“Alternative” TLD Traffic at the Root

Siôn Lloyd, Carlos Gañán and Samaneh Tajalizadehkhoob

ICANN DNS Symposium

5th September 2023

ICANN

“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:

Domain	Date	Price	US$ (*)
paradigm.eth	October 2021	420ETH	1.5M
pjfi.eth	September 2022	350ETH	463k
000.eth	July 2022	300ETH	317k

Other schemes too:

Domain	Date	US$
business.crypto	2022	121k
john.crypto	2022	30k
888.nft	2022	26k

(* 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.

TLD	№ Requests	№ Networks	Magnitude	Rank
.com	1,250,377,215	1,071,463	9.693	1
.local	740,087,978	249,520	8.675	11
.onion	2,005,084	37,579	7.354	213
.bit	103,897	2,925	5.571	1,249
.lib	22,170	1,470	5.091	2,179
.nft	3,243	591	4.455	4,347
.bazar	66,841	508	4.349	4,954

Why do we see these queries?

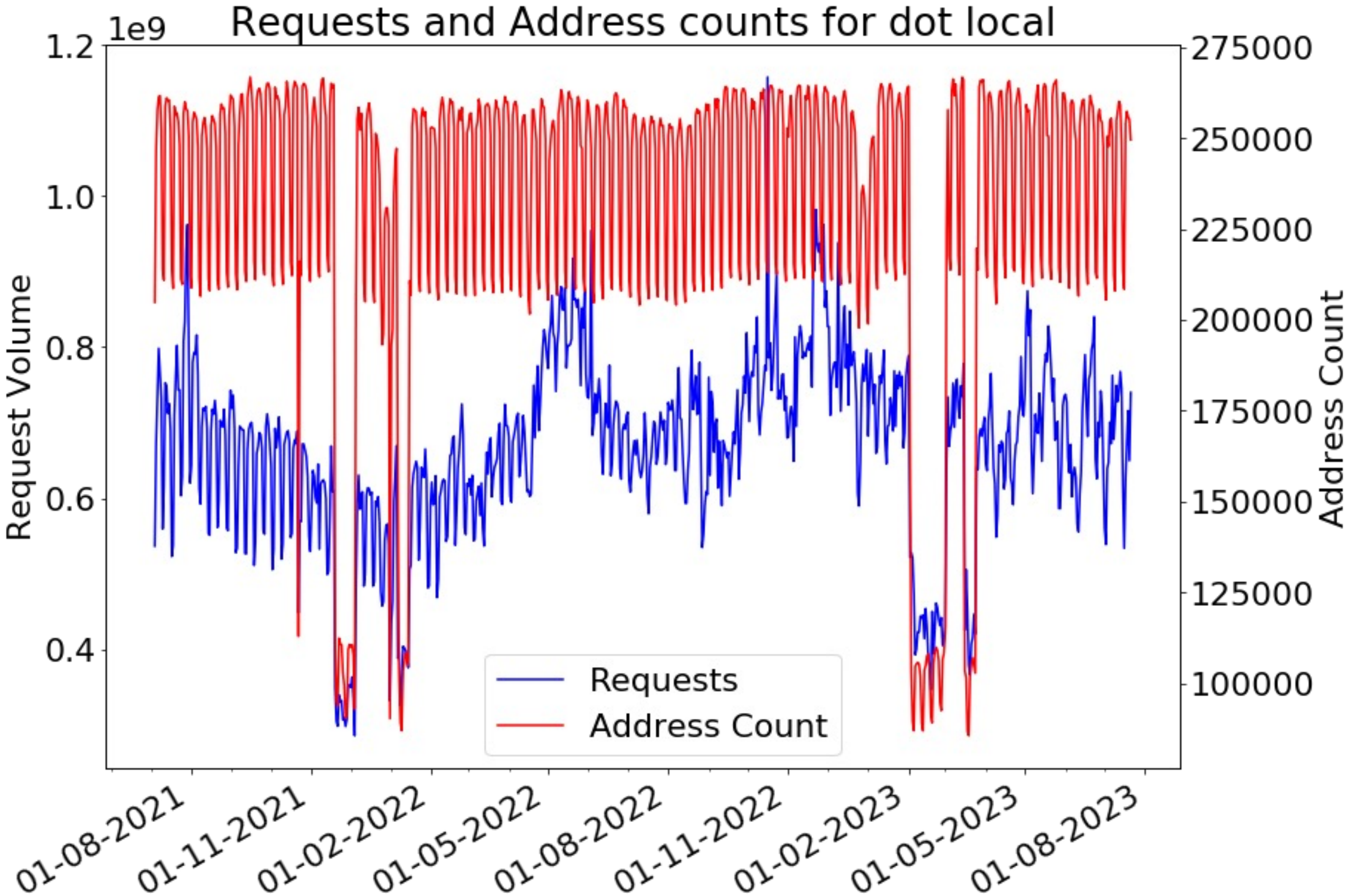
These requests will never get a positive answer

We are **ONLY** seeing misdirected queries…

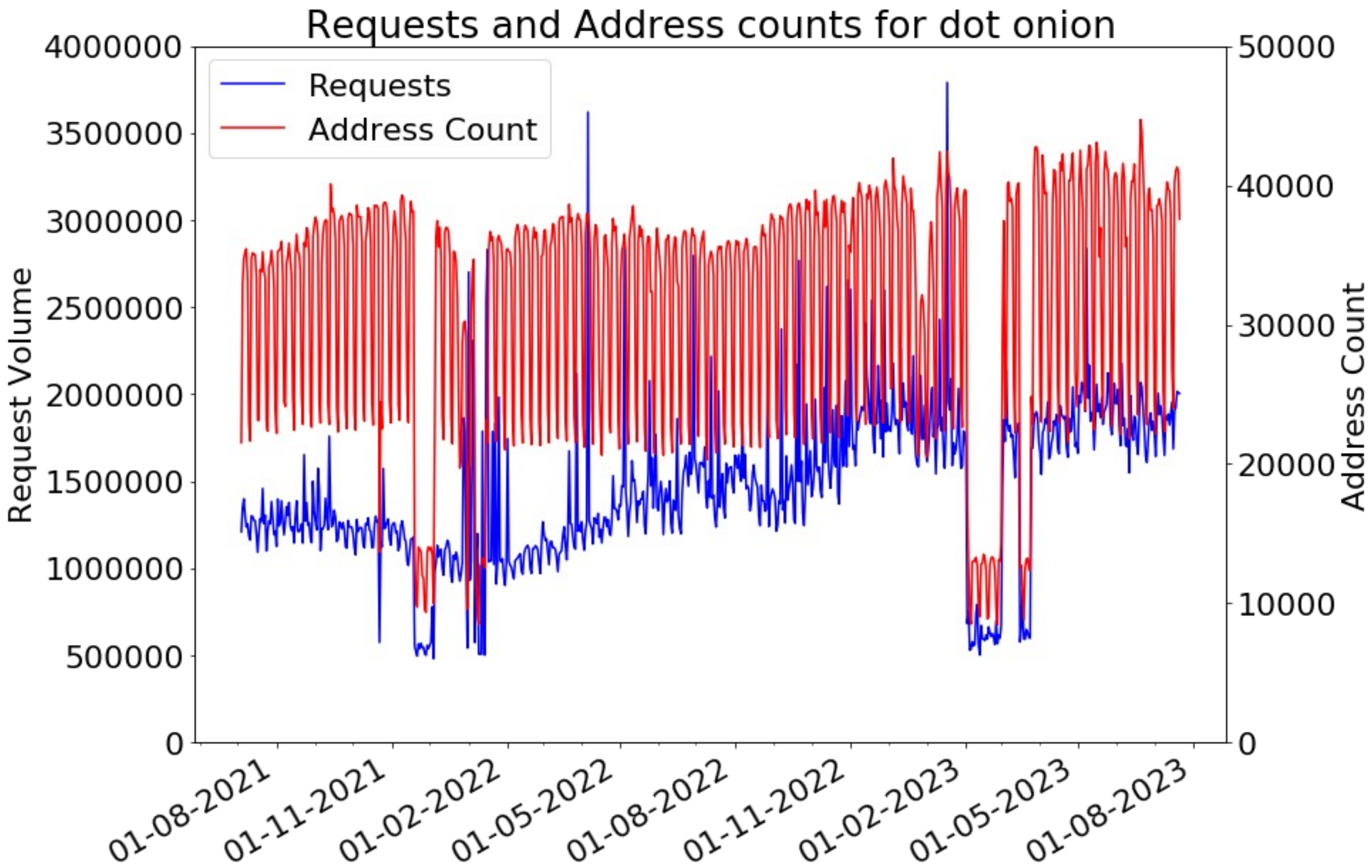
- Environments where DNS is redirected
- Missing browser plugin
- Browser pre-cache
- Naive requests
- *Etc…*

We will not see “correctly” routed queries

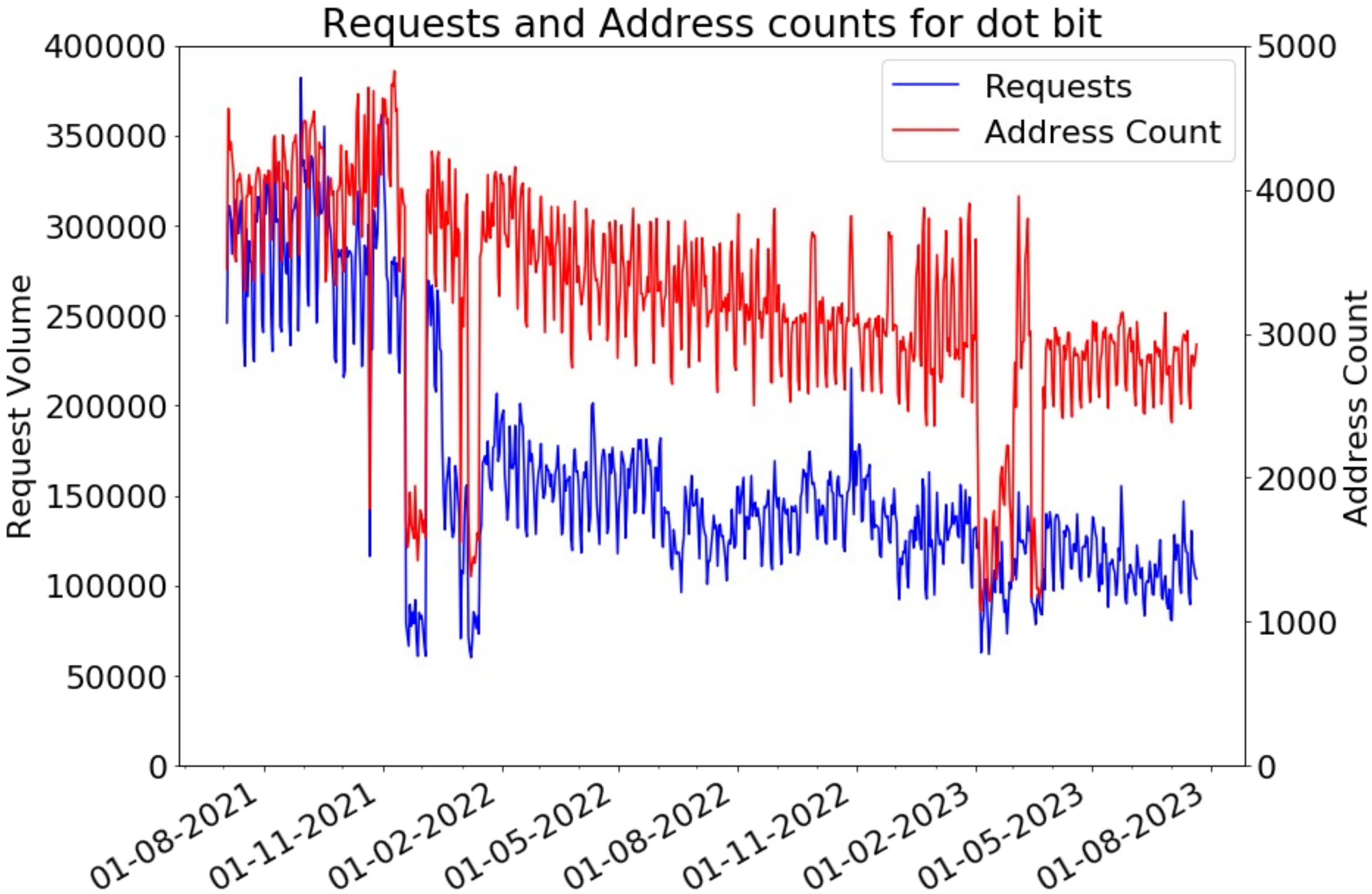
Snapshots are not the whole story – dot local



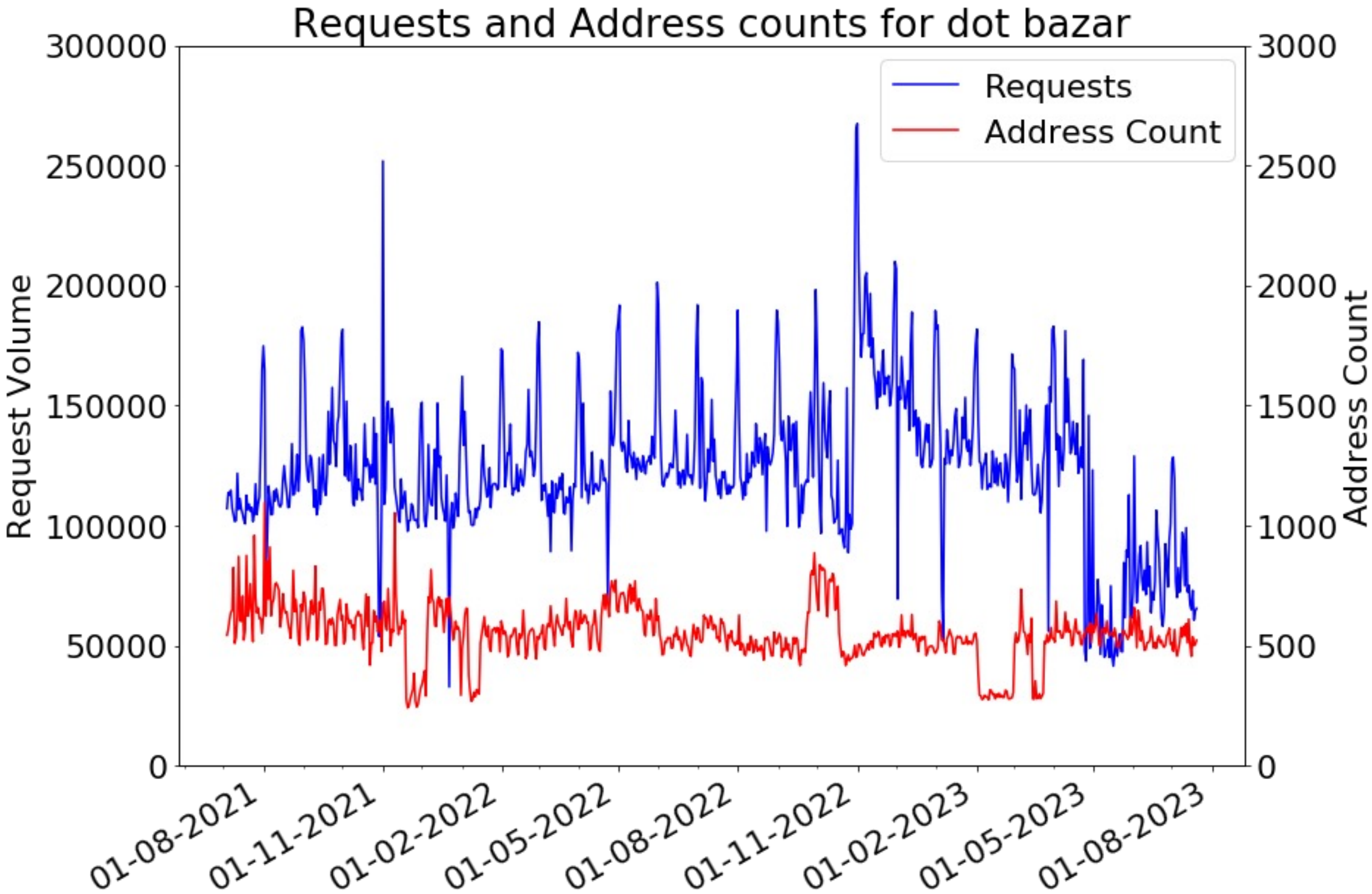
dot onion


Requests and Address counts for dot onion
Requests
Address Count
Request Volume
Address Count
0
500000
1000000
1500000
2000000
2500000
3000000
3500000
4000000
0
10000
20000
30000
40000
50000
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

dot bit


Requests and Address counts for dot bit
Requests
Address Count
Request Volume
Address Count
0
50000
100000
150000
200000
250000
300000
350000
400000
0
1000
2000
3000
4000
5000
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

dot bazar


Requests and Address counts for dot bazar
Requests
Address Count
Request Volume
Address Count
300000
250000
200000
150000
100000
50000
0
3000
2500
2000
1500
1000
500
0
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

TLD	Valid Entries	Valid DNS
coin	36,114	1,831
bazar	15,794	5,161
lib	13,305	1,578
emc	12,096	1,131

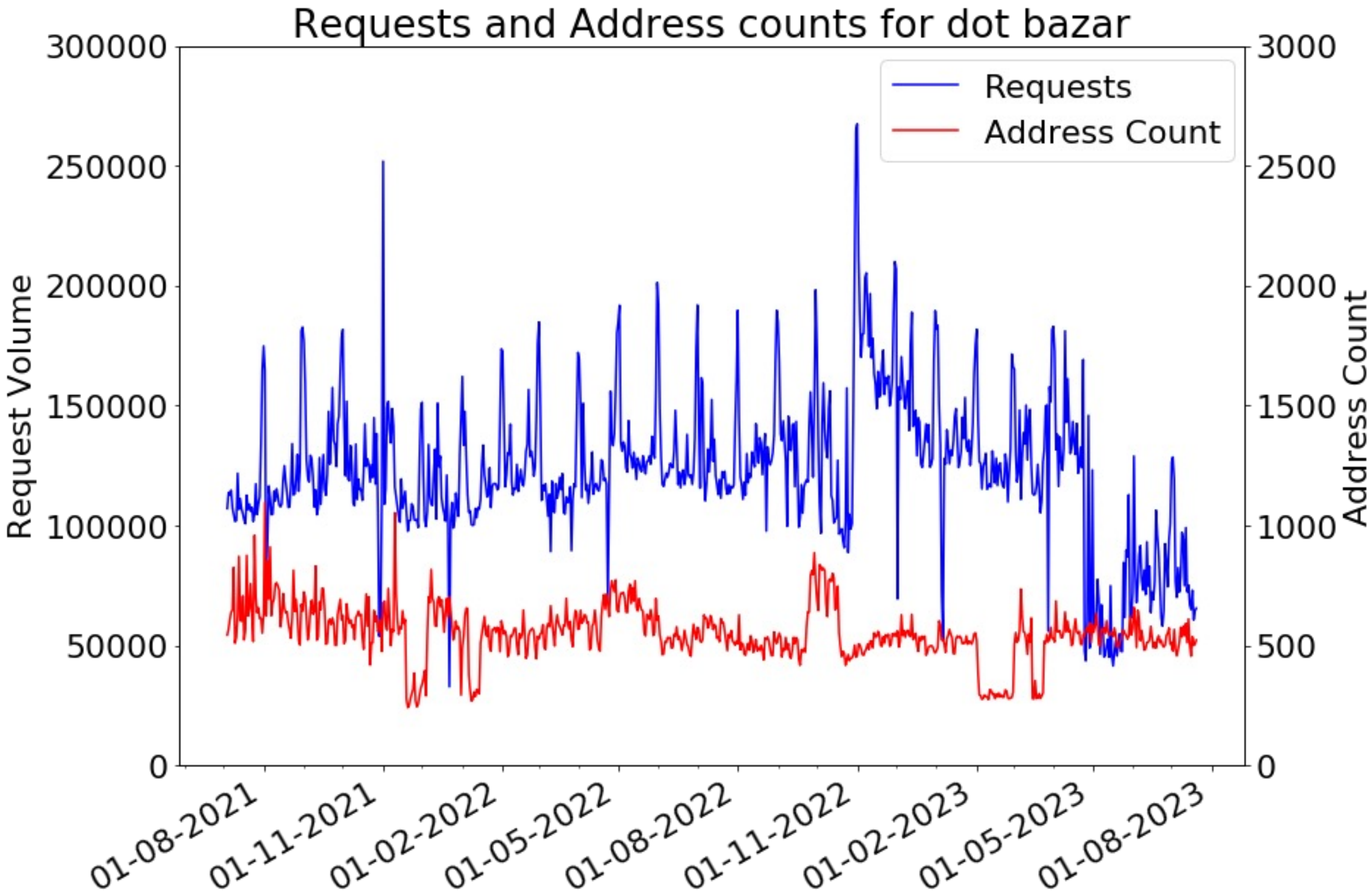
What do we see for EmerCoin?

In one week in August we see:

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

TLD	Queries for names on chain	"NXDomain"	Queries for entries with DNS
coin	3,832	94%	1,519
bazar	31,876	97%	26,213
lib	19,535	82%	5,022
emc	2,727	96%	60

dot bazar


Requests and Address counts for dot bazar
Requests
Address Count
Request Volume
Address Count
300000
250000
200000
150000
100000
50000
0
3000
2500
2000
1500
1000
500
0
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 -> 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

Engage with ICANN

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