“Alternative” TLD Traffic at the Root

Siôn Lloyd, Carlos Gañán and Samaneh Tajalizadeh khoob

ICANN DNS Symposium

5th September 2023
“Alternative” TLDs

Some background and examples
What are we talking about?

TLDs which are not in the DNS root

Current systems commonly use blockchain
  a.k.a. “decentralised DNS”

Integrated into some apps (commonly crypto currency related)

Also some browsers (e.g. Opera, Brave)

Some open recursive support (e.g. OpenNIC)
Example services/offerings

- EmerCoin
  - .bazar, .coin, .emc, .lib

- Unstoppable domains
  - .crypto, .nft, .blockchain, .bitcoin

- Namecoin
  - .bit

- Ethereum Name Service
  - .eth

not to be confused with

.local

.[TYPO]
Note that...

“Correctly” routed queries will not be seen at the root

Queries via unmodified DNS will get an NXDOMAIN
Examples

Some of these have changed hands for a lot of money, ENS sales include:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Date</th>
<th>Price</th>
<th>US$ (*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>paradigm.eth</td>
<td>October 2021</td>
<td>420ETH</td>
<td>1.5M</td>
</tr>
<tr>
<td>pjfi.eth</td>
<td>September 2022</td>
<td>350ETH</td>
<td>463k</td>
</tr>
<tr>
<td>000.eth</td>
<td>July 2022</td>
<td>300ETH</td>
<td>317k</td>
</tr>
</tbody>
</table>

Other schemes too:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Date</th>
<th>US$</th>
</tr>
</thead>
<tbody>
<tr>
<td>business.crypto</td>
<td>2022</td>
<td>121k</td>
</tr>
<tr>
<td>john.crypto</td>
<td>2022</td>
<td>30k</td>
</tr>
<tr>
<td>888.nft</td>
<td>2022</td>
<td>26k</td>
</tr>
</tbody>
</table>

(* value at time of purchase)
Traffic seen at IMRS

Compare traffic between example TLDs and other “non-existent” TLDs

Why do we see this traffic? Misdirected queries
What do we see at IMRS?

Measurements via DNS Magnitude

https://magnitude.research.icann.org/

Occasional appearances in top 2,000; but well below requests for common services, names and filetypes.

<table>
<thead>
<tr>
<th>TLD</th>
<th>Nº Requests</th>
<th>Nº Networks</th>
<th>Magnitude</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>1,250,377,215</td>
<td>1,071,463</td>
<td>9.693</td>
<td>1</td>
</tr>
<tr>
<td>.local</td>
<td>740,087,978</td>
<td>249,520</td>
<td>8.675</td>
<td>11</td>
</tr>
<tr>
<td>.onion</td>
<td>2,005,084</td>
<td>37,579</td>
<td>7.354</td>
<td>213</td>
</tr>
<tr>
<td>.bit</td>
<td>103,897</td>
<td>2,925</td>
<td>5.571</td>
<td>1,249</td>
</tr>
<tr>
<td>.lib</td>
<td>22,170</td>
<td>1,470</td>
<td>5.091</td>
<td>2,179</td>
</tr>
<tr>
<td>.nft</td>
<td>3,243</td>
<td>591</td>
<td>4.455</td>
<td>4,347</td>
</tr>
<tr>
<td>.bazar</td>
<td>66,841</td>
<td>508</td>
<td>4.349</td>
<td>4,954</td>
</tr>
</tbody>
</table>
Why do we see these queries?

These requests will never get a positive answer

We are **ONLY** seeing misdirected queries…

- Environments where DNS is redirected
- Missing browser plugin
- Browser pre-cache
- Naive requests
- *Etc*…

We will not see “correctly” routed queries
Snapshots are not the whole story – dot local
Requests and Address counts for dot bit

- **Requests**
- **Address Count**

request volume

address count

01-08-2021 01-11-2021 01-02-2022 01-05-2022 01-08-2022 01-11-2022 01-02-2023 01-05-2023 01-08-2023
What does this mean?

We will not see “correctly” routed queries

So we are not directly measuring popularity
And the figures can not be fairly compared to delegated TLDs
(not even clear if they can be compared within themselves)

A drop in requests or addresses seen only means we saw fewer
could be a drop in overall volume
could be better direction of queries

Similarly for an increase in signal

Same arguments for the discontinuities we see
Closer look at EmerCoin & bazar in particular

Look at, e.g. No of addresses, etc

Monthly spike?

Random-looking requests
What is EmerCoin?

EmerCoin is a blockchain which includes “EmerDNS”
   can be resolved by OpenNIC resolvers

~136k DNS entries

~83.1k “valid” entries
   ~7k in other TLDs (like dot x, which also exists on
   unstoppable domains) and will not resolved by
   OpenNIC

~12.2k valid dns (A, AAAA, TXT, etc.)
What do we see for EmerCoin?

For the entries we’d expect OpenNIC to handle

<table>
<thead>
<tr>
<th>TLD</th>
<th>Valid Entries</th>
<th>Valid DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>coin</td>
<td>36,114</td>
<td>1,831</td>
</tr>
<tr>
<td>bazar</td>
<td>15,794</td>
<td>5,161</td>
</tr>
<tr>
<td>lib</td>
<td>13,305</td>
<td>1,578</td>
</tr>
<tr>
<td>emc</td>
<td>12,096</td>
<td>1,131</td>
</tr>
</tbody>
</table>
What do we see for EmerCoin?

In one week in August we see:

<table>
<thead>
<tr>
<th>TLD</th>
<th>Queries</th>
<th>Addresses</th>
<th>QNAMES</th>
<th>Address / QNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>coin</td>
<td>61,631</td>
<td>1,632</td>
<td>7,370</td>
<td>13,178</td>
</tr>
<tr>
<td>bazar</td>
<td>941,364</td>
<td>673</td>
<td>71,285</td>
<td>422,604</td>
</tr>
<tr>
<td>lib</td>
<td>110,857</td>
<td>2,443</td>
<td>5,211</td>
<td>10,192</td>
</tr>
<tr>
<td>emc</td>
<td>63,735</td>
<td>674</td>
<td>1,753</td>
<td>4,285</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TLD</th>
<th>Queries for names on chain</th>
<th>“NXDomain”</th>
<th>Queries for entries with DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>coin</td>
<td>3,832</td>
<td>94%</td>
<td>1,519</td>
</tr>
<tr>
<td>bazar</td>
<td>31,876</td>
<td>97%</td>
<td>26,213</td>
</tr>
<tr>
<td>lib</td>
<td>19,535</td>
<td>82%</td>
<td>5,022</td>
</tr>
<tr>
<td>emc</td>
<td>2,727</td>
<td>96%</td>
<td>60</td>
</tr>
</tbody>
</table>
Requests and Address counts for dot bazar

- Blue line: Requests
- Red line: Address Count

Timeline:
- 01-08-2021
- 01-11-2021
- 01-02-2022
- 01-05-2022
- 01-08-2022
- 01-11-2022
- 01-02-2023
- 01-05-2023
- 01-08-2023
Why is dot bazar interesting?

Has a relatively high number of requests for the number of IP addresses

Random looking domain names

Monthly spikes in request volumes

It turns out this particular TLD is used by a domain generation algorithm (DGA)

Known as bazarloader (part of trickbot).
Bazarloader DGA

Look at the DGA (why have a DGA if the “domains” can’t be taken down?)

Do we see what we would expect?

Are any of the “domains” registered?
Bazarloader

Initially seen in early 2020 it used hardcoded dot bazar domains, then added DGA

Aside: why? If decentralised DNS can not be taken down what does a DGA add?

Generate domains on a monthly cycle

(https://bin.re/blog/the-dga-of-bazarbackdoor)
Bazarloader

A few variations/seeds; 3 listed in DGArchive

“v1” creates 2,160 dom/month
“v3” creates 12,996 &
“v4” creates 31,768 dom/month

Three August 2023 domains registered in one transaction
2 from v4 (+1 v3 from a year ago)
1 from v3

Also 3 other dot bazar domains with the same properties, including DNS – unknown variant?
Bazarloader

Further paranoia:

IP address returned xor’d with “0xFE” to get the real IP

127.0.0.1 $\rightarrow$ 129.254.254.255

March 2022:

Google’s Threat Analysis Group (TAG) reported actors replacing bazarloader with a new, more advanced loader dubbed “BUMBLEBEE”
Conclusions
Conclusions

- While still niche in overall terms, decentralized domains are taken seriously in their own markets

- We do see traffic for them at the root
  - but the levels are low
  - hard to draw too many conclusions

- Even have DGA presence - dot bazar
Thank You and Questions

Visit us at icann.org
Email: sion.lloyd@icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
soundcloud/icann
instagram.com/icannorg