Is Protective DNS Blocking the Wild West?

https://research.wiscnet.net/~plonka/pubs.html

David Plonka
plonka@wiscnet.net
WiscNet
Madison, Wisconsin, USA

Branden Palacio
branden.palacio@marquette.edu
Marquette University Milwaukee, Wisconsin, USA

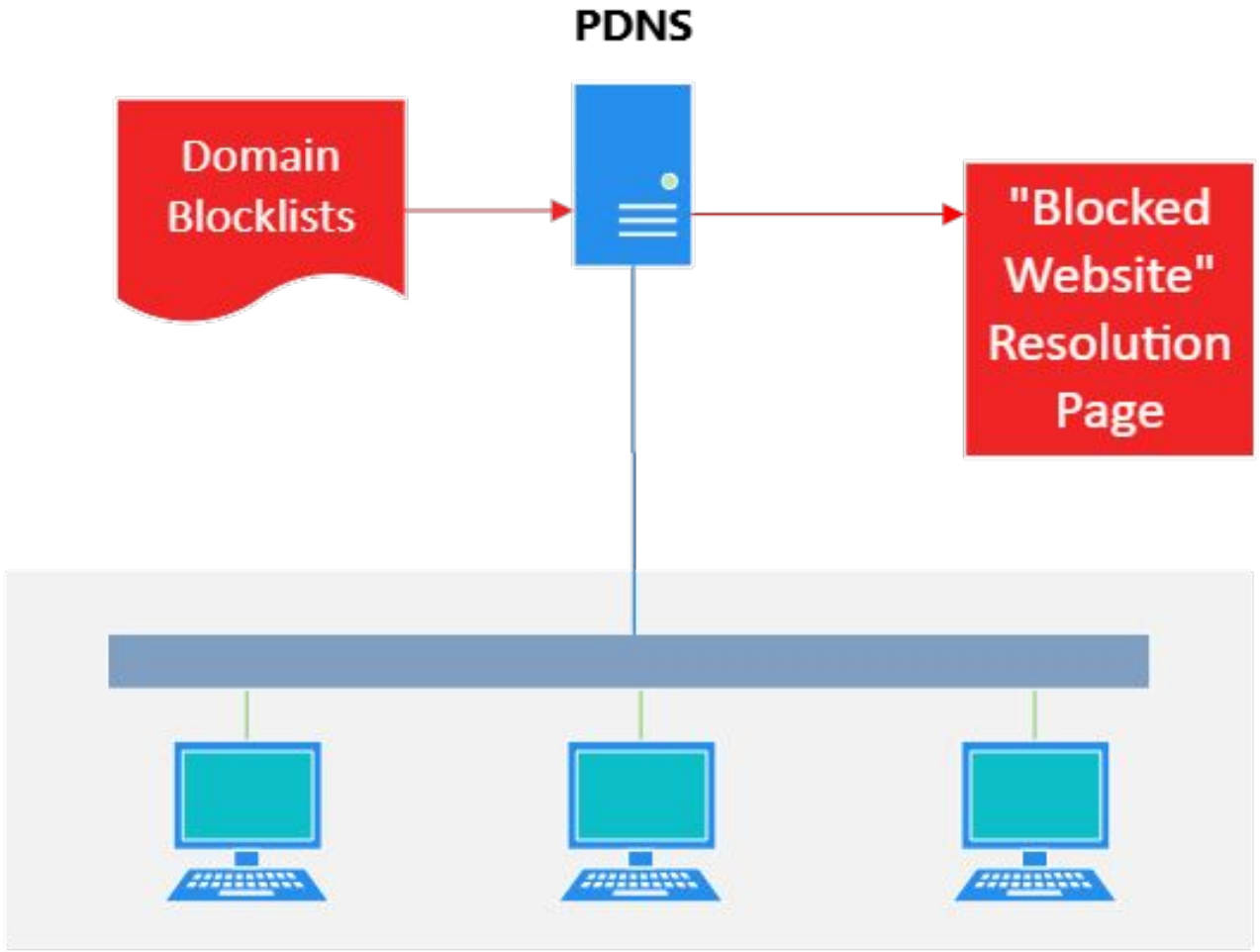
Debbie Perouli
despoina.perouli@marquette.edu
Marquette University Milwaukee, Wisconsin, USA

Protective DNS (PDNS)

Why do they Exist?

What methods do they employ?

What are the limitations?



PDNS Solutions

- Commercial
  - Cloudflare 1.1.1.1 for families
  - Cisco – Umbrella DNS SE
  - Palo Alto – Advanced DNS Security
  - MS-ISAC MDBR
- Freely Available
  - Phishing & Scam Domain Names (OTX)
  - HaGeZi Threat Intelligence Feed (TIF)
  - Université Toulouse Capitole's (Malware)

Measurement Approach

Goal: Test real DNS queries against three freely available threat based blocklists – OTX phishing, HaGeZI TIF, and Prigent Malware and identify which domains would have been blocked

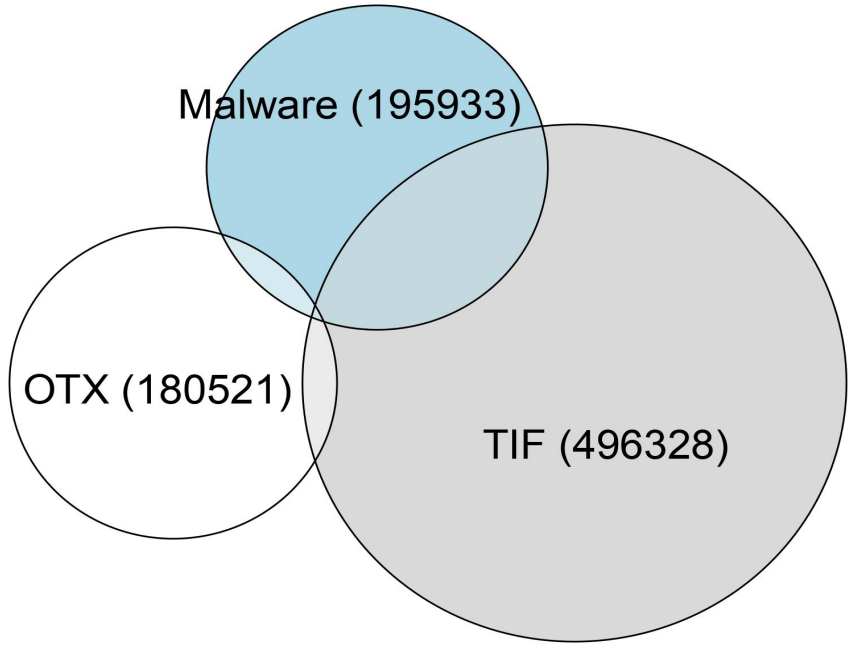


Figure 1: Domain names in the blocklists, June 2025.

- Subset of REN users' DNS queries and responses from June 19-25 2025
- Utilizing the custom DNS activity tool 'treetop' for domain information

Passive Measurements Results

- ~890M Queries
- 1.79M unique query names

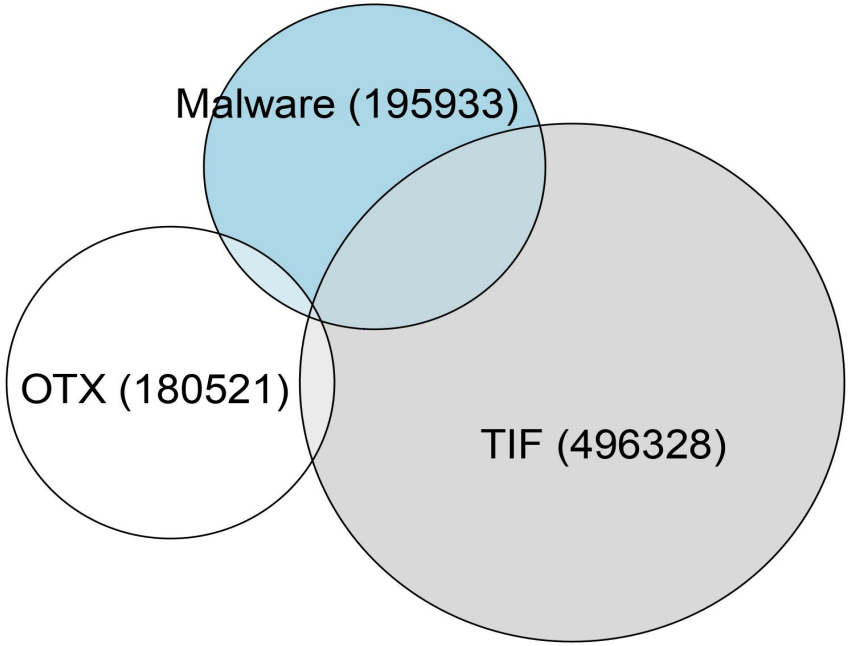


Figure 1: Domain names in the blocklists, June 2025.

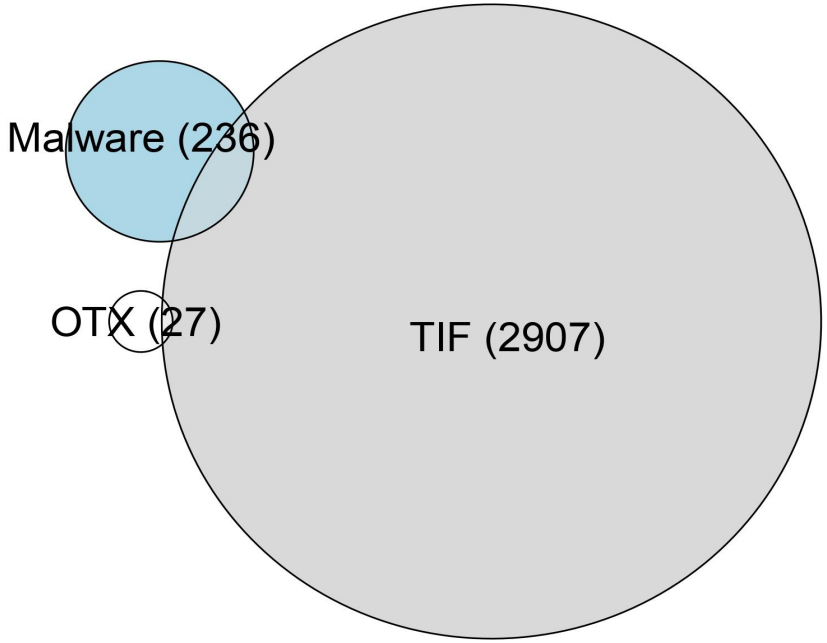


Figure 2: Query names matching blocklists, June 2025.

Observations

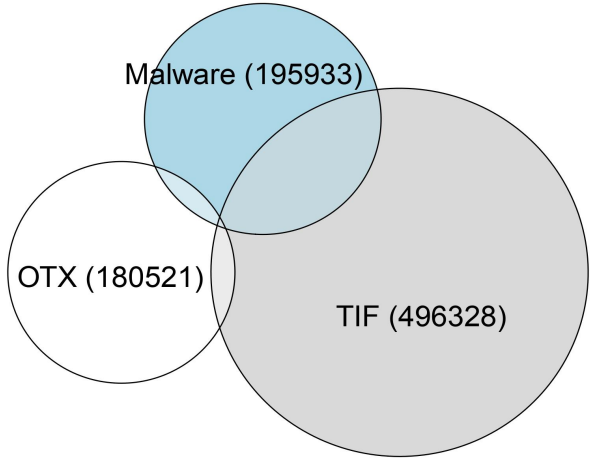


Figure 1: Domain names in the blocklists, June 2025.

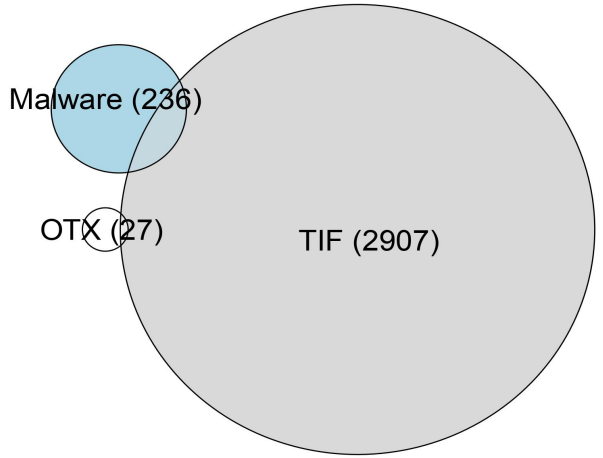


Figure 2: Query names matching blocklists, June 2025.

1. Blocklists are neither alike in content nor performance.
2. There is limited visibility into why a domain would be blocked.
3. Lack of a common taxonomy regarding the goals of blocking.
4. AI-driven blocking may increase inconsistencies and erode transparency.

Discussion & Feedback

Policy Purpose & Scope

- What should the primary goal of a PDNS policy be in a REN - security, privacy, or both?

- How can a PDNS policy balance the need to block harmful domains with the need to preserve open access to research and information?

Future Policy Development

- Should RENs collaborate to develop or vet PDNS standards and systems that align with REN members' goals?

- Can we minimize risks involved with employing a PDNS solution?