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?

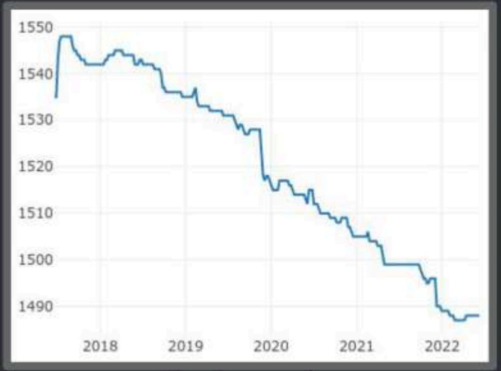
Top-level domain (TLD) refers to the last segment of a domain name, or the part that follows immediately after the "dot" symbol.

Common TLDs include:

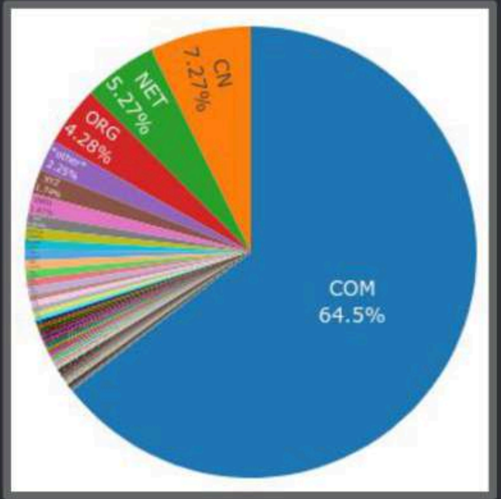
- gTLDs: com, net, org, info, …
- ccTLDs: io, co.uk, us, …
- Sponsored: aero, gov, mil, edu, tel
- Infra: arpa

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

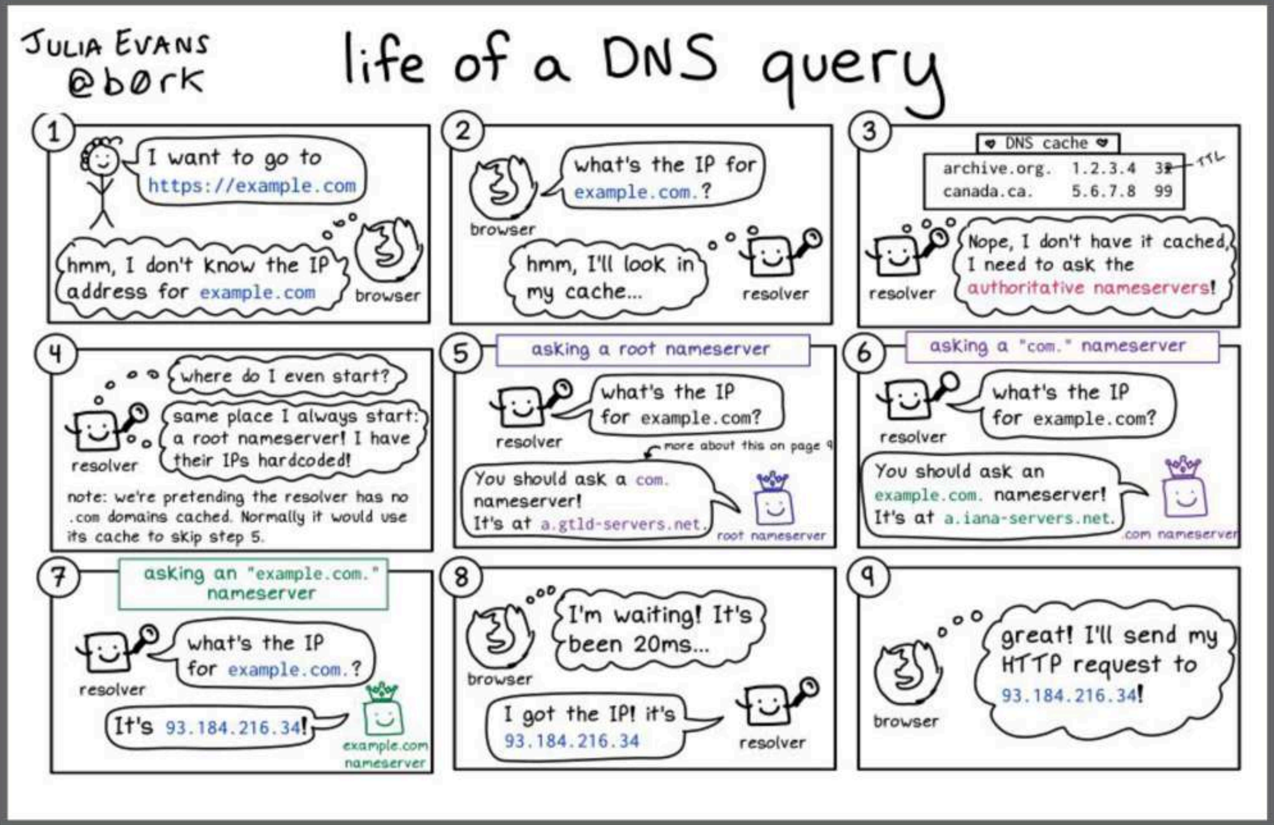
TLDs operate just like domains with subdomains.



Root zone size

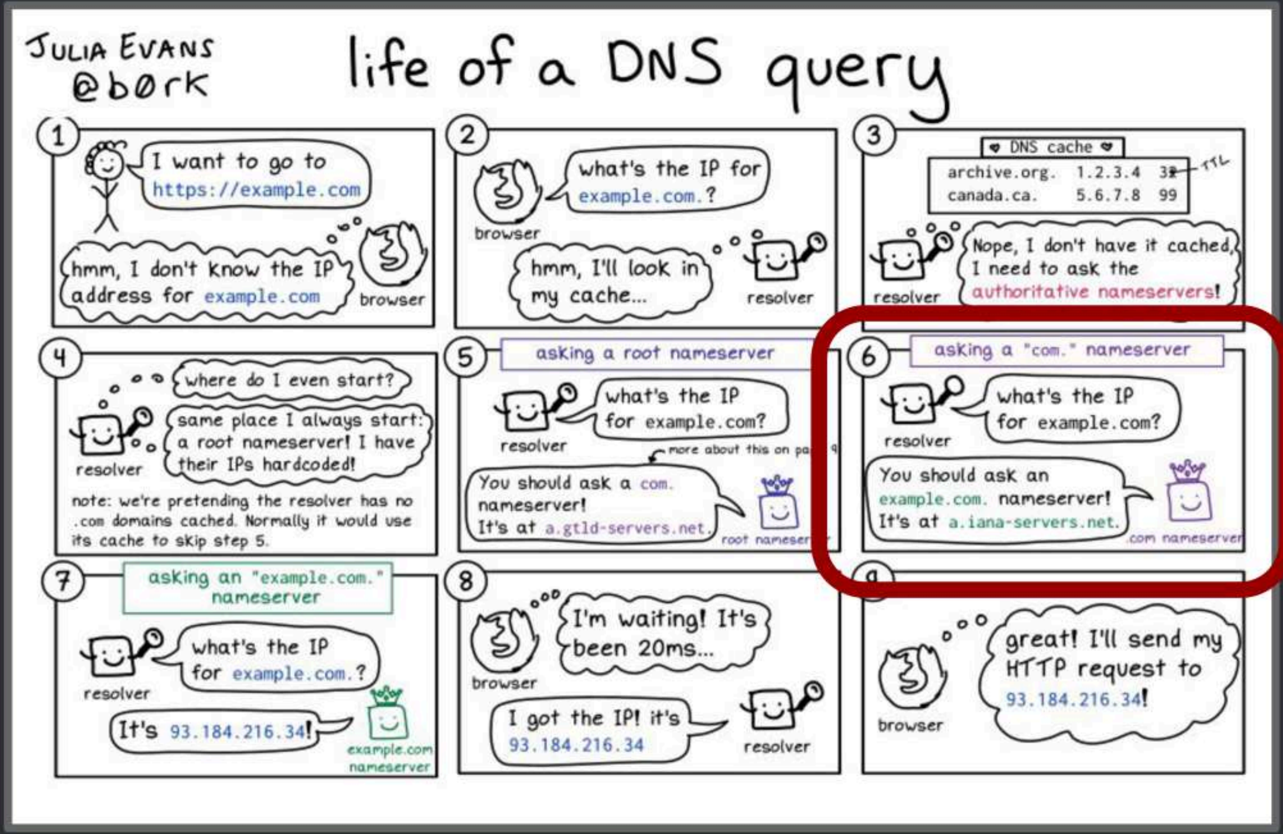


How Does DNS work?


JULIA EVANS
@bØrk
life of a DNS query
1
I want to go to https://example.com
hmm, I don't know the IP address for example.com
browser
2
what's the IP for example.com.?
browser
hmm, I'll look in my cache...
resolver
3
DNS cache
archive.org. 1.2.3.4 32
canada.ca. 5.6.7.8 99
TTL
resolver
Nope, I don't have it cached, I need to ask the authoritative nameservers!
4
where do I even start?
same place I always start: a root nameserver! I have their IPs hardcoded!
resolver
note: we're pretending the resolver has no .com domains cached. Normally it would use its cache to skip step 5.
5
asking a root nameserver
what's the IP for example.com?
resolver
more about this on page 9
You should ask a com. nameserver! It's at a.gtld-servers.net.
root nameserver
6
asking a "com." nameserver
what's the IP for example.com?
resolver
You should ask an example.com. nameserver! It's at a.iana-servers.net.
.com nameserver
7
asking an "example.com." nameserver
what's the IP for example.com.?
resolver
It's 93.184.216.34!
example.com nameserver
8
I'm waiting! It's been 20ms...
browser
I got the IP! it's 93.184.216.34
resolver
9
great! I'll send my HTTP request to 93.184.216.34!
browser

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

How Does DNS work?


JULIA EVANS
@børk
life of a DNS query
1
I want to go to https://example.com
hmm, I don't know the IP address for example.com
browser
2
browser
what's the IP for example.com.?
hmm, I'll look in my cache...
resolver
3
♥ DNS cache ♥
archive.org. 1.2.3.4 32
canada.ca. 5.6.7.8 99
TTL
resolver
Nope, I don't have it cached, I need to ask the authoritative nameservers!
4
resolver
where do I even start?
same place I always start: a root nameserver! I have their IPs hardcoded!
note: we're pretending the resolver has no .com domains cached. Normally it would use its cache to skip step 5.
5
asking a root nameserver
resolver
what's the IP for example.com?
more about this on pa
You should ask a com. nameserver! It's at a.gtld-servers.net.
root nameser
6
asking a "com." nameserver
resolver
what's the IP for example.com?
You should ask an example.com. nameserver! It's at a.iana-servers.net.
.com nameserver
7
asking an "example.com." nameserver
resolver
what's the IP for example.com.?
It's 93.184.216.34!
example.com nameserver
8
browser
I'm waiting! It's been 20ms...
I got the IP! it's 93.184.216.34
resolver
9
browser
great! I'll send my HTTP request to 93.184.216.34!

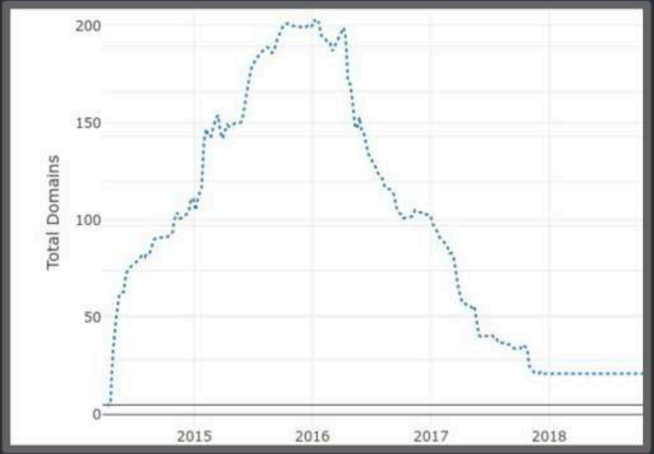
https://wizardzines.com/comics/life-of-a-dns-query/

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]

[1] https://www.icann.org/resources/pages/gtld-2012-02-25-en

[2] https://www.icann.org/resources/pages/cctld-2012-02-25-en



The birth & death of .wed

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

[1] https://thehackerblog.com/the-io-error-taking-control-of-all-io-domains-with-a-targeted-registration/
[2] https://thehackerblog.com/the-journey-to-hijacking-a-countrys-tld-the-hidden-risks-of-domain-extensions/
[3] https://labs.detectify.com/2021/01/15/how-i-hijacked-the-top-level-domain-of-a-sovereign-state/
[4] https://palisade.consulting/blog/tld-hacking

I want my own TLD too!

TLD Catch

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

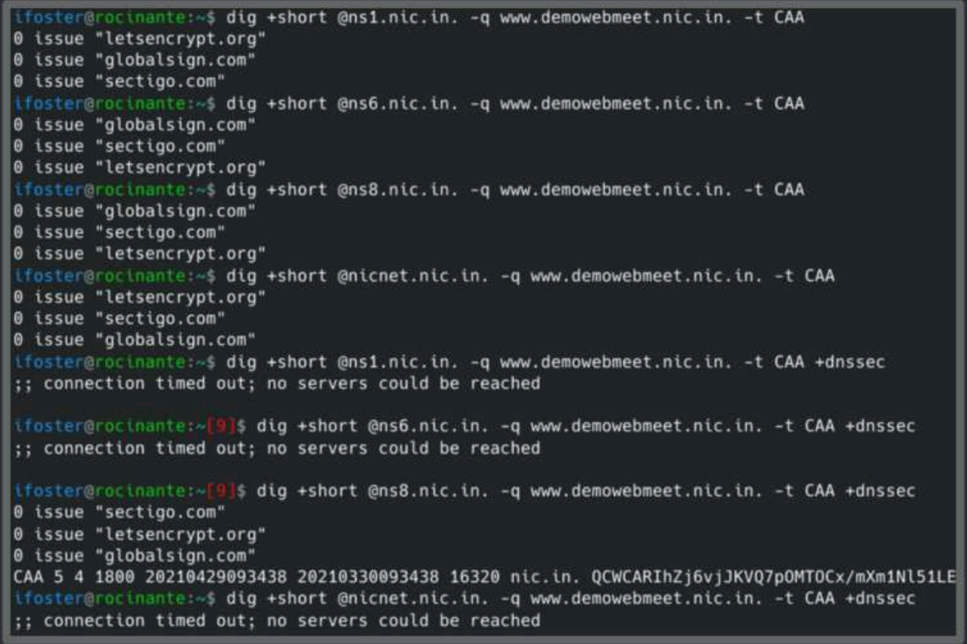
[1] https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en

A wild bug appears!

Queries to nic.in would randomly timeout or return different results..

Down the rabbit hole with nic.in

¾ of the nameservers for the nic.in zone timeout when querying for CAA records with DNSSEC.



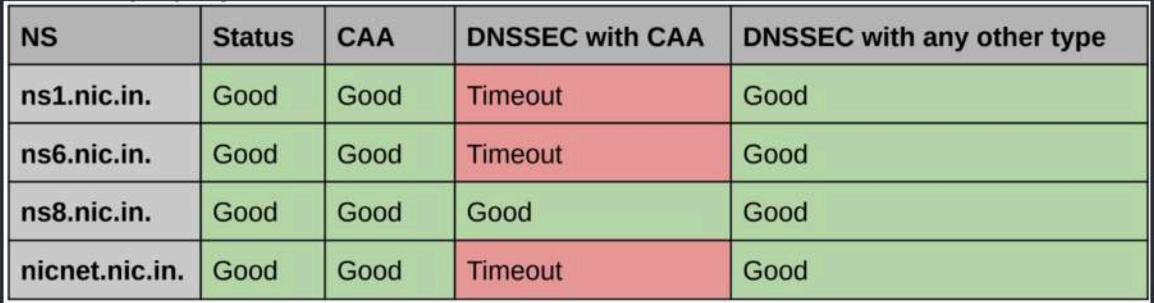
```
ifoster@rocinante:~$ dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. -t CAA
0 issue "letsencrypt.org"
0 issue "globalsign.com"
0 issue "sectigo.com"
ifoster@rocinante:~$ dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. -t CAA
0 issue "globalsign.com"
0 issue "sectigo.com"
0 issue "letsencrypt.org"
ifoster@rocinante:~$ dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. -t CAA
0 issue "globalsign.com"
0 issue "sectigo.com"
0 issue "letsencrypt.org"
ifoster@rocinante:~$ dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. -t CAA
0 issue "letsencrypt.org"
0 issue "sectigo.com"
0 issue "globalsign.com"
ifoster@rocinante:~$ dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
;; connection timed out; no servers could be reached

ifoster@rocinante:~[9]$ dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
;; connection timed out; no servers could be reached

ifoster@rocinante:~[9]$ dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
0 issue "sectigo.com"
0 issue "letsencrypt.org"
0 issue "globalsign.com"
CAA 5 4 1800 20210429093438 20210330093438 16320 nic.in. QCWCARIhZj6vjJKVQ7pOMTOCx/mXm1Nl51LE
ifoster@rocinante:~$ dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
;; connection timed out; no servers could be reached
```

nic.in

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.

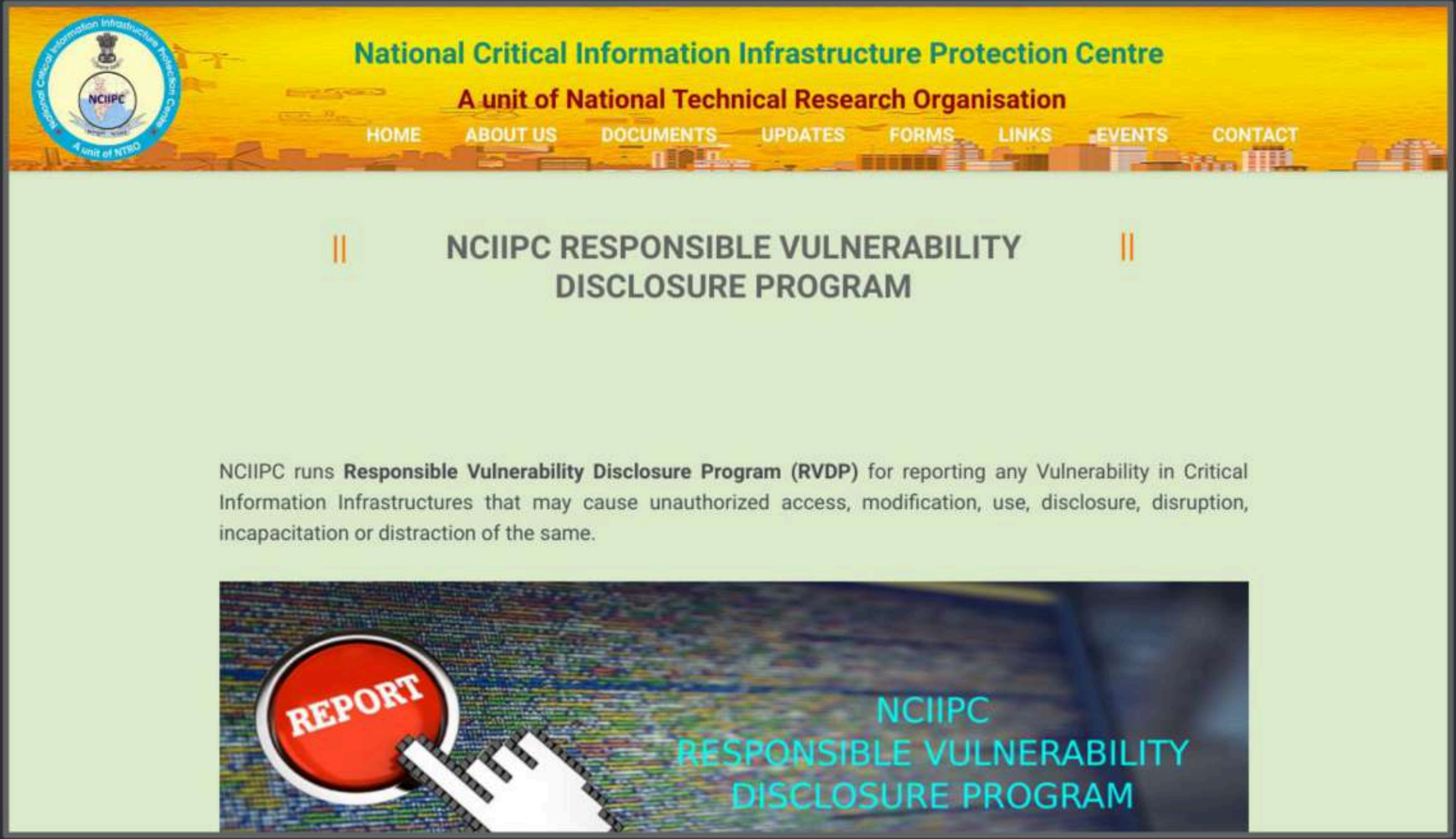
Failing open.



NS	Status	CAA	DNSSEC with CAA	DNSSEC with any other type
ns1.nic.in.	Good	Good	Timeout	Good
ns6.nic.in.	Good	Good	Timeout	Good
ns8.nic.in.	Good	Good	Good	Good
nicnet.nic.in.	Good	Good	Timeout	Good

[1] Section 3.2.2.8 of the CAB Forum BRs,

nic.in Disclosure

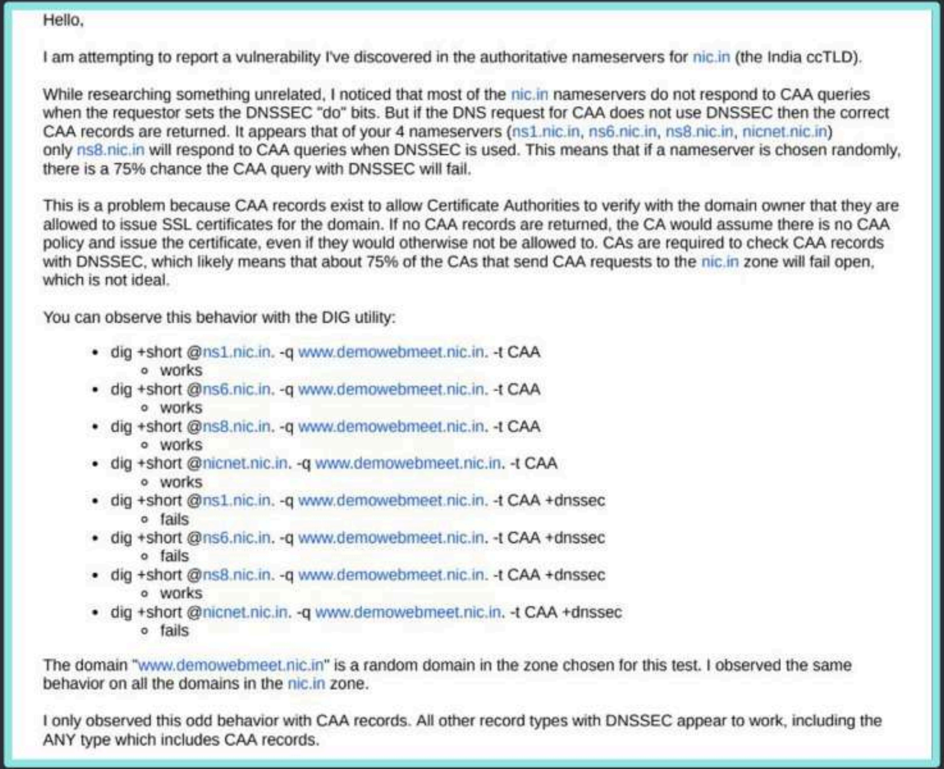


National Critical Information Infrastructure Protection Centre

A unit of National Technical Research Organisation

|| NCIIPC RESPONSIBLE VULNERABILITY DISCLOSURE PROGRAM ||

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 a 75% chance the CAA query with DNSSEC will fail.

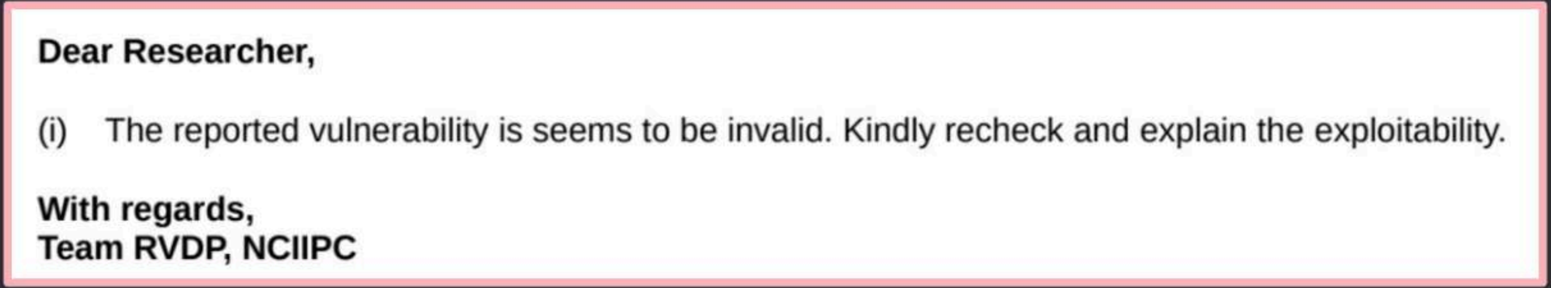
This is a problem because CAA records exist to allow Certificate Authorities to verify with the domain owner that they are allowed to issue SSL certificates for the domain. If no CAA records are returned, the CA would assume there is no CAA policy and issue the certificate, even if they would otherwise 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. -t CAA
  - works
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. -t CAA
  - works
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. -t CAA
  - works
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. -t CAA
  - works
- dig +short @ns1.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
  - fails
- dig +short @ns6.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
  - fails
- dig +short @ns8.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
  - works
- dig +short @nicnet.nic.in. -q www.demowebmeet.nic.in. -t CAA +dnssec
  - fails

The domain "www.demowebmeet.nic.in" is a random domain in the zone chosen for this test. I observed the same behavior on all the domains in the nic.in zone.

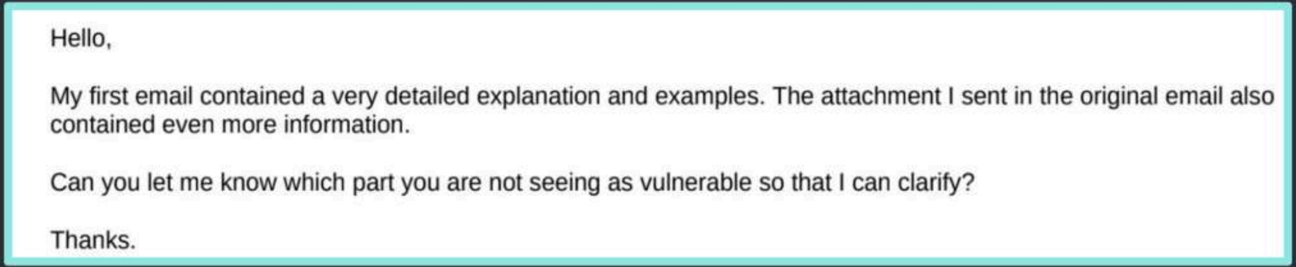
I only observed this odd behavior with CAA records. All other record types with DNSSEC appear to work, including the ANY type which includes CAA records.



Dear Researcher,

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

With regards,
Team RVDP, NCIIPC

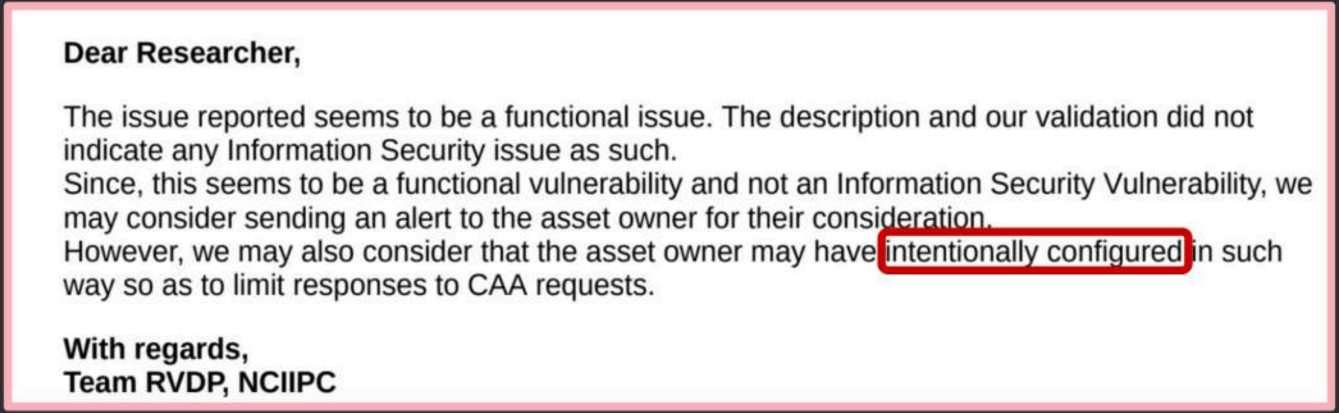


Hello,

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?

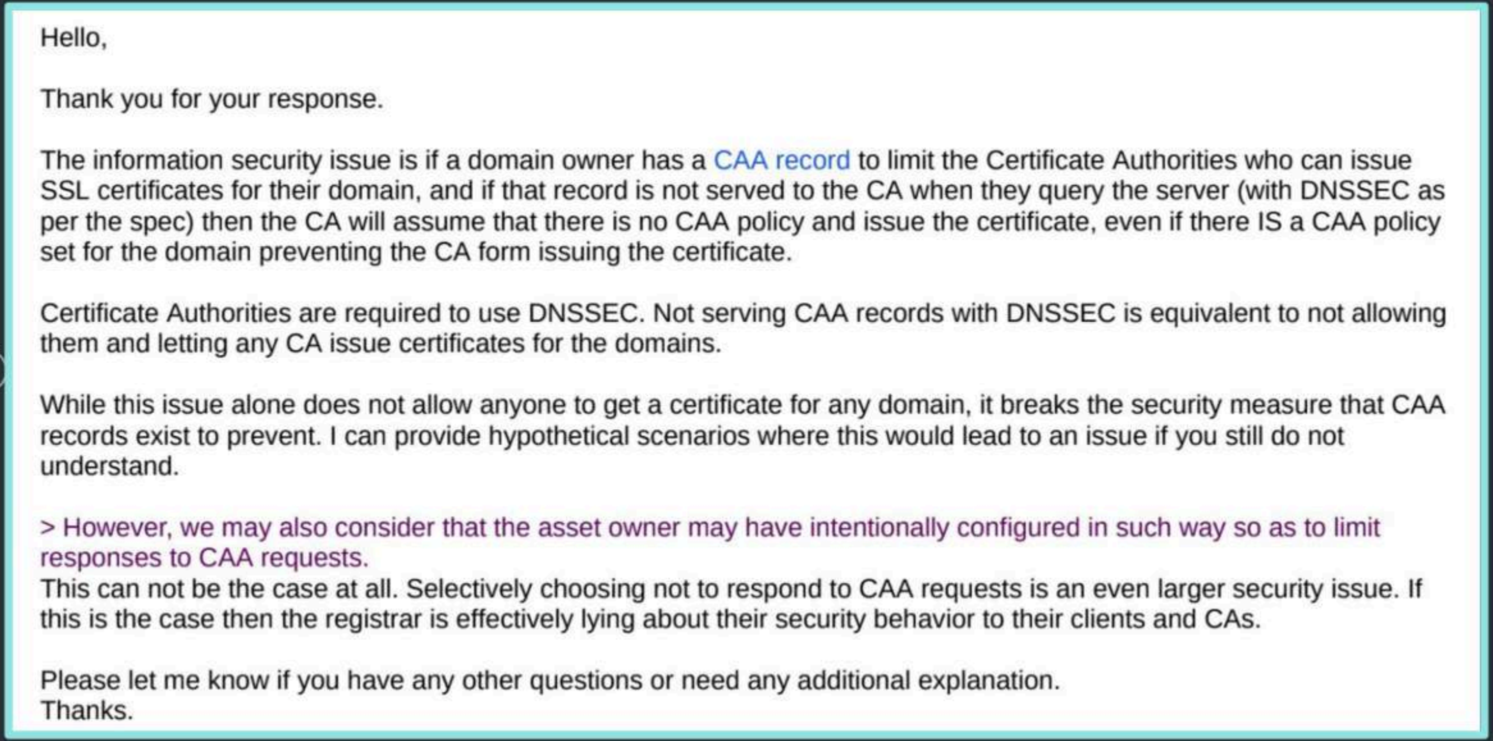
Thanks.



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 form 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.

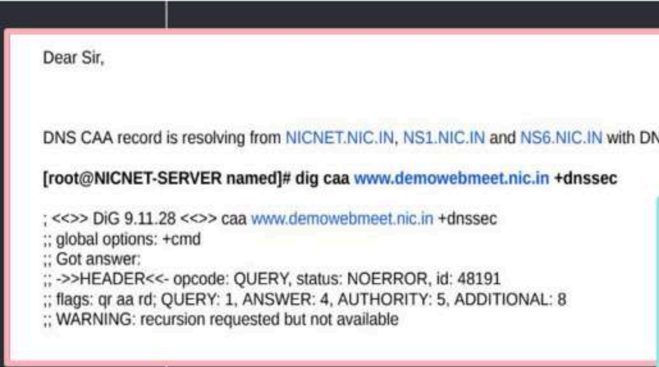
While this issue alone does not allow anyone to get a certificate for any domain, it breaks the security measure that CAA records exist to prevent. I can provide hypothetical scenarios where this would lead to an issue if you still do not understand.

> 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

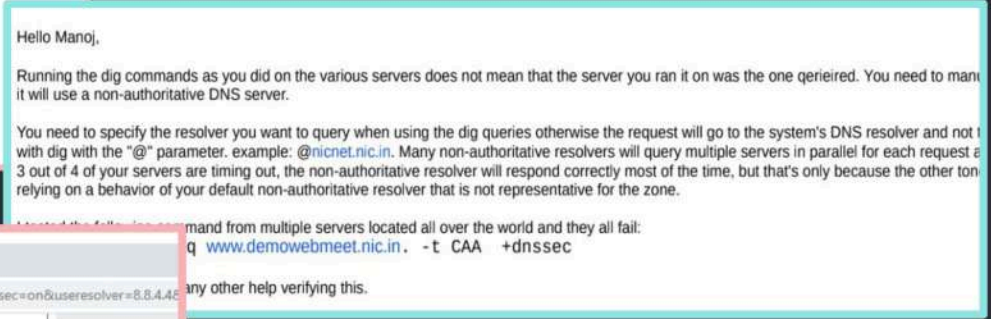


Dear Sir,

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
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48191
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 5, ADDITIONAL: 8
;; WARNING: recursion requested but not available
```



Hello Manoj,

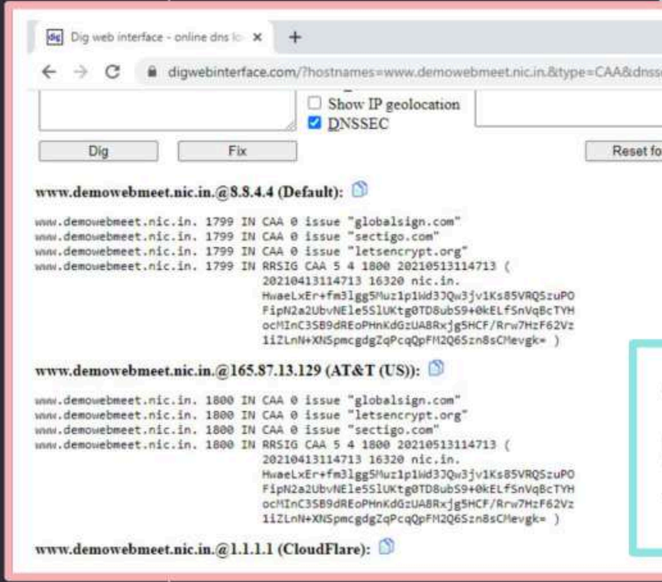
Running the dig commands as you did on the various servers does not mean that the server you ran it on was the one qerieired. You need to man
it will use a non-authoritative DNS server.

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
with dig with the "@" parameter. example: @nicnet.nic.in. Many non-authoritative resolvers will query multiple servers in parallel for each request a
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 ton
relying on a behavior of your default non-authoritative resolver that is not representative for the zone.

mand from multiple servers located all over the world and they all fail:

```
q www.demowebmeet.nic.in. -t CAA  +dnssec
```

any other help verifying this.



Dig web interface - online dns lo ×
+
digwebinterface.com/?hostnames=www.demowebmeet.nic.in.&type=CAA&dnssec=on&useresolver=8.8.4.4&
Dig
Fix
Reset form

□ Show IP geolocation
☑ DNSSEC

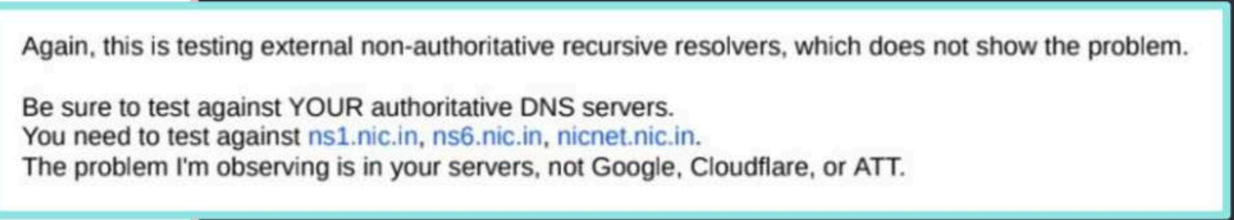
www.demowebmeet.nic.in.@8.8.4.4 (Default):

```
www.demowebmeet.nic.in. 1799 IN CAA 0 issue "globalsign.com"
www.demowebmeet.nic.in. 1799 IN CAA 0 issue "sectigo.com"
www.demowebmeet.nic.in. 1799 IN CAA 0 issue "letsencrypt.org"
www.demowebmeet.nic.in. 1799 IN RRSIG CAA 5 4 1800 20210513114713 (
                                20210413114713 16320 nic.in.
                                HwaeLxEr+fm3lgg5Muz1p1Wd3JQw3jv1Ks85VRQ5zuPO
                                FipN2a2UbvNEle5SlUKtg0TD8ubS9+0kELfSnVqBcTYH
                                ocMInC3SB9dREoPHnKdGzUABRxjg5HCF/Rrw7HzF62Vz
                                1iZLnN+XNSpmcgdgZqPcqQpFM2Q6Szn8sCMevgk= )
```

www.demowebmeet.nic.in.@165.87.13.129 (AT&T (US)):

```
www.demowebmeet.nic.in. 1800 IN CAA 0 issue "globalsign.com"
www.demowebmeet.nic.in. 1800 IN CAA 0 issue "letsencrypt.org"
www.demowebmeet.nic.in. 1800 IN CAA 0 issue "sectigo.com"
www.demowebmeet.nic.in. 1800 IN RRSIG CAA 5 4 1800 20210513114713 (
                                20210413114713 16320 nic.in.
                                HwaeLxEr+fm3lgg5Muz1p1Wd3JQw3jv1Ks85VRQ5zuPO
                                FipN2a2UbvNEle5SlUKtg0TD8ubS9+0kELfSnVqBcTYH
                                ocMInC3SB9dREoPHnKdGzUABRxjg5HCF/Rrw7MzF62Vz
                                1iZLnN+XNSpmcgdgZqPcqQpFM2Q6Szn8sCMevgk= )
```

www.demowebmeet.nic.in.@1.1.1.1 (CloudFlare):



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

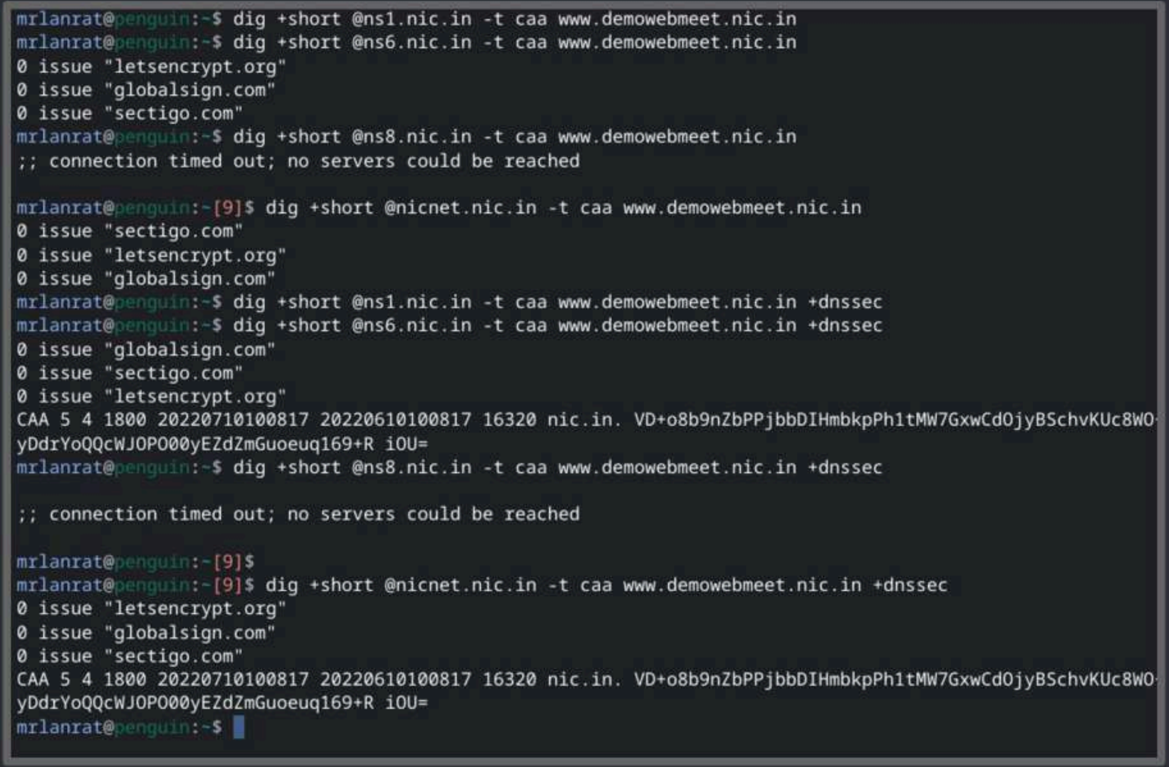
After 2 months of going nowhere, I report the issue to CERT and the CAB Forum, and the issue is resolved for 2 of the servers the next day.

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]

[1] https://security.googleblog.com/2014/07/maintaining-digital-certificate-security.html

Nic.in 1 year later....

2/4 servers fail with or without DNSSEC..



```
mrlanrat@penguin:~$ dig +short @ns1.nic.in -t caa www.demowebmeet.nic.in
mrlanrat@penguin:~$ dig +short @ns6.nic.in -t caa www.demowebmeet.nic.in
0 issue "letsencrypt.org"
0 issue "globalsign.com"
0 issue "sectigo.com"
mrlanrat@penguin:~$ dig +short @ns8.nic.in -t caa www.demowebmeet.nic.in
;; connection timed out; no servers could be reached

mrlanrat@penguin:~[9]$ dig +short @nicnet.nic.in -t caa www.demowebmeet.nic.in
0 issue "sectigo.com"
0 issue "letsencrypt.org"
0 issue "globalsign.com"
mrlanrat@penguin:~$ dig +short @ns1.nic.in -t caa www.demowebmeet.nic.in +dnssec
mrlanrat@penguin:~$ dig +short @ns6.nic.in -t caa www.demowebmeet.nic.in +dnssec
0 issue "globalsign.com"
0 issue "sectigo.com"
0 issue "letsencrypt.org"
CAA 5 4 1800 20220710100817 20220610100817 16320 nic.in. VD+o8b9nZbPPjbbDIHmbkpPh1tMW7GxwCdOjyBSchvKUc8WO
yDdrYoQQcWJOPO00yEZdZmGuoeuq169+R iOU=
mrlanrat@penguin:~$ dig +short @ns8.nic.in -t caa www.demowebmeet.nic.in +dnssec

;; connection timed out; no servers could be reached

mrlanrat@penguin:~[9]$
mrlanrat@penguin:~[9]$ dig +short @nicnet.nic.in -t caa www.demowebmeet.nic.in +dnssec
0 issue "letsencrypt.org"
0 issue "globalsign.com"
0 issue "sectigo.com"
CAA 5 4 1800 20220710100817 20220610100817 16320 nic.in. VD+o8b9nZbPPjbbDIHmbkpPh1tMW7GxwCdOjyBSchvKUc8WO
yDdrYoQQcWJOPO00yEZdZmGuoeuq169+R iOU=
mrlanrat@penguin:~$
```

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?

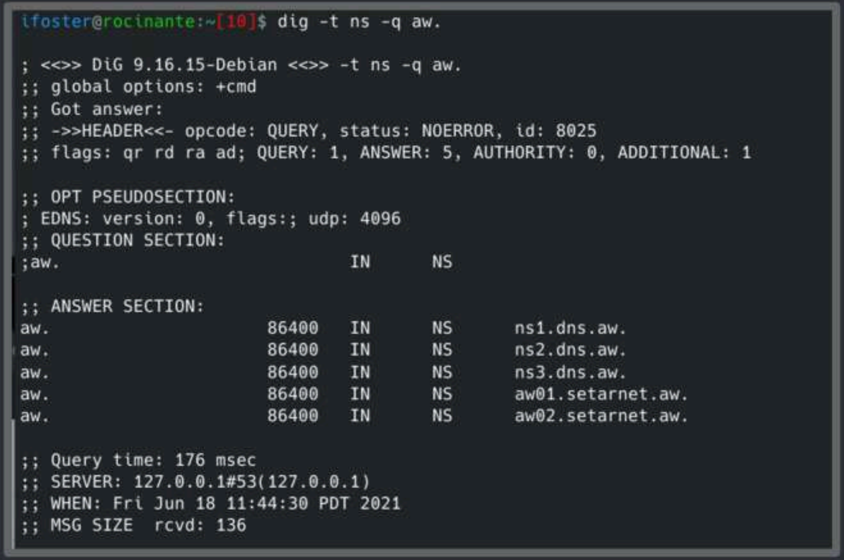
What is Aruba (AW)?

Small island in the caribbean Sea 🇦🇼

Part of the Netherlands

Population ~100k

~155k domains

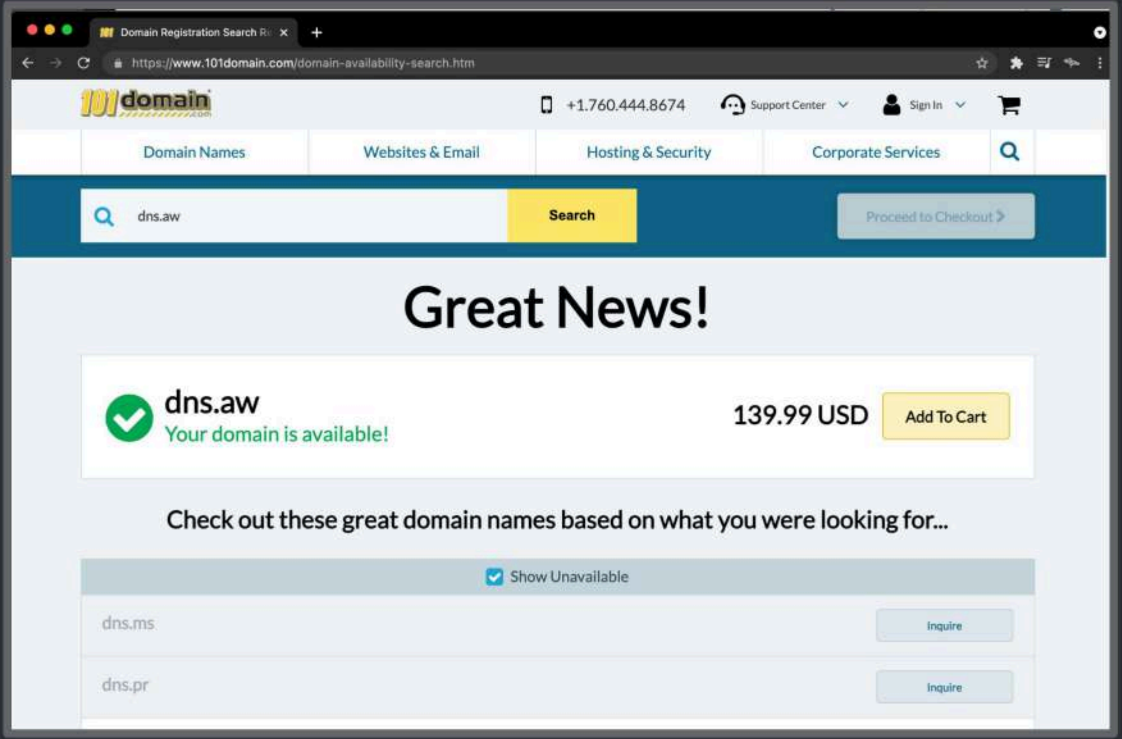


```
ifoster@rocinante:~[10]$ dig -t ns -q aw.

; <<>> DiG 9.16.15-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: 136
```

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



dns.aw

Great News!

dns.aw
Your domain is available!

139.99 USD

Add To Cart

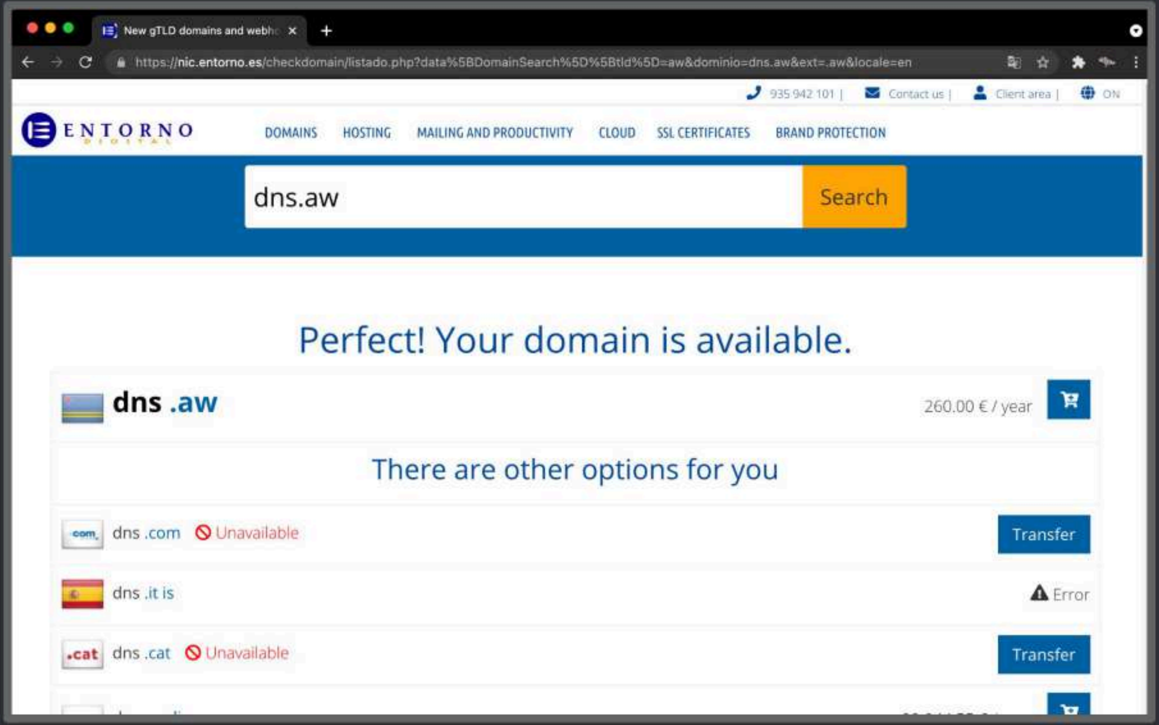
Check out these great domain names based on what you were looking for...

☑ Show Unavailable

dns.ms

dns.pr

Findings .aw



New gTLD domains and webh
https://nic.entorno.es/checkdomain/listado.php?data%5BDomainSearch%5D%5Btld%5D=aw&dominio=dns.aw&ext=.aw&locale=en
935 942 101 | Contact us | Client area | ON
ENTORNO DIGITAL
DOMAINS HOSTING MAILING AND PRODUCTIVITY CLOUD SSL CERTIFICATES BRAND PROTECTION
Search

dns.aw

Perfect! Your domain is available.

dns .aw 260.00 € / year

There are other options for you

dns .com Unavailable Transfer

dns .it is ⚠ Error

dns .cat Unavailable Transfer

.aw Impact

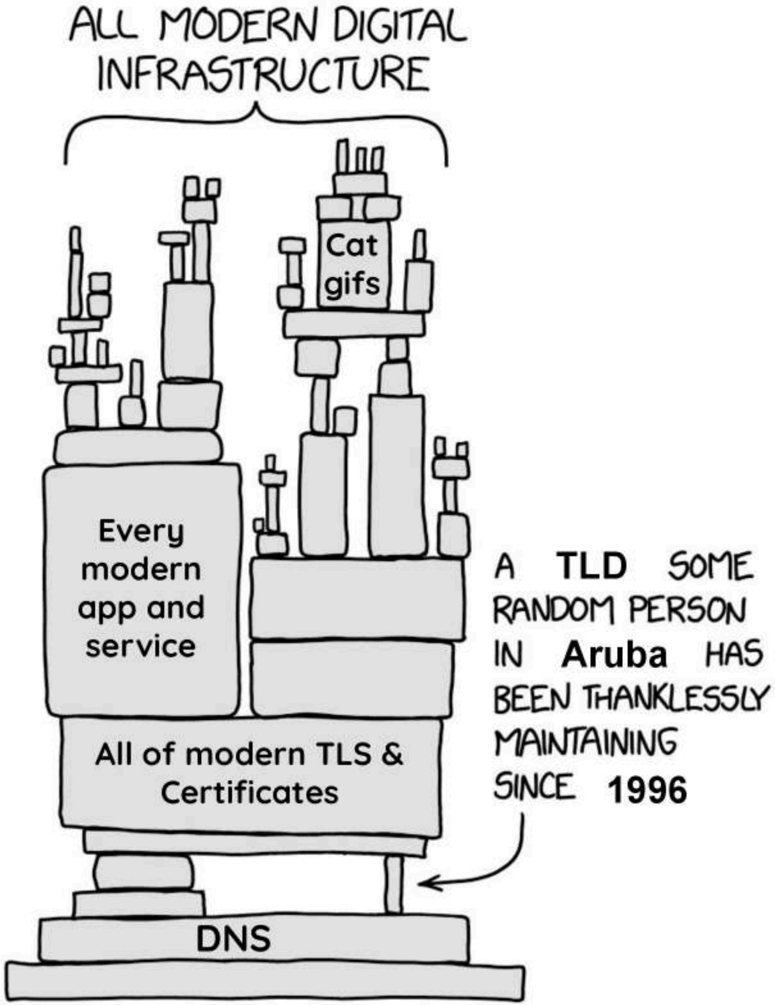
If I was to register nic.aw, I should expect to be able to control ~ 3/5th of all DNS requests for all domains in .aw...

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...

.aw Disclosure

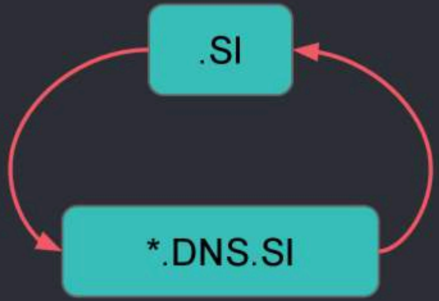
- Email any admin contacts I could find (bounce)
- Email contacts at ICANN
- Call the setar IT, they are clueless but take down my info
- Call admin's work number. "This voicemail box is full"
- Call admin's personal cell phone, leave voicemail
- Eventually I am able to get in touch with the admin who 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.


ALL MODERN DIGITAL INFRASTRUCTURE
Cat gifs
Every modern app and service
All of modern TLS & Certificates
DNS
A TLD SOME RANDOM PERSON IN Aruba HAS BEEN THANKLESSLY MAINTAINING SINCE 1996

Finding: .si

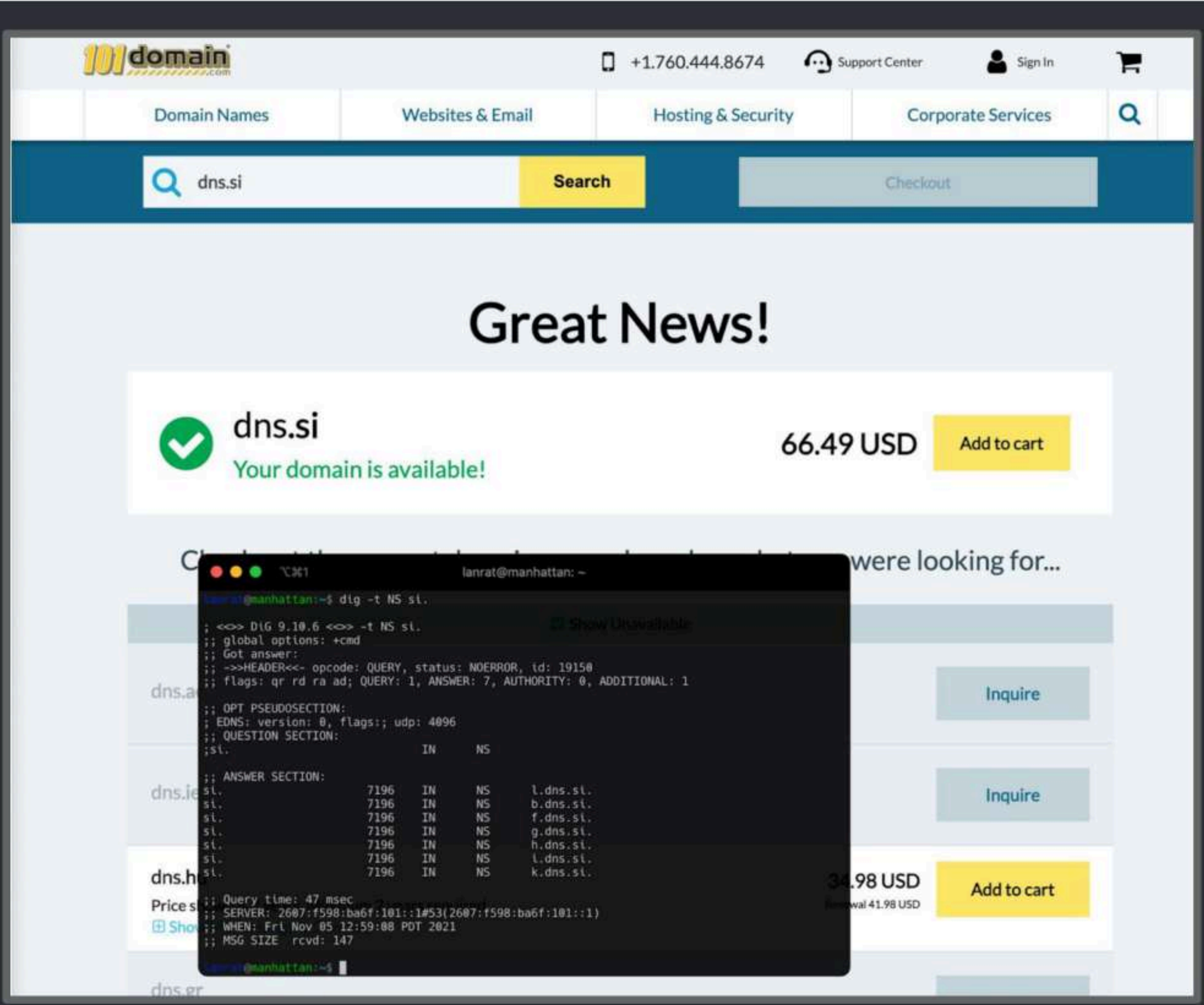
On November 5th, 2021, the domain name dns.si, used for all 5 of the authoritative nameservers for the .si ccTLD stopped responding to DNS queries.

Whois status: inactive



- Finding: .si

- Registrable: ✔



Great News!

✓ dns.si

Your domain is available!

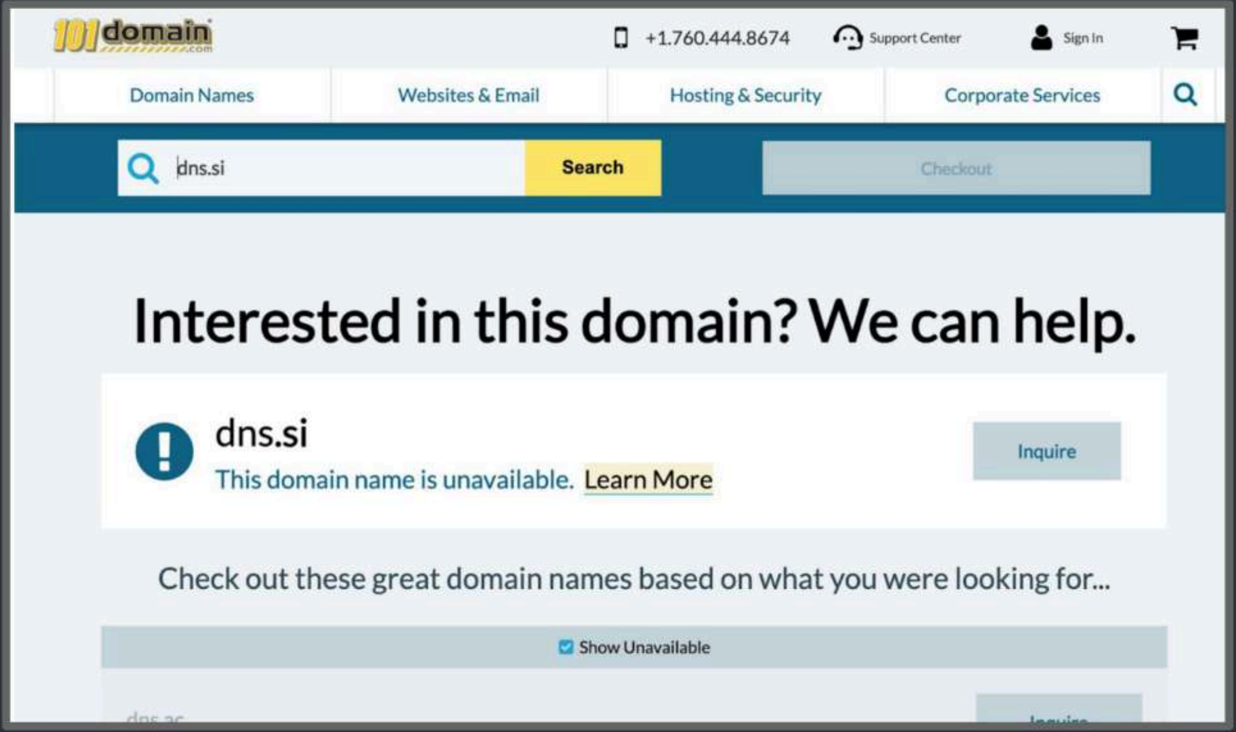
66.49 USD

C... were looking for...

```
lanrat@manhattan:~$ dig -t NS si.

; <<>> DiG 9.10.6 <<>> -t NS si.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19150
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;si.                            IN      NS

;; ANSWER SECTION:
si.                     7196    IN      NS      l.dns.si.
si.                     7196    IN      NS      b.dns.si.
si.                     7196    IN      NS      f.dns.si.
si.                     7196    IN      NS      g.dns.si.
si.                     7196    IN      NS      h.dns.si.
si.                     7196    IN      NS      i.dns.si.
si.                     7196    IN      NS      k.dns.si.

;; Query time: 47 msec
;; SERVER: 2607:f598:ba6f:101::1#53(2607:f598:ba6f:101::1)
;; WHEN: Fri Nov 05 12:59:08 PDT 2021
;; MSG SIZE  rcvd: 147

lanrat@manhattan:~$
```

Finding: .si

~5 hours later.....



Interested in this domain? We can help.

dns.si

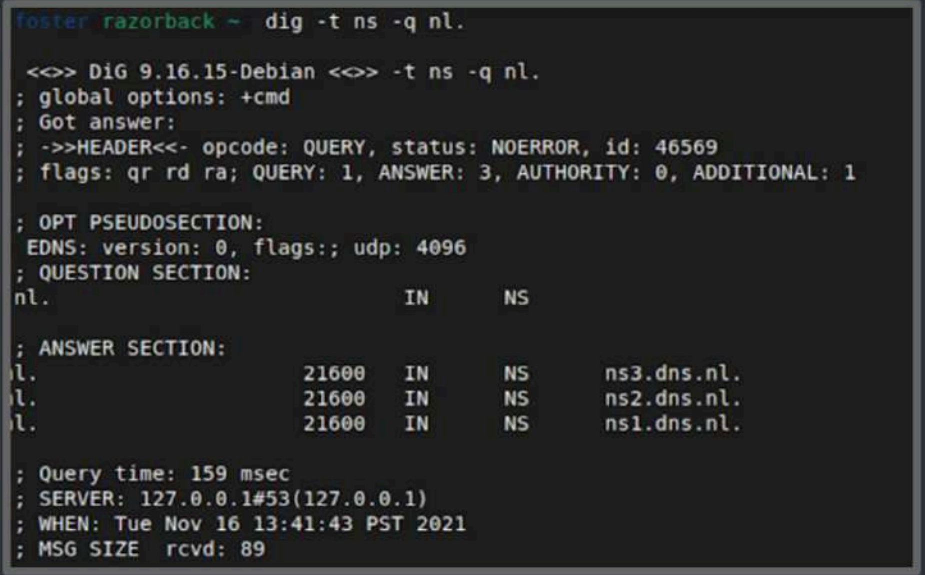
This domain name is unavailable. Learn More

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

Finding: .nl

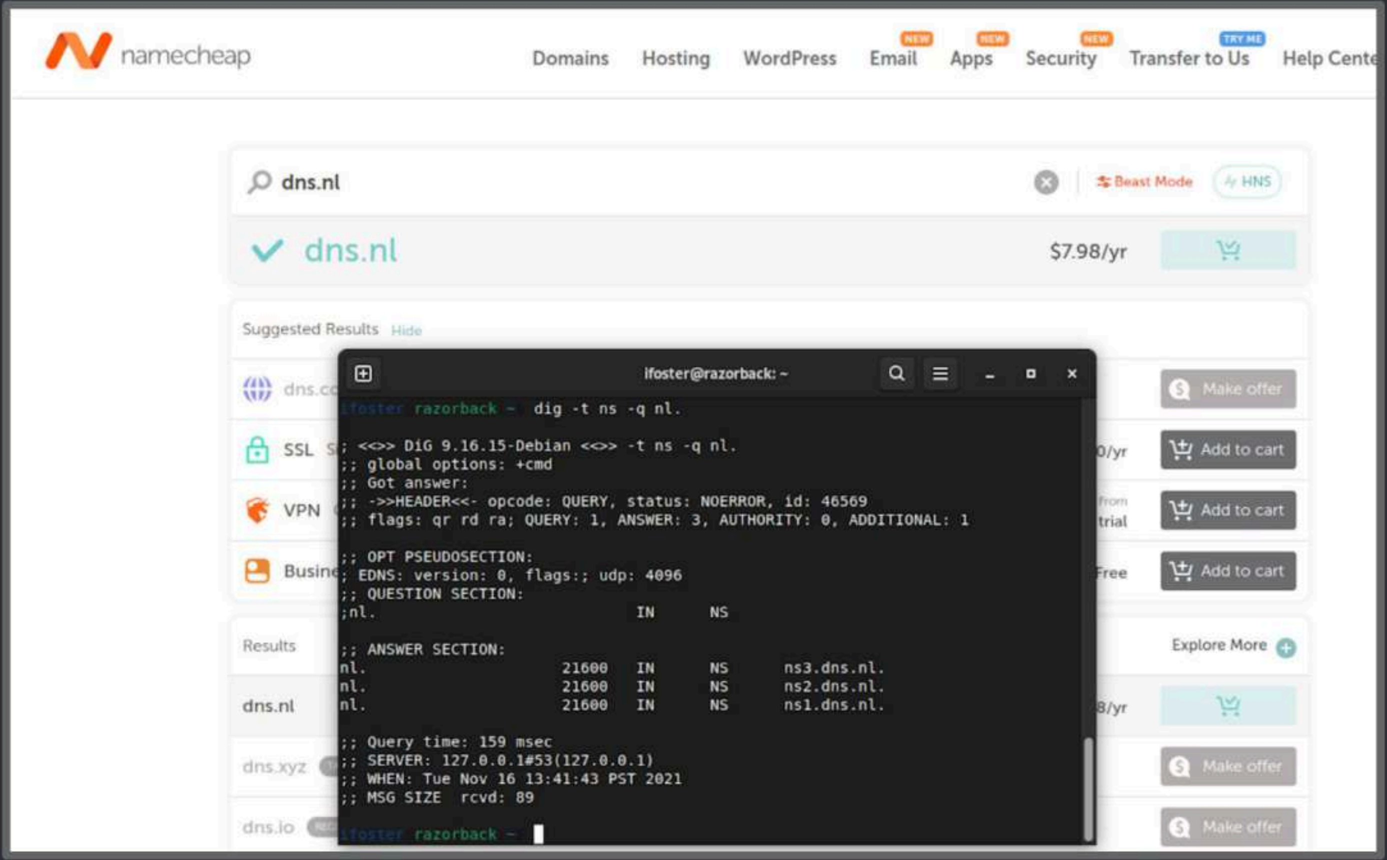
November 16th, 2021, dns.nl, which is the domain used for all authoritative nameservers starts to appear as registerable....

Same as .si.



```
foster razorback ~  dig -t ns -q nl.

 <<>> DiG 9.16.15-Debian <<>> -t ns -q nl.
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46569
; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

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

; Query time: 159 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: Tue Nov 16 13:41:43 PST 2021
; MSG SIZE  rcvd: 89
```

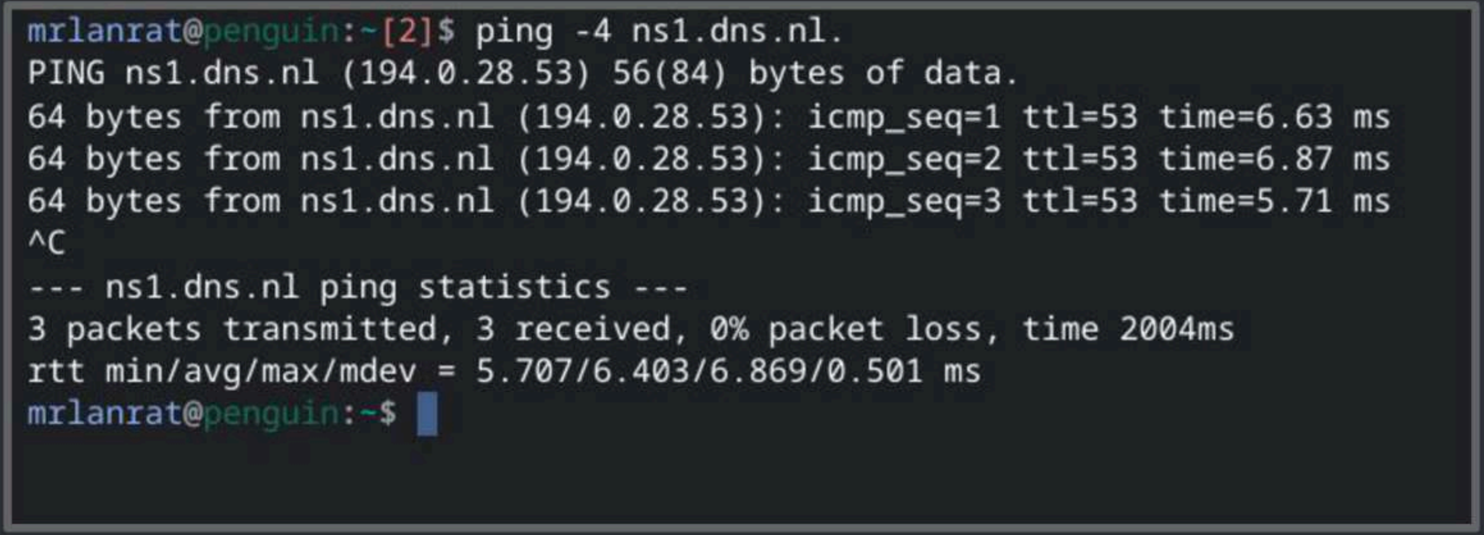
Finding: .nl



```
lfoster razorback ~  dig -t ns -q nl.

; <<>> DiG 9.16.15-Debian <<>> -t ns -q nl.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46569
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

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

;; Query time: 159 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 16 13:41:43 PST 2021
;; MSG SIZE  rcvd: 89

lfoster razorback ~
```

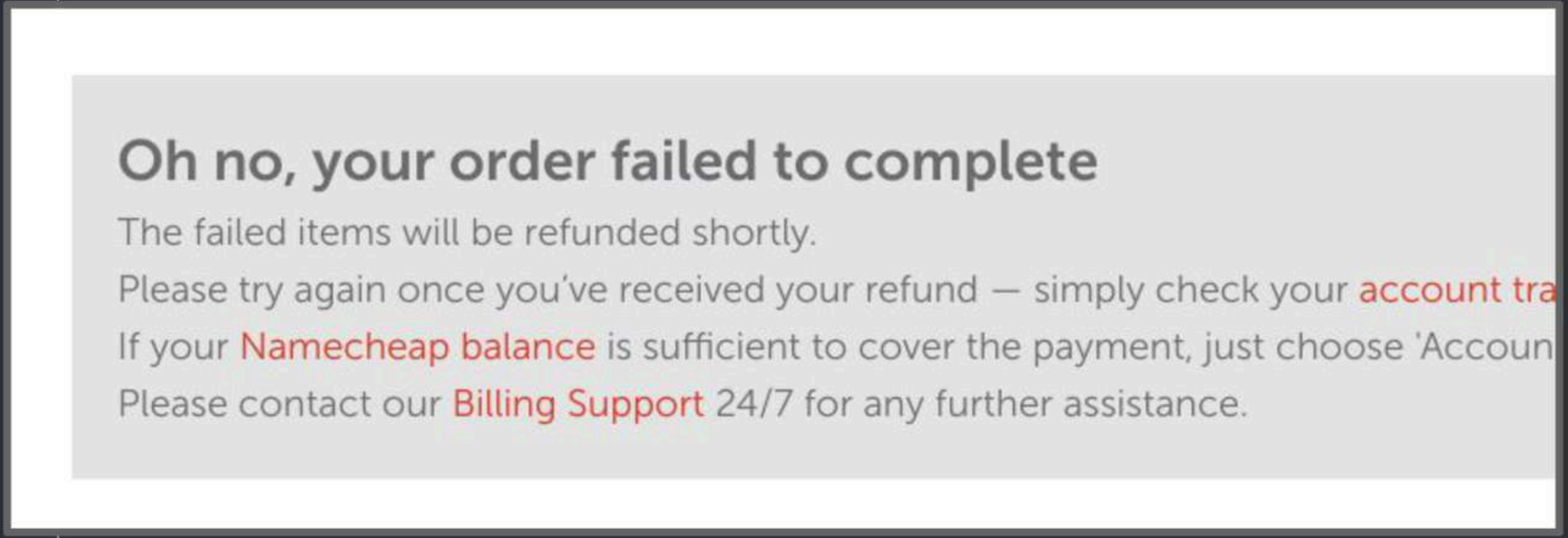
Findings: .nl

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:~$
```

Finding: .nl



Oh no, your order failed to complete

The failed items will be refunded shortly.

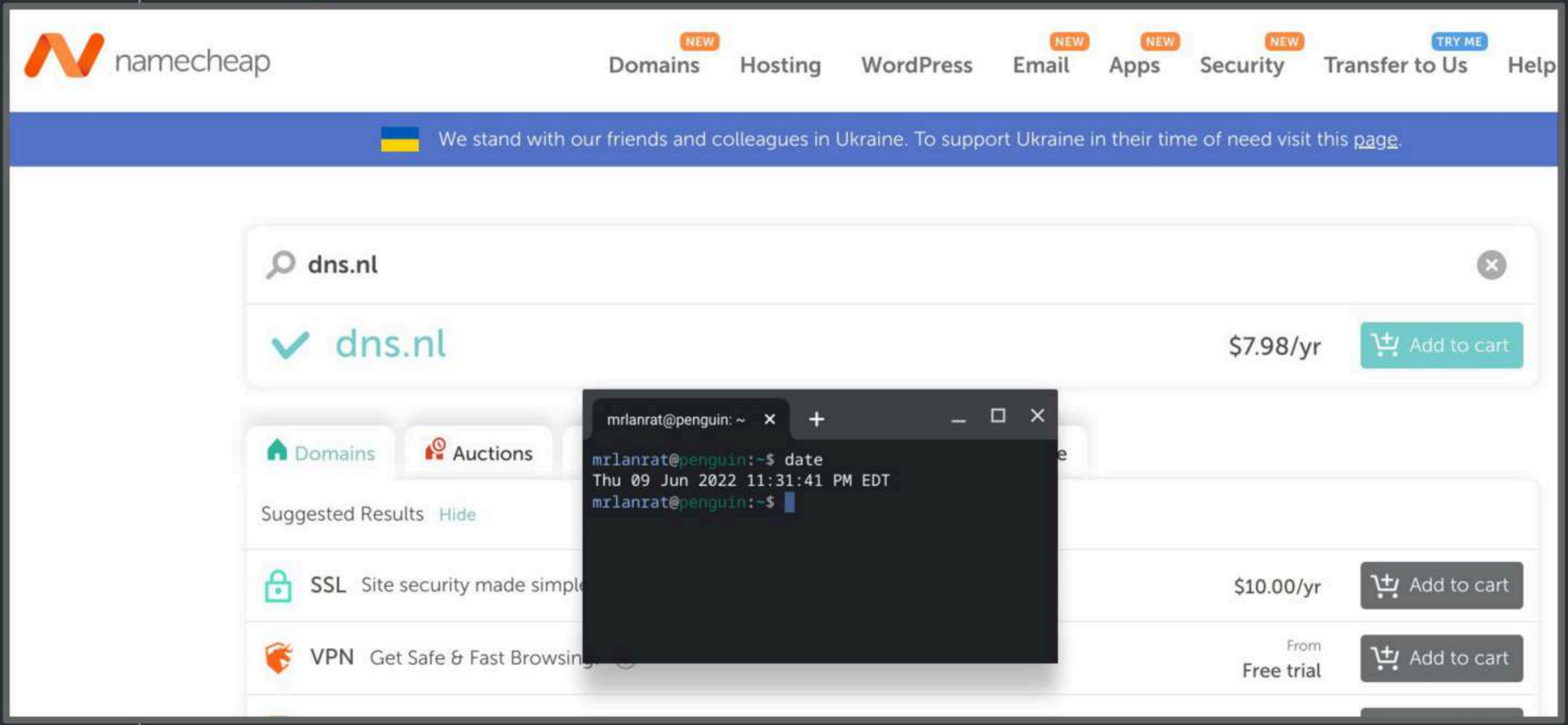
Please try again once you've received your refund — simply check your account tra

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

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

dns.nl started resolving again...

Findings: .nl



We stand with our friends and colleagues in Ukraine. To support Ukraine in their time of need visit this page.

dns.nl

✓ dns.nl $7.98/yr Add to cart

SSL Site security made simpl $10.00/yr Add to cart

VPN Get Safe & Fast Browsin From Free trial Add to cart

```
mrlanrat@penguin:~$ date
Thu 09 Jun 2022 11:31:41 PM EDT
mrlanrat@penguin:~$ 
```

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

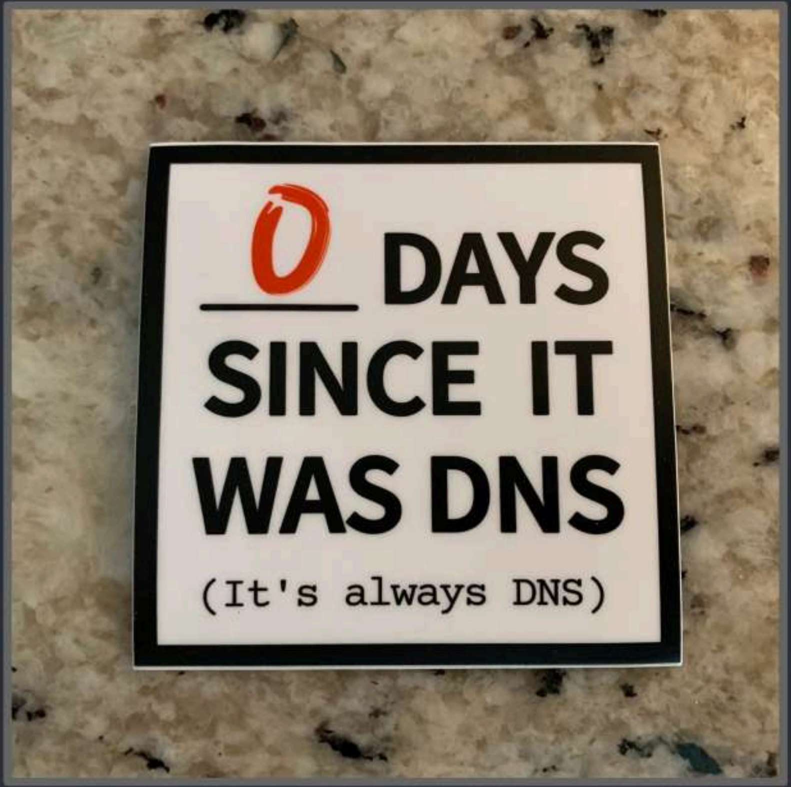
Future Work

- 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

generic	1245
country code	316
sponsored	14
test	11
generic-restricted	3
infrastructure	1
reserved	4

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