The TLDr on TLDs

What happens when Top Level Domains leave the lights on with nobody home

HushCon East 2022
$ whoami

- Ian Foster
- DNS Researcher/Historian
  - Certgraph
  - BygoneSSL
  - dns.coffee
- Way too interested in DNS & TLS
- Red Team Lead @ Snap
- @LANRAT
TLD what?

Top-level domain (TLD) refers to the last segment of a domain name, or the part that follows immediately after the "dot" symbol.

Common TLDs include:

- gTLDs: com, net, org, info, ...
- ccTLDs: io, co.uk, us, ...
- Sponsored: aero, gov, mil, edu, tel
- Infra:arpa

For example, the domain www.hushcon.com is in the com zone.

TLDs operate just like domains with subdomains.
How Does DNS work?

https://wizardzines.com/comics/life-of-a-dns-query/
How Does DNS work?

https://wizardzines.com/comics/life-of-a-dns-query/
ICANN Requirements

- ICANN sets requirements[1] that a TLD operator must follow to continue being included in the root zone
  - ICANN can take over a TLD for non-compliance
    - Ex: .wed
- ccTLDs are excluded from these requirements[2]

TLD Compromises

- TLDs can be compromised, just like any other domain
  - .io [1]
    - Lame delegations
    - Partial compromise
  - .ao & .na [2]
    - Lame delegations
    - Partial compromise
  - .cd [3]
    - SQLi in TLD registry portal
  - .to [4]
    - Dangling pointer
    - Partial compromise

I want my own TLD too!
TLD Catch: Methodology

- Query every nameserver in the root zone for its authoritative zones
  - Includes PSL (Public Suffix List)
- If DNS queries fail, perform whois to determine registerability
- If whois status is not an expected valid or functional result[1]
- If domain appears registrable at common registrars
- Email alert with failing zone, nameserver, whois status

Collected results for ~1 year in 2021

A wild bug appears!

Queries to nic.in would randomly timeout or return different results..
Down the rabbit hole with nic.in

\( \frac{3}{4} \) of the nameservers for the nic.in zone timeout when querying for CAA records with DNSSEC.
Certificate Authorities are required to use DNSSEC when querying for CAA records. [1]

This results in only a ¼ chance that a Certificate Authority would be able to prevent unauthenticated certificates from being issued. Failing open.

<table>
<thead>
<tr>
<th>NS</th>
<th>Status</th>
<th>CAA</th>
<th>DNSSEC with CAA</th>
<th>DNSSEC with any other type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns1.nic.in.</td>
<td>Good</td>
<td>Good</td>
<td>Timeout</td>
<td>Good</td>
</tr>
<tr>
<td>ns6.nic.in.</td>
<td>Good</td>
<td>Good</td>
<td>Timeout</td>
<td>Good</td>
</tr>
<tr>
<td>ns8.nic.in.</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>nicnet.nic.in.</td>
<td>Good</td>
<td>Good</td>
<td>Timeout</td>
<td>Good</td>
</tr>
</tbody>
</table>

[1] Section 3.2.2.8 of the CAB Forum BRs,
NCIIPC runs Responsible Vulnerability Disclosure Program (RVDP) for reporting any Vulnerability in Critical Information Infrastructures that may cause unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction of the same.
Hello,

I am attempting to report a vulnerability I've discovered in the authoritative nameservers for nic.in (the India ccTLD).

While researching something unrelated, I noticed that most of the nic.in nameservers do not respond to CAA queries when the requestor sets the DNSSEC "do" bits. But if the DNS request for CAA does not use DNSSEC then the correct CAA records are returned. It appears that of your 4 nameservers (ns1.nic.in, ns6.nic.in, ns8.nic.in, nicnet.nic.in) only ns8.nic.in will respond to CAA queries when DNSSEC is used. This means that if a nameserver is chosen randomly, there is an 75% chance the CAA query with DNSSEC will fail.

This is a problem because CAA records exist to allow Certificate Authorities to verify with the domain owner that they are allowed to issue SSL certificates for the domain. If no CAA records are returned, the CA would assume there is no CAA policy and issue the certificate, even if they would otherwise not be allowed to. CAs are required to check CAA records with DNSSEC, which likely means that about 75% of the CAs that send CAA requests to the nic.in zone will fail open, which is not ideal.

You can observe this behavior with the dig utility:

- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. +CAA +dnssec
- dig +short @ns8.nic.in. -q www.demowebmet
Dear Researcher,

(i) The reported vulnerability is seems to be invalid. Kindly recheck and explain the exploitability.

With regards,
Team RVDP, NCIPPC
Hello,

My first email contained a very detailed explanation and examples. The attachment I sent in the original email also contained even more information.

Can you let me know which part you are not seeing as vulnerable so that I can clarify?

Thanks.

Dear Researcher,

The issue reported seems to be a functional issue. The description and our validation did not indicate any Information Security issue as such.

Since, this seems to be a functional vulnerability and not an Information Security Vulnerability, we may consider sending an alert to the asset owner for their consideration.

However, we may also consider that the asset owner may have intentionally configured in such way so as to limit responses to CAA requests.

With regards,
Team RVDP, NCIIPC
Hello,

Thank you for your response.

The information security issue is if a domain owner has a CAA record to limit the Certificate Authorities who can issue SSL certificates for their domain, and if that record is not served to the CA when they query the server (with DNSSEC as per the spec) then the CA will assume that there is no CAA policy and issue the certificate, even if there IS a CAA policy set for the domain preventing the CA from issuing the certificate.

Certificate Authorities are required to use DNSSEC. Not serving CAA records with DNSSEC is equivalent to not allowing them and letting any CA issue certificates for the domains.

While this issue alone does not allow anyone to get a certificate for any domain, it breaks the security measure that CAA records exist to prevent. I can provide hypothetical scenarios where this would lead to an issue if you still do not understand.

> However, we may also consider that the asset owner may have intentionally configured in such way so as to limit responses to CAA requests. This can not be the case at all. Selectively choosing not to respond to CAA requests is an even larger security issue. If this is the case then the registrar is effectively lying about their security behavior to their clients and CAs.

Please let me know if you have any other questions or need any additional explanation.

Thanks.
*Crickets chirping*
Dear Sir,

DNS CAA record is resolving from NICNET.NIC.IN, NS1.NIC.IN and NS6.NIC.IN with DNSSEC

[root@NICNET-SERVER named]# dig caa www.demowebmeet.nic.in +dnssec
>>> DIG 9.11.28 >>>> caa www.demowebmeet.nic.in +dnssec
+cmd
+global options: +cmd
+flags: on
+ HEADERS<: opcode: QUERY, status: NOERROR, id: 48191
+flags: on
+aa rd: QUERY: 1, ANSWER: 4, AUTHORITY: 5, ADDITIONAL: 8
+WARNING: recursion requested but not available

Hello Manoj,

Running the dig commands as you did on the various servers does not mean that the server you ran it on was the one queried. You need to make it will use a non-authoritative DNS server.

You need to specify the resolver you want to query when using the dig queries otherwise the request will go to the system's DNS resolver and not to the one associated with dig with the @ip parameter. example: @nicnet.nic.in. Many non-authoritative resolvers will query multiple servers in parallel for each request. 3 out of 4 of your servers are timing out, the non-authoritative resolver will respond correctly most of the time, but that's only because the other resolvers are not consistent in the zone.

Most of the dig commands are coming from multiple servers located all over the world and they all fail. You may also try.

dig www.demowebmeet.nic.in +t CAA +dnssec

any other help verifying this.

Again, this is testing external non-authoritative recursive resolvers, which does not show the problem.

Be sure to test against YOUR authoritative DNS servers.
You need to test against ns1.nic.in, ns6.nic.in, nicnet.nic.in.
The problem I'm observing is in your servers, not Google, Cloudflare, or ATT.
nic.in Disclosure

After 2 months of going nowhere, I report the issue to CERT and the CAB Forum, and the issue is resolved for 2 of the servers the next day.

Fun fact: nic.in was the CA that issued illegitimate SSL certificates in 2014 for google.com and other sites resulting in the creation of Certificate Transparency! [1]

Nic.in 1 year later....

2/4 servers fail with or without DNSSEC.
Findings: .aw

On June 18th, 2021, one of .aw’s authoritative nameservers stopped responding to DNS queries.

- `dns[1-3].dns.aw` could no longer be resolved
- `aw0[1-2].setarnet.aw` continued to work normally, resulting in no downtime and likely caused the issue to go unnoticed.
- Can we register dns.aw?

What is Aruba (AW)?

- Small island in the Caribbean Sea
- Part of the Netherlands
- Population ~100k
- ~155k domains

```
[foster@rocinante:~]# dig -t ns -q aw.
;
;; DiG 0.16.15-Debian <<>> -t ns -q aw.
;; global options: +cmd
;; Got answer:
;; >>>HEADER<<- opcode: QUERY, status: NOERROR, id: 8025
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;aw.   IN   NS
;; ANSWER SECTION:
;aw.     86400 IN   NS   ns1.dns.aw.
;aw.     86400 IN   NS   ns2.dns.aw.
;aw.     86400 IN   NS   ns3.dns.aw.
;aw.     86400 IN   NS   aw01.setarnet.aw.
;aw.     86400 IN   NS   aw02.setarnet.aw.

;; Query time: 176 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jun 18 11:44:30 PDT 2021
;; MSG SIZE  rcvd: 138
```
Findings .aw

$ whois dns.aw
Domain name: dns.aw
Status: inactive

Registrar:
    SETAR N.V.
    Administration Building
    Seroe Blanco 29A
    Oranjestad
    Aruba

Abuse Contact:

Creation Date: 2014-02-25
Updated Date: 2014-02-28
DNSSEC: no

Record maintained by: AW Domain Registry
Findings .aw

Great News!

dns.aw
Your domain is available!

139.99 USD
Add To Cart

Check out these great domain names based on what you were looking for...

Show Unavailable

dns.ms
Inquire

dns.pr
Inquire
Findings .aw

Perfect! Your domain is available.

dns.aw

There are other options for you

dns.com Unavailable

DNS .aw

Transfer

dns.it is

Transfer

dns.is Unavailable

dns.cat

Transfer
.aw Impact

If I was to register nic.aw, I should expect to be able to control ~ 3/5th of all DNS requests for all domains in .aw...

Which means that...

- I could get an SSL certificate for any .aw domain
- I could MitM any traffic to any .aw domain
  - HTTPS, email, ..., everything... (with 3/5th probability)
- If any nameservers in other zones use any domains in .aw I could do the same to them as well...
Email any admin contacts I could find (bounce)
Email contacts at ICANN
Call the setar IT, they are clueless but take down my info
Call admin’s work number. “This voicemail box is full”
Call admin’s personal cell phone, leave voicemail
Eventually I am able to get in touch with the admin who understands the issue
  ○ Believes that any attempts to register the domain would have failed....

dns.aw is re-registered and starts responding to DNS queries again before day’s end.
A TLD SOME RANDOM PERSON IN Aruba HAS BEEN THANKLESSLY MAINTAINING SINCE 1996
Finding: .si

On November 5th, 2021, the domain name dns.si, used for all 5 of the authoritative nameservers for the .si ccTLD stopped responding to DNS queries.

Whois status: inactive
Finding: .si

Registrable: ✓
Finding: .si

~5 hours later.....

Interested in this domain? We can help.

dns.si
This domain name is unavailable. Learn More

Check out these great domain names based on what you were looking for...
Finding: .nl

November 16th, 2021, dns.nl, which is the domain used for all authoritative nameservers starts to appear as registerable.

Same as .si.
Finding: .nl

```
 dig -t ns -q nl.
```

```
; Got answer:
; OPT PSEUDOSECTION: EDNS: version: 0, flags: udp: 4096
; QUESTION SECTION:
; IN   NS       
; dns.nl

; ANSWER SECTION:
; 21600 IN NS   ns3.dns.nl.
; 21600 IN NS   ns2.dns.nl.
; 21600 IN NS   ns1.dns.nl.

Query time: 159 msec
SERVER: 127.0.0.1 (127.0.0.1)
WHEN: Wed Nov 16 12:41:43 PST 2021
```
Findings: .nl

But it still works?

```
mrlanrat@penguin:~[2]$ ping -4 ns1.dns.nl.
PING ns1.dns.nl (194.0.28.53) 56(84) bytes of data.
64 bytes from ns1.dns.nl (194.0.28.53): icmp_seq=1 ttl=53 time=6.63 ms
64 bytes from ns1.dns.nl (194.0.28.53): icmp_seq=2 ttl=53 time=6.87 ms
64 bytes from ns1.dns.nl (194.0.28.53): icmp_seq=3 ttl=53 time=5.71 ms
^C
--- ns1.dns.nl ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 5.707/6.403/6.869/0.501 ms
mrlanrat@penguin:~$  
```
Oh no, your order failed to complete

The failed items will be refunded shortly.

Please try again once you’ve received your refund — simply check your account.

If your Namecheap balance is sufficient to cover the payment, just choose 'Account'.

Please contact our Billing Support 24/7 for any further assistance.

dns.nl started resolving again...
Defensive Measures

For TLD operators
- Use internal & external monitoring
- Make it easy to relay information to technical operators
- Hold yourself to ICANN’s standards, even if you don’t need to

For everyone else
- Choose a reputable/robust TLD
- Avoid ccTLDs
- Run your own lame delegation checks on your domains and their dependencies
- Use DNSSEC
Future Work

- Lame-DNS
  - https://github.com/lanrat/lame-dns
- DNS.Coffee
  - More coming soon™
Questions?

https://dns.coffee

@LANRAT
Types of TLDs

ICANN defines 6 types of TLDs. [1]

- Generic
  - gTLDs (99% of domains)
  - com, net, org, info, etc..
- Country code
  - Issued to a "country" or "territory"
  - Always 2 letters long
  - Includes past or non-existent countries as well. ex: .su
- Sponsored
  - Special interest TLDs
  - aero, gov, mil, edu, tel
- Test
  - Changes often
  - New TLDs may start here
- Generic Restricted
  - Registrations "restricted" to a limited set of entities
  - biz, pro, name
- Infrastructure
  - .arpa
- Reserved
  - Example, invalid, localhost, test
  - Honorable mention: .onion

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>generic</td>
<td>1245</td>
</tr>
<tr>
<td>country code</td>
<td>316</td>
</tr>
<tr>
<td>sponsored</td>
<td>14</td>
</tr>
<tr>
<td>test</td>
<td>11</td>
</tr>
<tr>
<td>generic-restricted</td>
<td>3</td>
</tr>
<tr>
<td>infrastructure</td>
<td>1</td>
</tr>
<tr>
<td>reserved</td>
<td>4</td>
</tr>
</tbody>
</table>

[1] https://www.iana.org/domains/root/db