Lost in Transit: A First Look at Residual Traffic from Transient Domains

Raffaele Sommese

University of Twente

ICANN 83 Prague

A quick recap in four slides

DarkDNS: Revisiting the Value of Rapid Zone Update

Raffaele Sommese
University of Twente
Enschede, The Netherlands
r.sommese@utwente.nl

Gautam Akiwate
Stanford University
Stanford, CA, USA
gakiwate@cs.stanford.edu

Antonia Affinito
University of Twente
Enschede, The Netherlands
a.affinito@utwente.nl

Moritz Müller
SIDN Labs
Arnhem, The Netherlands
University of Twente
Enschede, The Netherlands
moritz.muller@sidn.nl

Mattijs Jonker
University of Twente
Enschede, The Netherlands
m.jonker@utwente.nl

KC Claffy
CAIDA
San Diego, CA, USA
kc@caida.org

Abstract

Malicious actors exploit the DNS namespace to launch spam campaigns, phishing attacks, malware, and other harmful activities. Combating these threats requires visibility into domain existence, ownership and nameservice activity that the DNS protocol does not itself provide. To facilitate visibility and security-related study of the expanding gTLD namespace, ICANN introduced the Centralized Zone Data Service (CZDS) that shares daily zone file snapshots

1 Introduction

Malicious actors exploit (abuse) the DNS namespace to launch spam campaigns, phishing attacks, malware, and other harmful activities. In many dimensions the DNS ecosystem is more opaque than other aspects of Internet transport. Unlike BGP, DNS is a pull protocol, so learning internal dynamics requires an entry point *i.e.,* a domain name. Without knowing this entry point, any abuse that lies behind a domain remains opaque to everyone except the targets.

TRANSIENT DOMAINS!?...

By leveraging CT Logs (stream) we demonstrated that:

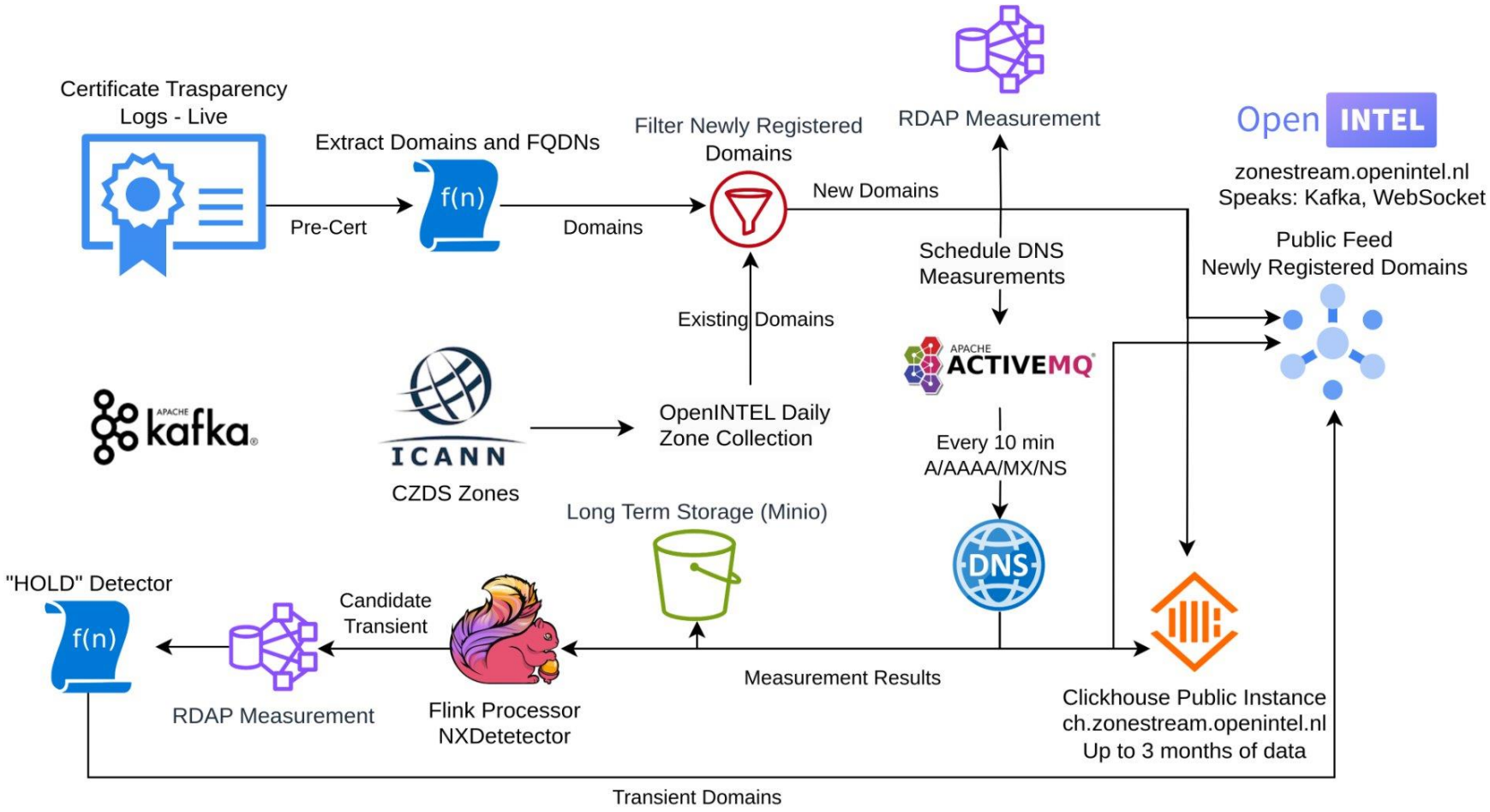
- We detected 42% of the newly registered domains in gTLDs **before** they appear in the CZDS snapshot*.
- ~76K domains per day - - almost 1 domain per second.
- ~760 (1%) of our daily detected newly registered domains never appear in the next CZDS snapshot.
- Predominantly malicious!
- With half of them died within their first 6 hours of life.

Analysis conducted in the period: Nov 2023 – Jan 2024.

Blocking those names:

- The paper focused on detecting transient domains in a post-mortem scenario.
- Being able to **block them quicker (after deletion)** can help against **attackers who may leverage caching.**
- How can we detect them as soon as they die?
  - Measuring newly registered domains (every 10 min, for 48h. A/AAAA/NS (@TLDs)/MX).
  - Detect deletion: 3x NXDOMAIN at **TLD Level.**
  - Issuing 2 RDAP requests, one when the domain is first detected, one when the domain is marked as deleted.
  - Checking RDAP responses for status **(sever hold, client hold)**.

Building a blocklist....



...and now: What's new!?

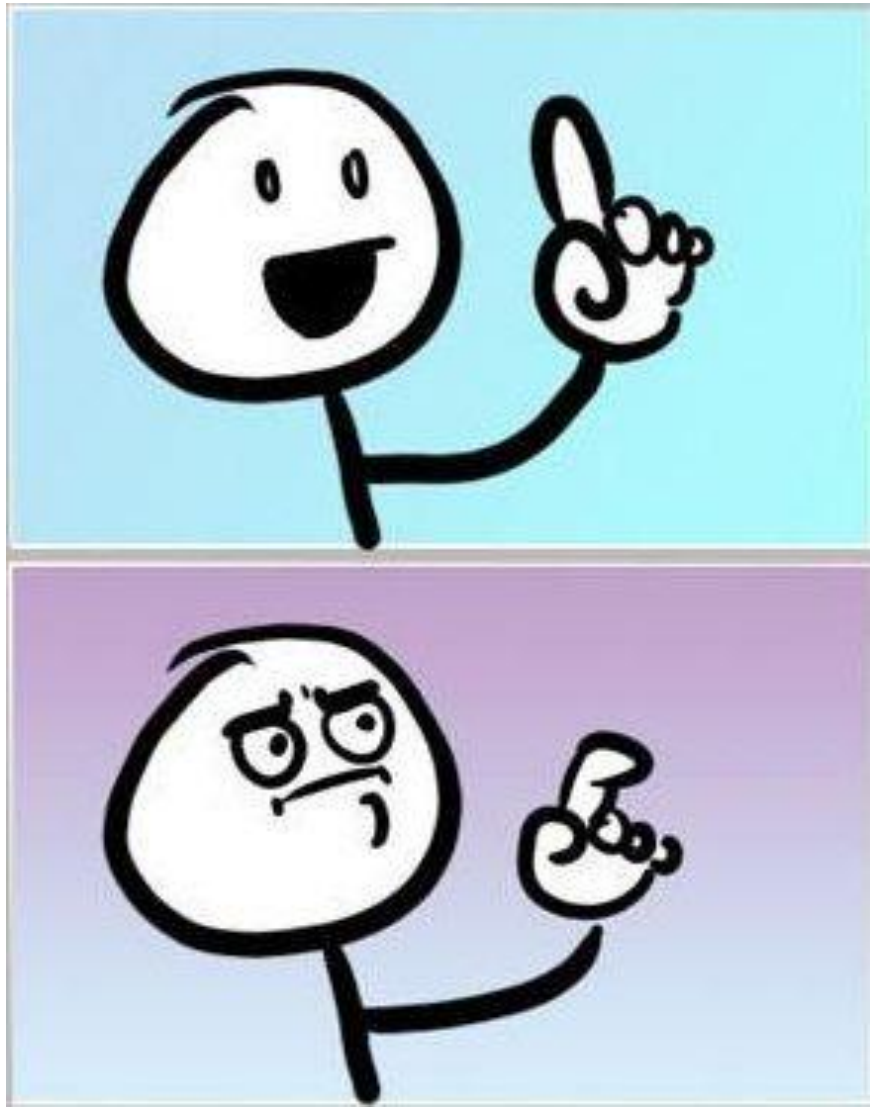
https://blocklist.dacs.utwente.nl/transient-domains

~700 deleted transient domains a day

- Updated every 60 seconds
- Deleted (transient) domains are blocklisted for 24 hours (to avoid that residual attack activity may leverage recursive resolvers caching).
- We chose 24 hours as **a safe margin**: most recursive resolvers in the wild honor 24 hours as maximum TTL/caching period (and domains could be potentially **re-registered** for benign purposes)


WE ARE GOING TO BLOCK
THOSE TRANSIENT DELETED DOMAINS
AFTER ALL THERE IS NO
RESIDUAL TRAFFIC ON THEM
THERE IS NO RESIDUAL
TRAFFIC ON THEM, RIGHT?
imgflip.com

Well...
not really

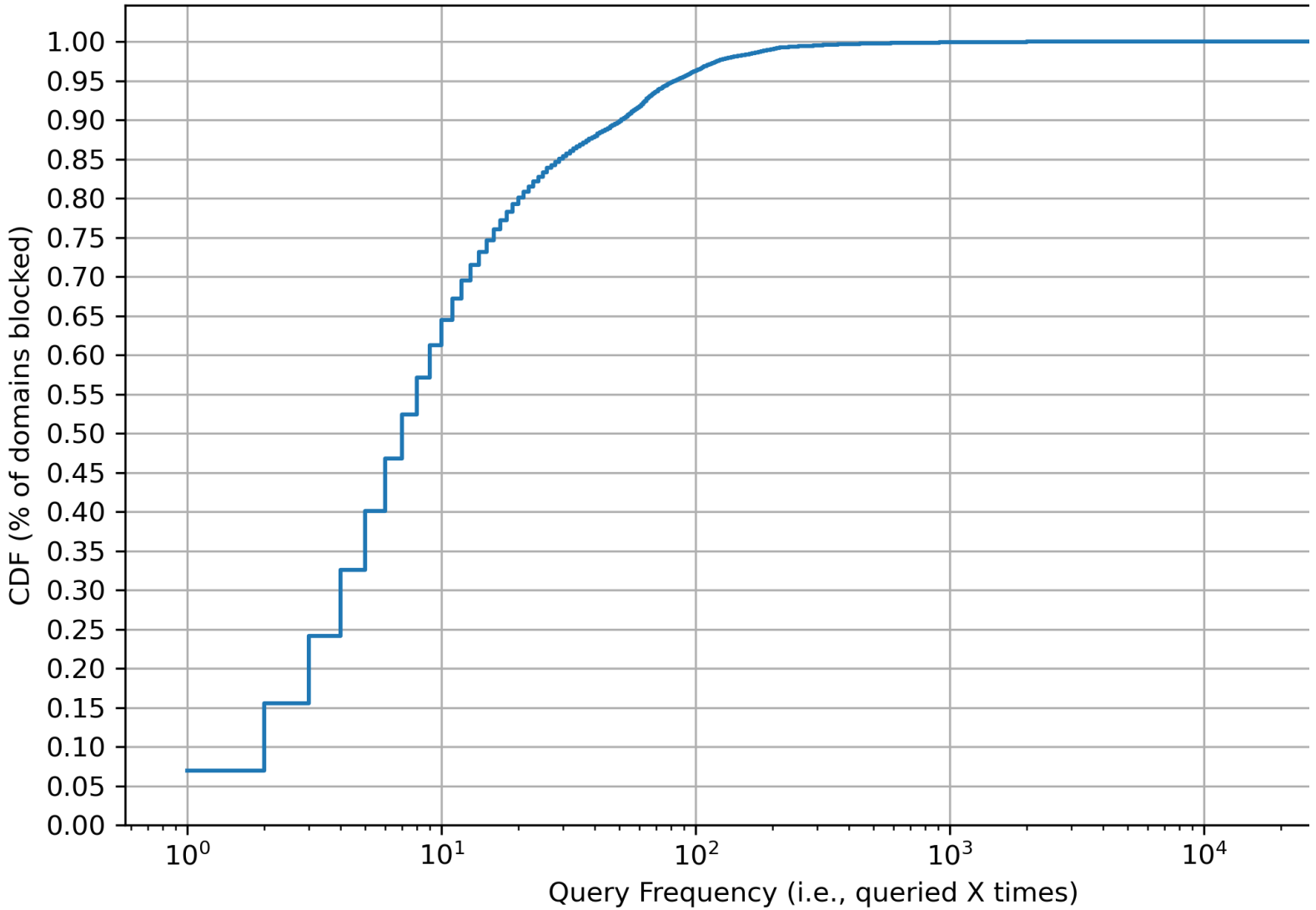


Residual traffic on Transient Domains

- **Quad9** deployed our blocklist as part of their threat intelligence feeds.
- Providing us with **anonymized threat intelligence statistics.**
- Enabling **analysis of the residual traffic** over those transient domains (after their deletion).
- Over a 2-month period (Apr-May 2025), **we blocked ~42K domains.**
- **33K (78%) of these received at least 1 query!**
- And those should have been domains that no one cared about!? Right?

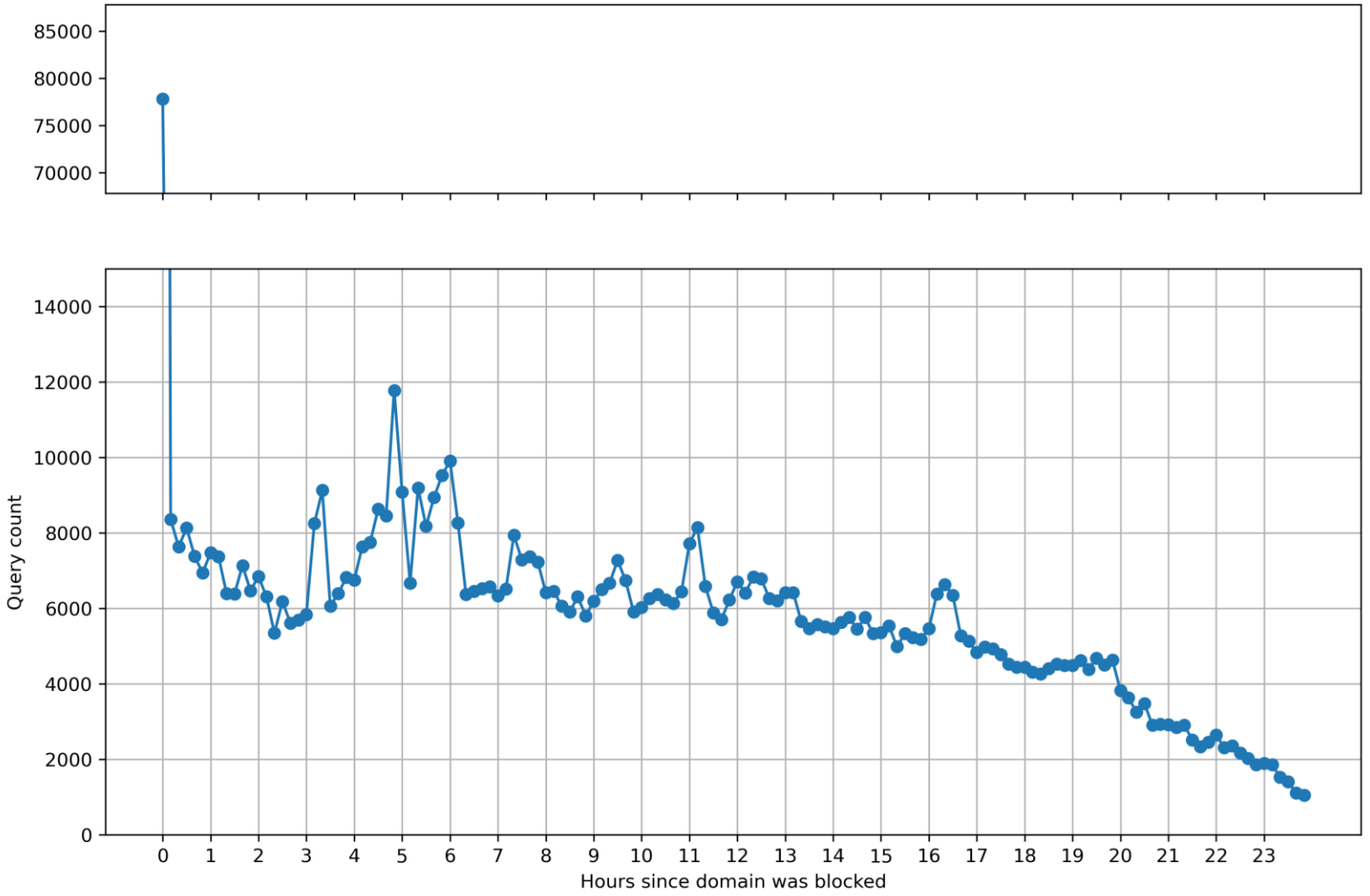
Queries frequency

- Most of those domains (~60%) get queried less than 10 times in 24 hours.
- However, a notable 4% get queried more than 100 times.
- Why? We will look at them later.



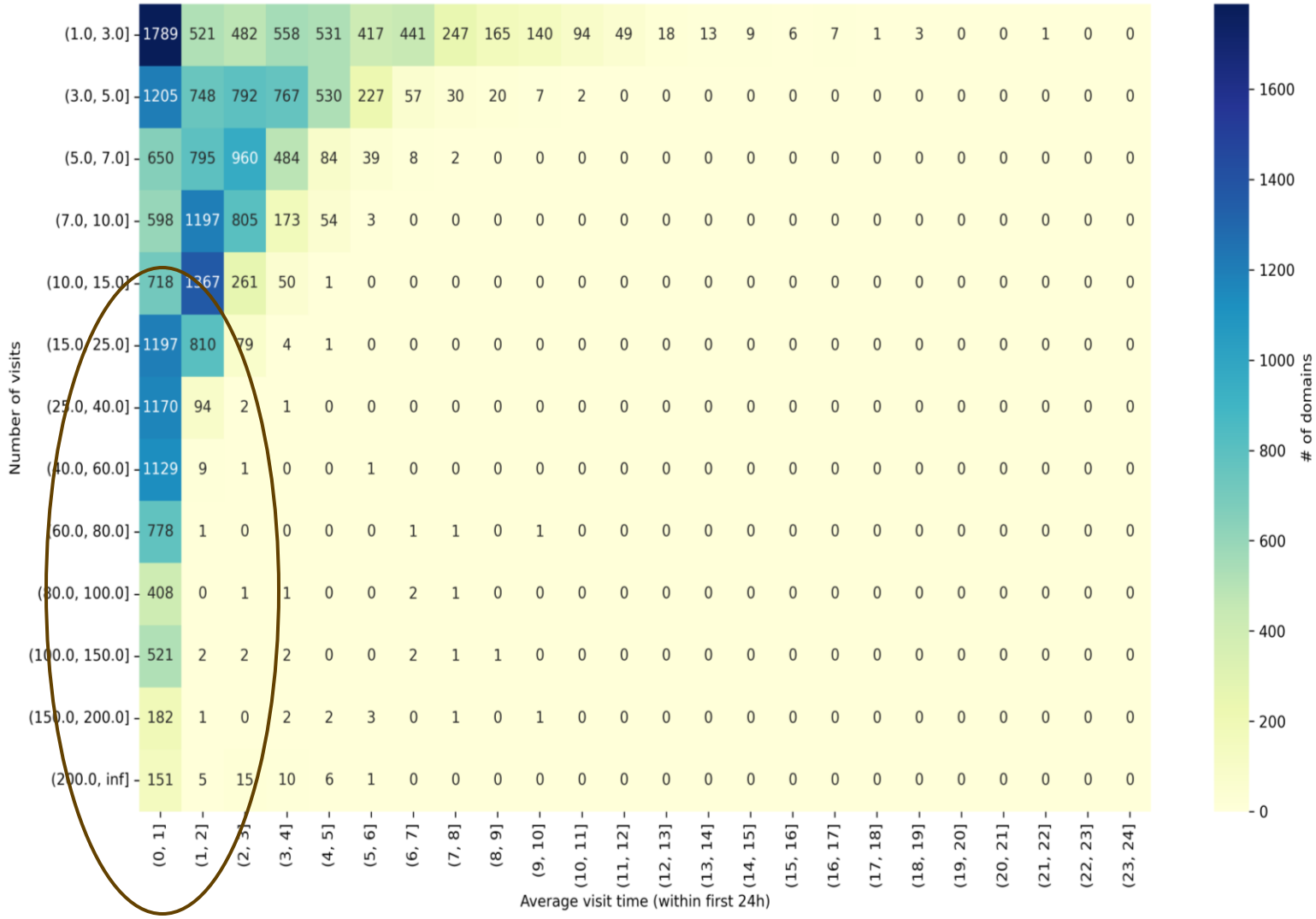
Query Timing

- Most of the queries happen immediately after the blocking.
- However, there is a long tail of queries for the remaining 24 hours.
- Remember: Domains get removed from the blocklist after 24 hours (for scalability)



Queried regularly?

- Domains that get queried more often are queried more evenly during the 24-hour block.



A deeper look into some of the top queried domains

mbhbank.one

- Likely a banking impersonation attempt (https://www.mbhbank.com/) with only the www subdomain actively queried.
- **32110 queries** in 24 hours.
- Mostly from Japan, south-east Asia and Ireland.

escueladefutbolcampeones.org

- *Most DMARC And DKIM subdomains*
- *Likely a spam campaign impersonating a legitimate not-for-profit association*
- *Most traffic from the US (~5K queries)*

arborconsult.space

- Subdomains:_ep, www, charles._domainkey, default._bimi, _dmarc, _adsp._domainkey, _policy._domainkey, _domainkey
- Likely a spam campaign impersonating arborconsultancy.nl or arborconsult.de or Charles McCorkell arboricultural consultancy.
- **84237 queries** in 24 hours.
- Queried mostly from US, Netherland and Germany (with residual traffic around the globe)

More banking related activity

targobank-verifizieren.com, caixadirectaclienteson.com, gob-postalah.live, gob-postalv.live, paganets.click, ubankdigital.live, gob-trackf.live

- *Mostly Finnish traffic*

bca-bank.club
wise-assesoria.com
suport-wise.com

- *Mostly US traffic*

- *Both with more than **200 subdomains** related to popular banks (e.g., ING Direct, Santander, Revolut, N26, Caixa, and many others).*
- *Looks like a large-scale **payment confirmation phishing** attempt.*
- *~ 1000 queries per domain in the 24 hours block period.*

Where next?

- Investigating TTL of blocked domains to quantify the risk of data remaining in cache of popular resolvers.
  - Possibly exploitable: see Ghost Domain Names: Revoked Yet Still Resolvable (Jiang et al.)
- Behavior before blocking?
  - We only see (telemetry) traffic patterns after the insertion of a domain in the blocklist (which, by design in our system, happens 30 minutes after the domain name is deleted)
  - Investigating traffic patterns before deletion would require a "*grey-listing*" (log, but not block) all the newly registered domains we detect (and then consider only transient).
  - ...maybe not a bad idea!? :)
- Any recursive resolver willing to jump on board?

The benefit of real-time data sharing

- These results demonstrate that faster, more immediate access to real-time data significantly i**mproves the ability to block malicious activity on the Internet.**
- DNS plays a crucial role in this, yet most of our research relies on daily snapshots (e.g., CZDS) to combat abuse.
- We urgently need to rethink the security model of the DNS ecosystem and loudly call on registries, registrars, and all stakeholders to (re)introduce timelier, ideally real-time, access to DNS registration and infrastructural data.
- We need more **DNS transparency!**

An SSAC WP?

- We (KC Claffy and I) are proposing a work party that aims to:
  - Analyze the **security benefits and risks** of reviving the concept of Rapid Zone Updates.
  - Provide more **timely access** to TLD zone changes and/or domain removal information.
  - Investigate the opportunity of **enhanced data sharing of registration data**.
  - Identify and analyze possible approaches to these challenges and possible **technical and legal pitfalls.**
- With the final goal of facilitating **abuse prevention and security research**.
- For the registrar and registry community, researchers, security firms, and policy analysts and developers.

Questions?

Reach me out:

Raffaele Sommese
r.sommese@utwente.nl
University of Twente

https://blocklist.dacs.utwente.nl/transient-domains