records contained an unassigned digest algorithm type (8).

11. Stale Answer (32 domains): the resolver responded with the previously cached data. In particular, 6 domains had the *Stale Answer (3)* response with *No Reachable Authority (22)* and *Network error (23)*, because nameservers responded with the REFUSED RCODE. Other 12 domains resulted in the combination of *Stale Answer (3)* and *No Reachable authority (22)*, as nameservers would not respond to resolver queries.

12. Signature Not Yet Valid (29 domains): apart from one domain name deliberately misconfigured by researchers from another organisation, the remaining 28 have two pairs of DNSSEC signatures: valid and those that will be valid starting from year 2045. Consequently, the resolution of these domains is inconsistent—NOERROR when valid signatures are returned and SERVFAIL otherwise. Interestingly, the nameserver domains themselves experience the same problem.

13. Cached Error (8 domains): means that the resolver returned SERFVAIL responses directly from its cache, possibly after previously failed resolution attempts. The authoritative nameservers of all the 8 domains respond to resolver queries with NOTAUTH RCODE, unexpected in this context as it must only be generated when processing the client TSIG record. We repeated the resolution attempts from various locations worldwide, but the problem persisted.

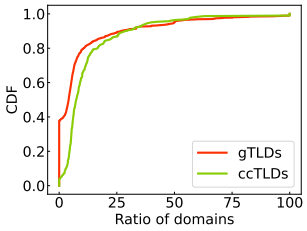

Figure 1: The ratio of domains that trigger EDE codes across gTLDs and ccTLDs.

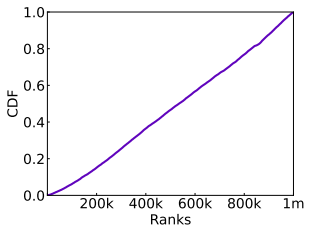

Figure 2: The distribution of domains that trigger EDE codes across the Tranco list.

14. Other (7 domains): this error code was received with the "iteration limit exceeded" EXTRA-TEXT and resulted in SERVFAIL for all the domains. Interestingly, one did not have any DNS-specific misconfigurations and was successfully resolved using Google DNS, Quad9, and OpenDNS. The remaining 6 have authoritative nameservers responding with REFUSED for non-recursive queries from recursive resolvers.

4.3 Concentration of Misconfigurations

We now investigate the distribution of misconfigured domain names per TLD. We compute the ratio of the domains that trigger extended error codes to all domains scanned per TLD and present the results in Figure 1. Overall, almost 38% of gTLDs and 4% of ccTLDs do not have any misconfigured domain. At the other extreme, all the registered domains under 11 gTLDs and 2 ccTLDs resulted in extended error codes, mostly *RRSIGs Missing (10)*, *No Reachable Authority (22)*, and *Network Error (23)*. We note that these TLDs accounted for a mere fraction of our input list, totaling 108k domains. Although we observe that ccTLDs are generally more likely to have misconfigured domain names than gTLDs, it also indicates the efforts of ccTLD registries to deploy DNSSEC and comply with best current practices.

We then assess the popularity of domains that trigger EDE codes. Misconfigurations of popular domains can have far-reaching consequences because many end users rely on them. We compared the Tranco top 1M ranking [62] with our list of 17.7M domains. Overall, 22.1k entries were in common. As further shown in Figure 2, the domains triggering EDE codes are evenly distributed across the Tranco list. We also note that 12.2k domains resulted in the NOERROR response code, suggesting that Cloudflare DNS did not encounter any unrecoverable errors, but rather used EDE to provide more information about the DNS resolutions.

5 ETHICS AND REPRODUCIBILITY

Our research uses active network measurements and follows industry best practices [26, 32, 61]. The Cloudflare public DNS resolver receives around 600 billion requests per day or almost 7 million per second [19]. The traffic generated for our experiment peaked at 11.5K packets per second and lasted for 12 hours in total. Moreover, The Cloudflare Terms of Use [20] do not limit the number of

requests per client and we did not see evidence to have triggered any rate limiting. As Cloudflare DNS functions as a caching resolver, we anticipate a portion of our requests to be resolved from its internal cache. We randomized our input list to spread the load across different authoritative nameservers and we did not reveal misconfigurations of individual domains to protect their owners. When probing open resolvers, we only targeted ten large public systems meant to resolve queries from arbitrary clients.

Finally, we release all the tools necessary to reproduce our study at https://extended-dns-errors.com. They include i) the list of misconfigured domains that we host and can be freely queried, ii) instructions on how to set up all the misconfigured domains, iii) instructions on how to set up recursive resolvers supporting EDE, and iv) instructions on how to run our domain scans.

6 RELATED WORK

Despite ongoing efforts to improve DNS availability and resiliency, domain misconfigurations persist [14, 24]. Pappas et al. [60] highlighted cyclic dependencies, lame delegation, and insufficient server redundancy as prevalent issues in 2004. These problems still exist today [56, 72]. Lame delegation affects a significant number of domains [5], including 14.8 million identified in our research. DNSSEC deployment and IPv6 adoption have introduced additional types of mismanagement [18, 37, 38, 74, 77, 80].

Domain misconfigurations lead to erroneous DNS resolutions [53]. Failure rates range from 13.5% to 19% based on studies in different regions [34, 50, 82]. Moreover, most of the requests at DNS root servers are "pollution" queries (e.g., non-existing TLDs, malformed packets) [16, 17, 35, 81], leading to resolution failures. To address the extent of erroneous DNS in the wild, the IETF released RFCs and Best Current Practice documents discussing most common misconfigurations [9–11, 25, 31]. Methods for formal verification and online tools like DNSViz, DNSSEC Analyzer, and DNS Checker help in the analysis [27, 28, 48, 49, 59, 78].

The present work explores the use of EDE codes with a novel approach to troubleshooting name resolution problems that relies on the DNS protocol itself and does not require installing any external tools.

7 CONCLUSIONS

In this paper, we have provided the first analysis of how EDE helps in troubleshooting DNS problems at scale. We set up 63 domains and tested the implementation of RFC 8914 by four DNS software vendors and three public DNS resolvers. The results reveal high inconsistency between tested systems—almost 94% of test cases. We have also scanned 303M domains using Cloudflare DNS and identified that 17.7M (5.8%) of them trigger EDE codes, showing that decades-long problems of lame delegations and DNSSEC misconfigurations remain widely present.

The high level of inconsistency in returned EDE codes may raise the question of how useful they are when troubleshooting DNS problems. Our measurements reveal that all the tested systems were successful in determining root causes of misconfigurations with different levels of specificity. Therefore, we believe that EDE is a promising technique that assists DNS operators, domain owners, and end clients in identifying and resolving DNS issues. Further discussions with the community, software vendors, and public resolver operators may increase result consistency and the ease of the EDE interpretation for all involved parties.

ACKNOWLEDGMENTS

This work has been partially supported by Carnot LSI and Grenoble Alpes Cybersecurity Institute (under the contract ANR-15-IDEX-02), the French Ministry of Research projects PERSYVAL-Lab under contract ANR-11-LABX-0025-01 and DiNS under contract ANR-19-CE25-0009-01.

REFERENCES

[1] Donald E. Eastlake 3rd. 2000. Secret Key Establishment for DNS (TKEY RR). RFC 2930. (2000).
[2] Donald E. Eastlake 3rd. 2001. RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS). (May 2001).
[3] Donald E. Eastlake 3rd. 2013. Domain Name System (DNS) IANA Considerations. RFC 6895. (2013).
[4] Donald E. Eastlake 3rd and Mark P. Andrews. 2016. Domain Name System (DNS) Cookies. RFC 7873. (2016).
[5] Gautam Akiwate, Mattijs Jonker, Raffaele Sommese, Ian Foster, Geoffrey M. Voelker, Stefan Savage, and KC Claffy. 2020. Unresolved Issues: Prevalence, Persistence, and Perils of Lame Delegations. In *IMC*. Association for Computing Machinery, New York, NY, USA, 281–294.
[6] Mark Andrews. 2020. Return Extended EDNS Errors (EDE). https://gitlab.isc.org/isc-projects/bind9/-/issues/1836. (May 2020).
[7] Roy Arends and Matt Larson. 2023. *DNS Error Reporting*. Internet-Draft draft-ietf-dnsop-dns-error-reporting-04. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-dnsop-dns-error-reporting/04/ Work in Progress.
[8] Roy Arends, Geoffrey Sisson, David Blacka, and Ben Laurie. 2008. DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. RFC 5155. (2008).
[9] Piet Barber and Matt Larson. 2006. Observed DNS Resolution Misbehavior. RFC 4697. (2006).
[10] David Barr. 1996. Common DNS Operational and Configuration Errors. RFC 1912. (1996).
[11] Piet Beertema. 1993. Common DNS Data File Configuration Errors. RFC 1537. (1993).
[12] Ray Bellis, Stuart Cheshire, John Dickinson, Sara Dickinson, Ted Lemon, and Tom Pusateri. 2019. DNS Stateful Operations. RFC 8490. (2019).
[13] Bert Hubert. 2023. Overview of relevant DNS standards and drafts. https://powerdns.org/dns-camel/. (Feb. 2023).
[14] Petar D. Bojović and Slavko Gajin. 2017. An approach to evaluation of common DNS misconfigurations. (2017). https://doi.org/10.48550/ARXIV.1711.05696
[15] Cali Dog Security. 2022. Certstream. (March 2022). https://calidog.io.
[16] Sebastian Castro, Duane Wessels, Marina Fomenkov, and Kimberly Claffy. 2008. A Day at the Root of the Internet. *SIGCOMM Comput. Commun. Rev.* 38, 5 (sep 2008), 41–46.
[17] Sebastian Castro, Min Zhang, Wolfgang John, Duane Wessels, and Kimberly Claffy. 2010. Understanding and Preparing for DNS Evolution. In *TMA*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1–16.
[18] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. A Longitudinal, End-to-End View of the DNSSEC Ecosystem. In *USENIX Security*. USENIX Association, Vancouver, BC, 1307–1322.
[19] Cloudflare. 2022. Announcing experimental DDR in 1.1.1.1. https://blog.cloudflare.com/announcing-ddr-support/. (March 2022).
[20] Cloudflare. 2023. Cloudflare Website and Online Services Terms of Use. https://www.cloudflare.com/website-terms/. (May 2023).
[21] Cloudflare. 2023. Extended DNS error codes. https://developers.cloudflare.com/1.1.1.1/infrastructure/extended-dns-error-codes/. (Sept. 2023).
[22] CZ.NIC. 2023. Knot Resolver. https://gitlab.nic.cz/knot/knot-resolver. (Feb. 2023).
[23] Joao da Silva Damas, Michael Graff, and Paul A. Vixie. 2013. Extension Mechanisms for DNS (EDNS(0)). RFC 6891. (2013).
[24] Tianxiang Dai, Haya Shulman, and Michael Waidner. 2016. DNSSEC Misconfigurations in Popular Domains. In *CANS*. Springer International Publishing, Cham, 651–660.
[25] Peter B. Danzig, Anant Kumar, Steve Miller, Clifford Neuman, and Jon Postel. 1993. Common DNS Implementation Errors and Suggested Fixes. RFC 1536. (1993).
[26] D Dittrich and E Kenneally. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://catalog.caida.org/paper/2012_menlo_report_actual_formatted. (2012).

[27] DNS Checker. 2023. Domain DNS Health Checker Tool. https://dnschecker.org/domain-health-checker.php. (March 2023).

[28] DNSViz. 2023. A DNS visualization tool. https://dnsviz.net. (Feb. 2023).

[29] Trinh Viet Doan, Justus Fries, and Vaibhav Bajpai. 2021. Evaluating Public DNS Services in the Wake of Increasing Centralization of DNS. In *IFIP Networking*. IEEE.

[30] Francis Dupont, Stephen Morris, Paul A. Vixie, Donald E. Eastlake 3rd, Ólafur Guðmundsson, and Brian Wellington. 2020. Secret Key Transaction Authentication for DNS (TSIG). RFC 8945. (2020).

[31] Alain Durand, Johan Stenstam, and Pekka Savola. 2006. Operational Considerations and Issues with IPv6 DNS. RFC 4472. (2006).

[32] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-Wide Scanning and Its Security Applications. In *USENIX Security*. USENIX Association, Washington, D.C., 605–620.

[33] Rafael Elvira. 2022. The Case of the Recursive Resolvers. https://slack.engineering/what-happened-during-slacks-dnssec-rollout/. (2022).

[34] Paweł Foremski, Oliver Gasser, and Giovane C. M. Moura. 2019. DNS Observatory: The Big Picture of the DNS. In *IMC*. Association for Computing Machinery, New York, NY, USA, 87–100.

[35] Hongyu Gao, Vinod Yegneswaran, Yan Chen, Phillip Porras, Shalini Ghosh, Jian Jiang, and Haixin Duan. 2013. An Empirical Reexamination of Global DNS Behavior. In *SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 267–278.

[36] Wes Hardaker and Viktor Dukhovni. 2022. Guidance for NSEC3 Parameter Settings. RFC 9276. (2022).

[37] Elias Heftrig, Haya Shulman, and Michael Waidner. 2022. Poster: The Unintended Consequences of Algorithm Agility in DNSSEC. In *CCS*. Association for Computing Machinery, New York, NY, USA, 3363–3365.

[38] Luuk Hendriks, Pieter-Tjerk de Boer, and Aiko Pras. 2017. IPv6-specific misconfigurations in the DNS. In *CNSM*. IEEE Computer Society, Los Alamitos, CA, USA, 1–5.

[39] IANA. 2023. DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms. https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml. (May 2023).

[40] IANA. 2023. Domain Name System (DNS) Parameters (Extended DNS Error Codes). https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#extended-dns-error-codes. (Feb. 2023).

[41] IANA. 2023. Domain Name System Security (DNSSEC) Algorithm Numbers. https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml. (April 2023).

[42] IANA. 2023. IANA IPv4 Special-Purpose Address Registry. https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml. (April 2023).

[43] ICANN. 2022. Centralized Zone Data Service. (March 2022). https://czds.icann.org.

[44] IETF. 2023. References to rfc8914. https://datatracker.ietf.org/doc/rfc8914/referencedby/. (March 2023).

[45] Internet Systems Consortium. 2023. BIND. https://gitlab.isc.org/isc-projects/bind9. (April 2023).

[46] Liz Izhikevich, Gautam Akiwate, Briana Berger, Spencer Drakontaidis, Anna Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. ZDNS: A Fast DNS Toolkit for Internet Measurement. In *IMC*. Association for Computing Machinery, New York, NY, USA, 33–43.

[47] Jelte Jansen. 2009. Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. RFC 5702. (2009).

[48] Siva Kesava Reddy Kakarla, Ryan Beckett, Behnaz Arzani, Todd Millstein, and George Varghese. 2020. GRooT: Proactive Verification of DNS Configurations. In *SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 310–328.

[49] Siva Kesava Reddy Kakarla, Ryan Beckett, Todd Millstein, and George Varghese. 2022. SCALE: Automatically Finding RFC Compliance Bugs in DNS Nameservers. In *NSDI*. USENIX Association, Renton, WA, 307–323.

[50] Yuta Kazato, Kensuke Fukuda, and Toshiharu Sugawara. 2013. Towards Classification of DNS Erroneous Queries. In *AIEC*. Association for Computing Machinery, New York, NY, USA, 25–32.

[51] Olaf Kolkman, Matthijs Mekking, and R. (Miek) Gieben. 2012. DNSSEC Operational Practices, Version 2. RFC 6781. (2012).

[52] Warren "Ace" Kumari, Evan Hunt, Roy Arends, Wes Hardaker, and David C Lawrence. 2020. Extended DNS Errors. RFC 8914. (Oct. 2020).

[53] Xianran Liao, Jiacen Xu, Qifan Zhang, and Zhou Li. 2022. A Comprehensive Study of DNS Operational Issues by Mining DNS Forums. *IEEE Access* 10 (2022), 110807–110820.

[54] Paul Mockapetris. 1987. Domain names - concepts and facilities. RFC 1034. (1987).

[55] Paul Mockapetris. 1987. Domain names - implementation and specification. RFC 1035. (1987).

[56] Giovane CM Moura, Sebastian Castro, John Heidemann, and Wes Hardaker. 2021. TsuNAME: Exploiting Misconfiguration and Vulnerability to DDoS DNS. In *IMC*. Association for Computing Machinery, New York, NY, USA, 398–418.

[57] NLnetLabs. 2023. Unbound. https://github.com/NLnetLabs/unbound. (Feb. 2023).

[58] Mark Nottingham and Piotr Sikora. 2022. The Proxy-Status HTTP Response Header Field. RFC 9209. (2022).

[59] Vasileios Pappas, Patrik Fältström, Daniel Massey, and Lixia Zhang. 2004. Distributed DNS Troubleshooting. In *NetT*. Association for Computing Machinery, New York, NY, USA, 265–270.

[60] Vasileios Pappas, Zhiguo Xu, Songwu Lu, Daniel Massey, Andreas Terzis, and Lixia Zhang. 2004. Impact of Configuration Errors on DNS Robustness. *SIGCOMM Comput. Commun. Rev.* 34, 4 (aug 2004), 319–330.

[61] Craig Partridge and Mark Allman. 2016. Ethical Considerations in Network Measurement Papers. *Commun. ACM* 59, 10 (sep 2016), 58–64. https://doi.org/10.1145/2896816

[62] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *NDSS*. The Internet Society, Reston, The USA.

[63] PowerDNS.COM BV. 2023. pdns. https://github.com/PowerDNS/pdns. (Feb. 2023).

[64] Vicky Risk. 2020. RFC 8914 - Extended error for No Reachable Authority. https://gitlab.isc.org/isc-projects/bind9/-/issues/2268. (Nov. 2020).

[65] Vicky Risk. 2021. RFC 8914 - DNSSEC validation failures. https://gitlab.isc.org/isc-projects/bind9/-/issues/2715. (May 2021).

[66] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. Protocol Modifications for the DNS Security Extensions. RFC 4035. (2005).

[67] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. Resource Records for the DNS Security Extensions. RFC 4034. (2005).

[68] Scott Rose and Wouter Wijngaards. 2012. DNAME Redirection in the DNS. RFC 6672. (2012).

[69] Salesforce. 2021. Multi-Instance Service Disruption on May 11-12, 2021. https://help.salesforce.com/s/articleView?id=000390251&type=1. (17 08 2021).

[70] SIE Europe. 2022. Passive DNS Data Sharing. (March 2022). https://www.sie-europe.net.

[71] Laura Smith. 2021. Anyone else seeing DNSSEC failures from EU Commission ? (european-union.europa.eu). https://seclists.org/nanog/2021/Dec/94. (08 12 2021).

[72] R Sommese, G Moura, M Jonker, R Van Rijswijk-Deij, A Dainotti, k claffy, and A Sperotto. 2020. When Parents and Children Disagree: Diving into DNS Delegation Inconsistency. In *PAM*. Springer International Publishing, Cham, 175–189.

[73] Spamhaus technology. 2023. DNS Firewall for PowerDNS. https://docs.spamhaus.com/dns-firewall/docs/source/configuration/power_dns_config.html. (Feb. 2023).

[74] Florian Streibelt, Patrick Sattler, Franziska Lichtblau, Carlos H. Gañán, Anja Feldmann, Oliver Gasser, and Tobias Fiebig. 2023. How Ready is DNS for an IPv6-Only World?. In *PAM*. Springer Nature Switzerland, Cham, 525–549.

[75] Team NLnet Labs. 2022. Extended DNS Error support for Unbound. https://blog.nlnetlabs.nl/extended-dns-error-support-for-unbound/. (June 2022).

[76] Willem Toorop, Sara Dickinson, Shivan Kaul Sahib, Pallavi Aras, and Allison Mankin. 2021. DNS Zone Transfer over TLS. RFC 9103. (Aug. 2021).

[77] Niels L. M. van Adrichem, Norbert Blenn, Antonio Reyes Lúa, Xin Wang, Muhammad Wasif, Ficky Fatturrahman, and Fernando A. Kuipers. 2015. A Measurement Study of DNSSEC Misconfigurations. *Security Informatics* 4, 1 (19 Oct 2015), 8.

[78] VERISIGN Labs. 2023. DNSSEC Analyzer. https://dnssec-analyzer.verisignlabs.com. (Feb. 2023).

[79] Paul A. Vixie, Susan Thomson, Yakov Rekhter, and Jim Bound. 1997. Dynamic Updates in the Domain Name System (DNS UPDATE). RFC 2136. (1997).

[80] Matthäus Wander. 2017. Measurement Survey of Server-side DNSSEC Adoption. In *TMA*. IEEE.

[81] D Wessels and M Fomenkov. 2003. Wow, That's a Lot of Packets. In *PAM*.

[82] Donghui Yang, Zhenyu Li, and Gareth Tyson. 2020. A Deep Dive into DNS Query Failures. In *USENIX ATC*. USENIX Association, USA, 507–514.

[83] Dan York. 2012. Comcast Releases Detailed Analysis of NASA.gov DNSSEC Validation Failure. https://www.internetsociety.org/blog/2012/01/comcast-releases-detailed-analysis-of-nasa-gov-dnssec-validation-failure/. (25 01 2012).

A TESTING INFRASTRUCTURE

Table 3: Configuration details of each subdomain.

Subdomain	Configuration
valid	The correctly configured control domain
no-ds	The subdomain is correctly signed but no DS record was published at the parent zone
ds-bad-tag	The key tag field of the DS record at the parent zone does not correspond to the KSK DNSKEY ID at the child zone
ds-bad-key-algo	The algorithm field of the DS record at the parent zone does not correspond to the KSK DNSKEY algorithm at the child zone
ds-unassigned-key-algo	The algorithm value of the DS record at the parent zone is unassigned (100)
ds-reserved-key-algo	The algorithm value of the DS record at the parent zone is reserved (200)
ds-unassigned-digest-algo	The digest algorithm value of the DS record at the parent zone is unassigned (100)
ds-bogus-digest-value	The digest value of the DS record at the parent zone does not correspond to the KSK DNSKEY at the child zone
rrsig-exp-all	All the RRSIG records are expired
rrsig-exp-a	The RRSIG over A RRset is expired
rrsig-not-yet-all	All the RRSIG records are not yet valid
rrsig-not-yet-a	The RRSIG over A RRset is not yet valid
rrsig-no-all	All the RRSIGs were removed from the zone file
rrsig-no-a	The RRSIG over A RRset was removed from the zone file
rrsig-exp-before-all	All the RRSIGs expired before the inception time
rrsig-exp-before-a	The RRSIG over A RRset expired before the inception time
nsec3-missing	All the NSEC3 records were removed from the zone file
bad-nsec3-hash	Hashed owner names were modified in all the NSEC3 records
bad-nsec3-next	Next hashed owner names were modified in all the NSEC3 records
bad-nsec3-rrsig	RRSIGs over NSEC3 RRsets are bogus
nsec3-rrsig-missing	RRSIGs over NSEC3 RRsets were removed from the zone file
nsec3param-missing	NSEC3PARAM resource record was removed from the zone file
bad-nsec3param-salt	The salt value of the NSEC3PARAM resource record is wrong
no-nsec3param-nsec3	NSEC3 and NSECPARAM resource records were removed from the zone file
nsec3-iter-200	NSEC3 iteration count is set to 200
no-zsk	The ZSK DNSKEY was removed from the zone file
bad-zsk	The ZSK DNSKEY resource record is wrong
no-ksk	The KSK DNSKEY was removed from the zone file
no-rrsig-ksk	The RRSIG over KSK DNSKEY was removed from the zone file
bad-rrsig-ksk	The RRSIG over KSK DNSKEY is wrong
bad-ksk	The KSK DNSKEY is wrong
no-rrsig-dnskey	All the RRSIGs over DNSKEY RRsets were removed from the zone file
bad-rrsig-dnskey	All the RRSIGs over DNSKEY RRsets are wrong
no-dnskey-256	The Zone Key Bit is set to 0 for the ZSK DNSKEY
no-dnskey-257	The Zone Key Bit is set to 0 for the KSK DNSKEY
no-dnskey-256-257	The Zone Key Bit is set to 0 for both the KSK DNSKEY and ZSK DNSKEY
bad-zsk-algo	The ZSK DNSKEY algorithm number is wrong
unassigned-zsk-algo	The ZSK DNSKEY algorithm number is unassigned (100)
reserved-zsk-algo	The ZSK DNSKEY algorithm number is reserved (200)
v6-mapped	The AAAA glue record at the parent zone is an IPv6-mapped IPv4 address
v6-unspecified	The AAAA glue record at the parent zone is an unspecified address
v4-hex	The AAAA glue record at the parent zone is an IPv4 address in hex form
v6-link-local	The AAAA glue record at the parent zone is a link local address
v6-localhost	The AAAA glue record at the parent zone is a localhost
v6-mapped-dep	The AAAA glue record at the parent zone is a deprecated IPv6-mapped IPv4 address
v6-doc	The AAAA glue record at the parent zone is from the documentation range
v6-unique-local	The AAAA glue record at the parent zone is from a unique local address
v6-nat64	The AAAA glue record at the parent zone is used for NAT64
v6-multicast	AAAA The glue record at the parent zone is from a multicast range
v4-private-10	The A glue record at the parent zone is a private address
v4-private-172	The A glue record at the parent zone is a private address
v4-private-192	The A glue record at the parent zone is a private address
v4-this-host	The A glue record at the parent zone is a 0.0.0.0
v4-loopback	The A glue record at the parent zone is a loopback address
v4-link-local	A The glue record at the parent zone is a link-local address
v4-doc	The A glue record at the parent zone is a documentation address
v4-reserved	The A glue record at the parent zone is a reserved address
unsigned	The domain name is not signed with DNSSEC
ed448	The zone is signed with ED448 algorithm
rsamd5	The zone is signed with RSAMD5 algorithm
dsa	The zone is signed with DSA algorithm
allow-query-none	Nameserver does not accept queries for the subdomain
allow-query-localhost	Nameserver only accepts queries from the localhost

B TESTING RESULTS

Table 4: Subdomains and extended error codes returned by DNS software and public resolvers.

#	Subdomain	BIND 9.19.9	Unbound 1.16.2	PowerDNS 4.8.2	Knot 5.6.0	Cloudflare DNS	Quad9	OpenDNS
1.	valid	None	None	None	None	None	None	None
2.	no-ds	None	None	None	None	None	None	None
3.	ds-bad-tag	None	9	9	6	9	9	6
4.	ds-bad-key-algo	None	9	9	6	9	9	6
5.	ds-unassigned-key-algo	None	None	None	0	9	None	6
6.	ds-reserved-key-algo	None	None	None	0	1	None	6
7.	ds-unassigned-digest-algo	None	None	None	0	2	None	None
8.	ds-bogus-digest-value	None	9	9	6	6	9	6
9.	rrsig-exp-all	None	7	7	7	7	7	6
10.	rrsig-exp-a	None	6	7	None	7	6	7
11.	rrsig-not-yet-all	None	9	8	8	8	9	6
12.	rrsig-not-yet-a	None	6	8	None	8	8	8
13.	rrsig-no-all	None	10	10	10	10	9	6
14.	rrsig-no-a	None	10	10	10	10	10	None
15.	rrsig-exp-before-all	None	9	7	7	10	9	6
16.	rrsig-exp-before-a	None	6	7	None	7	7	7
17.	nsec3-missing	None	12	None	12	6	None	12
18.	bad-nsec3-hash	None	6	None	6	6	6	12
19.	bad-nsec3-next	None	6	None	6	6	6	6
20.	bad-nsec3-rrsig	None	6	None	6	6	None	6
21.	nsec3-rrsig-missing	None	12	None	10	6	9	12
22.	nsec3param-missing	None	10	10	10	10	9	6
23.	bad-nsec3param-salt	None	12	None	12	6	9	12
24.	no-nsec3param-nsec3	None	10	10	10	10	10	6
25.	nsec3-iter-200	None	None	None	None	None	None	None
26.	no-zsk	None	9	6	6	6	9	6
27.	bad-zsk	None	9	6	6	6	6	6
28.	no-ksk	None	9	9	6	9	9	6
29.	no-rrsig-ksk	None	10	9	6	10	9	6
30.	bad-rrsig-ksk	None	9	6	6	6	6	6
31.	bad-ksk	None	9	9	6	9	9	6
32.	no-rrsig-dnskey	None	10	10	10	10	9	6
33.	bad-rrsig-dnskey	None	9	6	6	6	9	6
34.	no-dnskey-256	None	9	6	6	6	9	6
35.	no-dnskey-257	None	9	9	6	9	9	6
36.	no-dnskey-256-257	None	9	10	10	9	10	6
37.	bad-zsk-algo	None	9	6	6	6	6	6
38.	unassigned-zsk-algo	None	9	6	6	6	9	6
39.	reserved-zsk-algo	None	9	6	6	6	6	6
40-49.	v6-mapped, v6-multicast, v6-unspecified, v4-hex, v6-unique-local, v6-doc, v6-link-local, v6-localhost, v6-mapped-dep, v6-nat64	None	None	None	None	22	None	None
50-57.	v4-private-10, v4-doc, v4-private-172, v4-loopback, v4-private-192, v4-reserved, v4-this-host, v4-link-local	None	None	None	None	22	None	None
58.	unsigned	None	None	None	None	None	None	None
59.	ed448	None	None	None	None	1	None	None
60.	rsamd5	None	None	None	0	1	None	None
61.	dsa	None	None	None	0	1	None	None
62.	allow-query-none	None	None	None	None	9,22,23	None	18
63.	allow-query-localhost	None	None	None	None	9,22,23	None	18