Maynard Koch TU Dresden, Germany
Marcin Nawrocki NETSCOUT, Berkeley, CA, USA
Thomas C. Schmidt HAW Hamburg, Germany
Matthias Wählisch TU Dresden, Germany

Transparent DNS Forwarders

A (still) unnoticed component of the open DNS infrastructure

DINR'24 Virtual Workshop, 2024-04-04

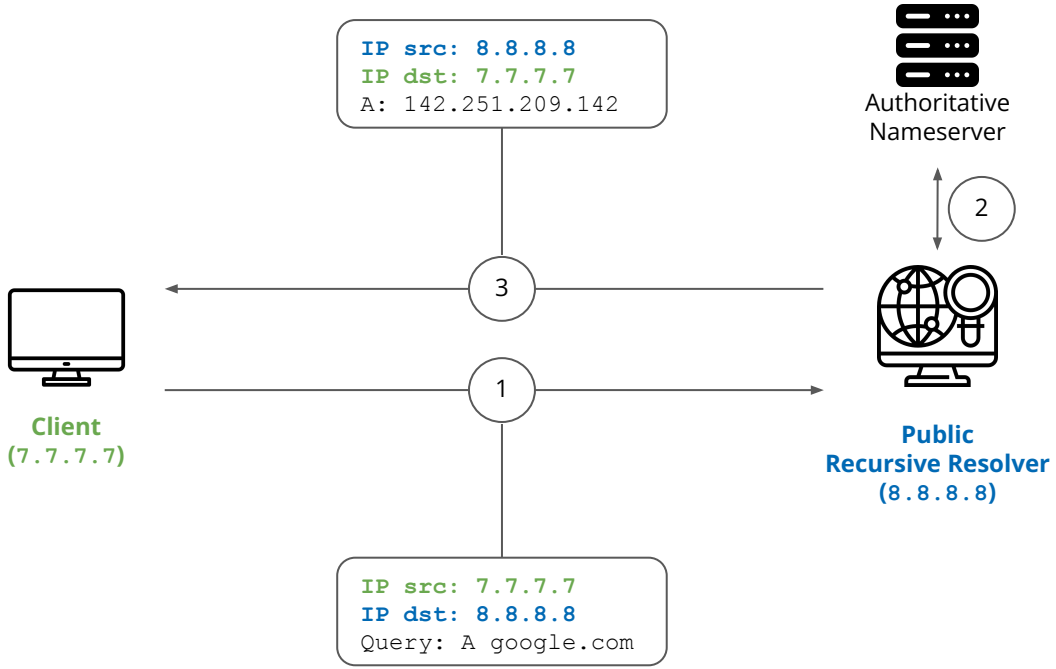
Contact: maynard.koch@tu-dresden.de

Why should we care? Open DNS enables amplification attacks!

Leading to unwanted traffic and unexpected traffic shifts

Open and Public DNS Infrastructure
Components

- Recursive Resolver
- Recursive Forwarder
- Transparent Forwarder

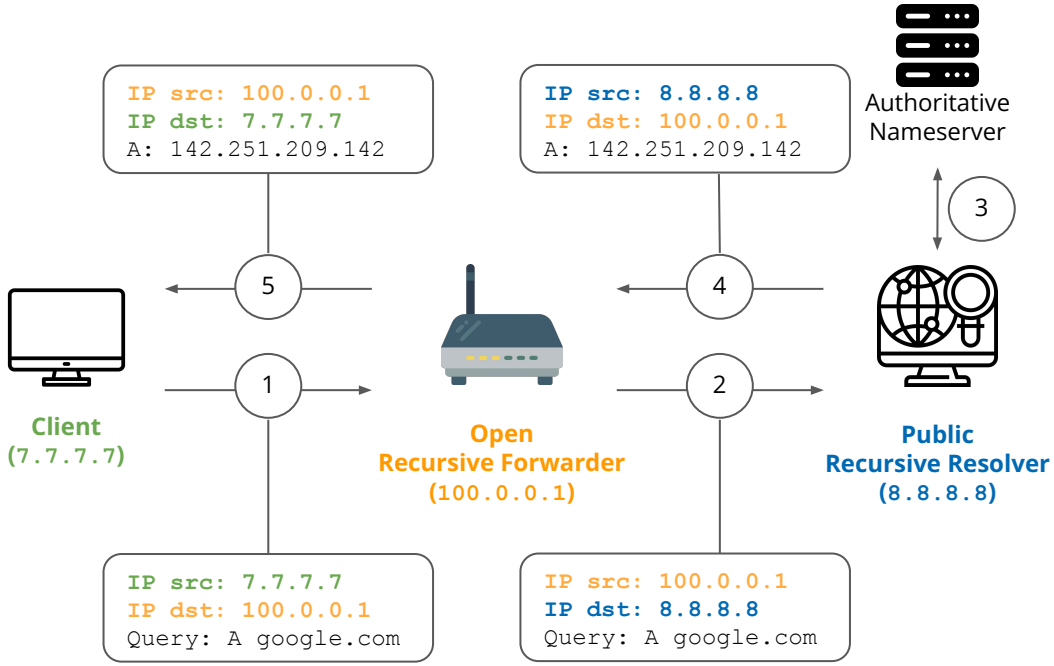


Open and Public DNS Infrastructure
Components

Recursive Resolver

Recursive Forwarder

Transparent Forwarder

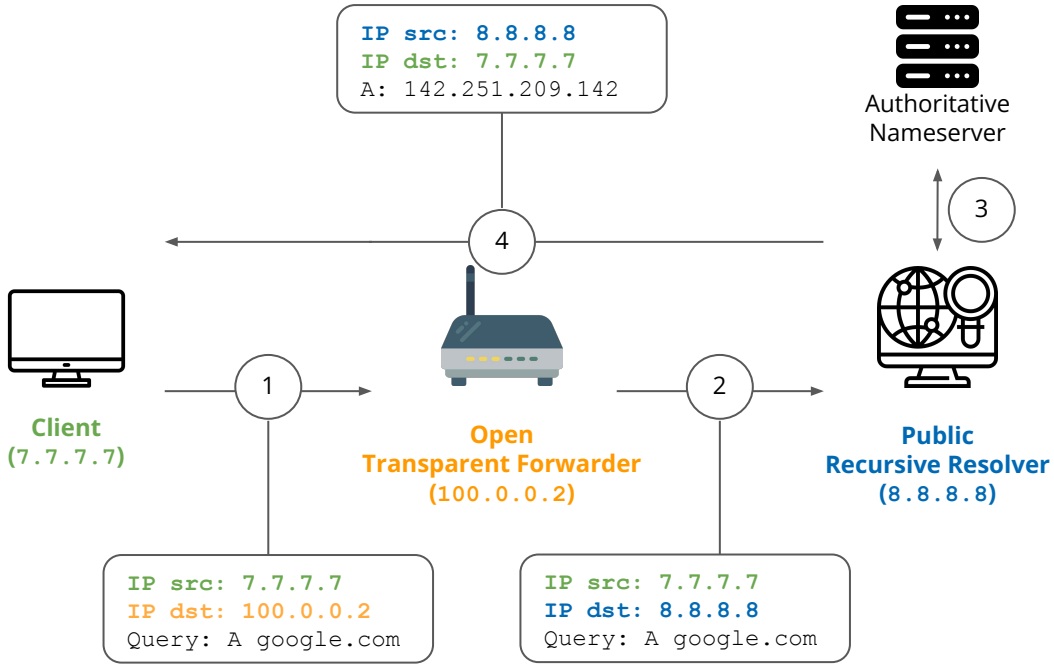


Open and Public DNS Infrastructure
Components

Recursive Resolver

Recursive Forwarder

Transparent Forwarder



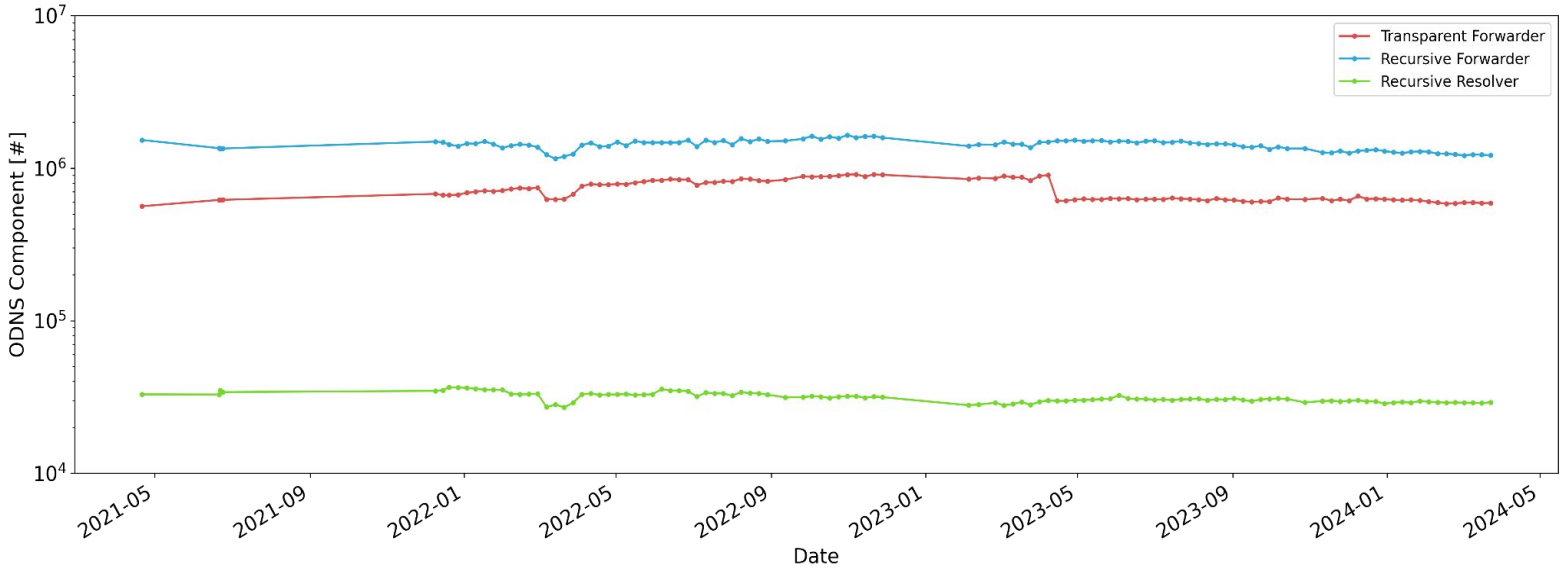
Controlled Experiments
Transparent forwarders fall off the radar

Details, see paper.

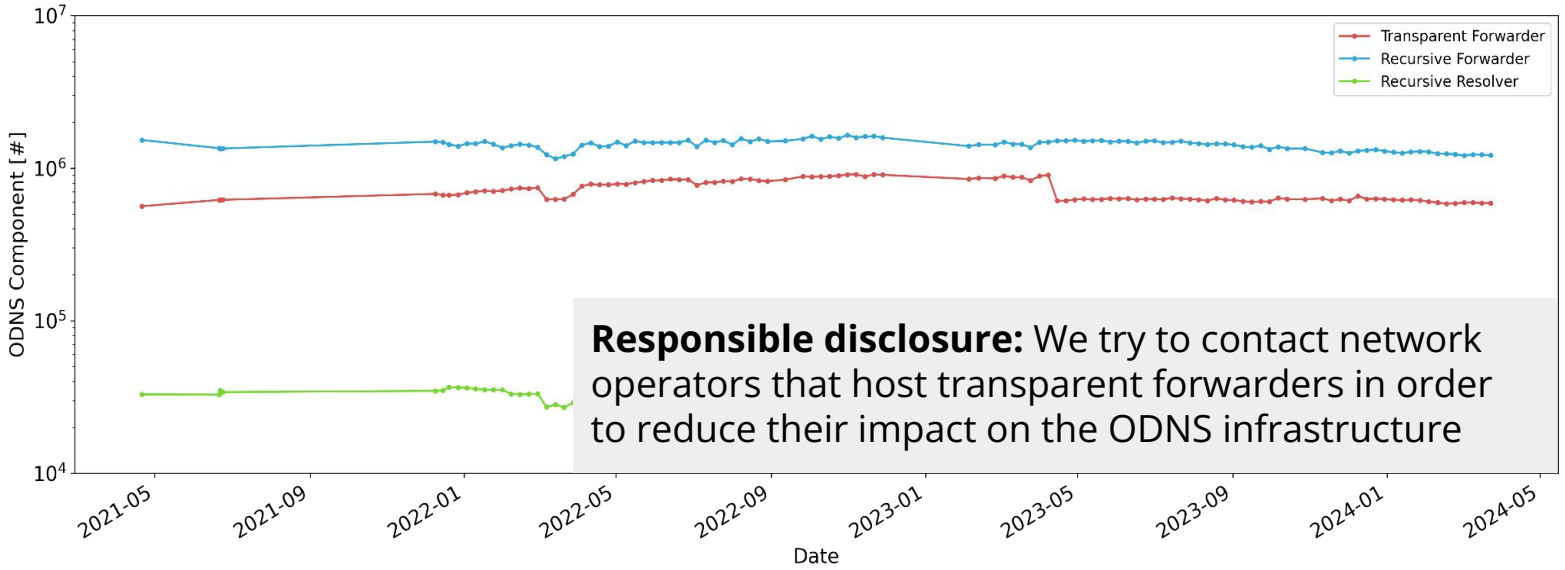
	Censys	Shadowserver	Shodan	Our Scans
# ODNS	1.6M	1.9M	1.1M	1.84M
Transparent forwarders detected	✗	✗	✗	✓ (31% forwarders)

M. Nawrocki, M. Koch, T. C. Schmidt, M. Wählisch, ACM CoNEXT, 2021,
https://doi.org/10.1145/3485983.3494872

Our Contribution
Monitoring and analyzing ODNS infrastructure

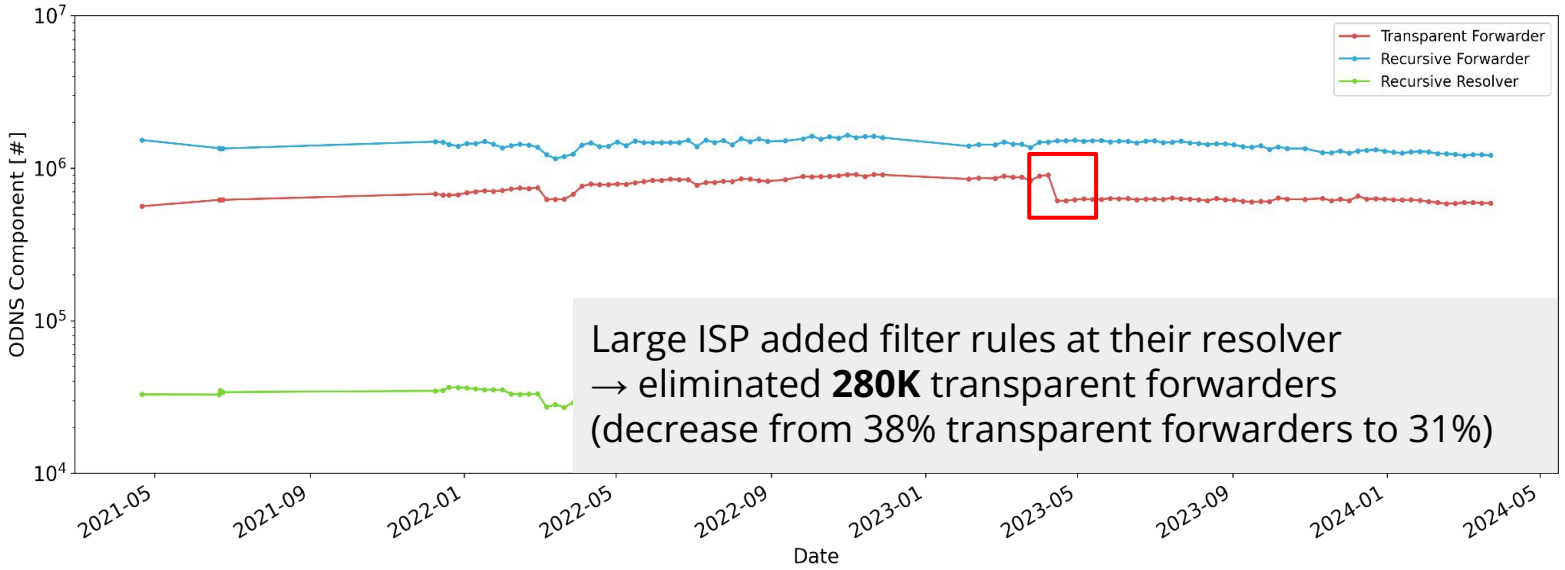


Our Contribution
Monitoring and analyzing ODNS infrastructure

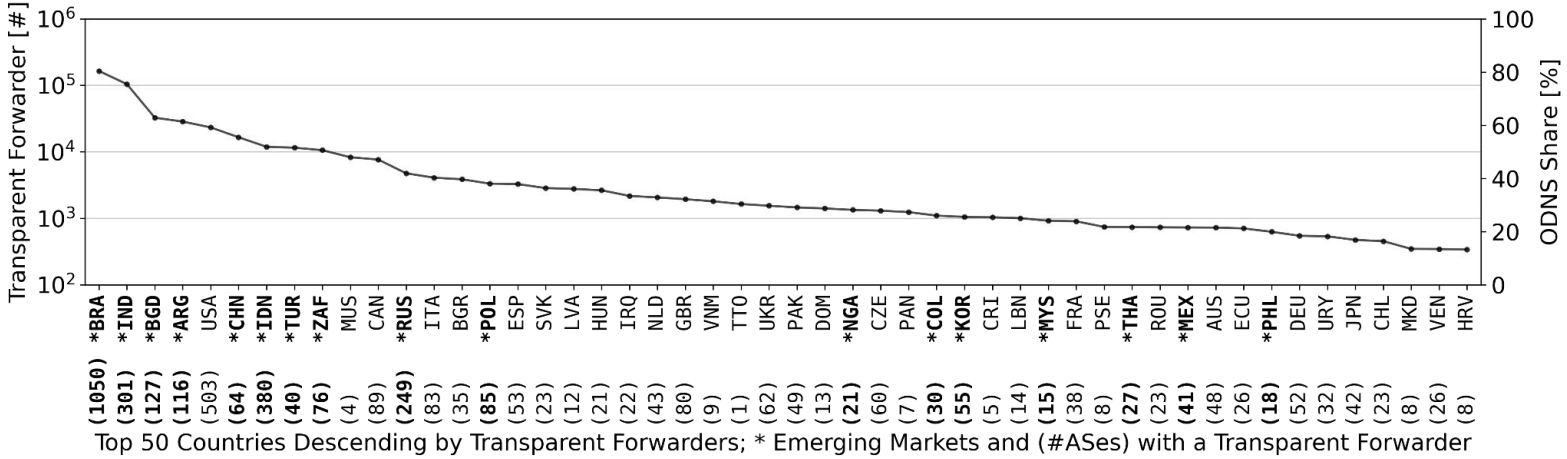


Responsible disclosure: We try to contact network operators that host transparent forwarders in order to reduce their impact on the ODNS infrastructure

Our Contribution
Monitoring and analyzing ODNS infrastructure

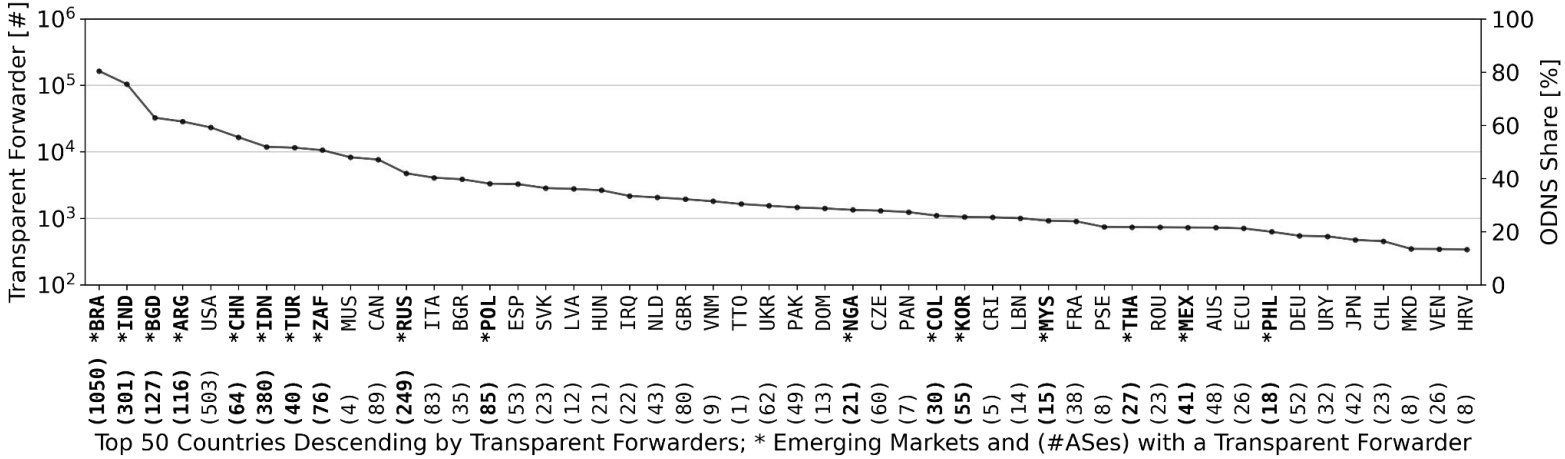


Where is transparent forwarder deployment most popular?
Current results



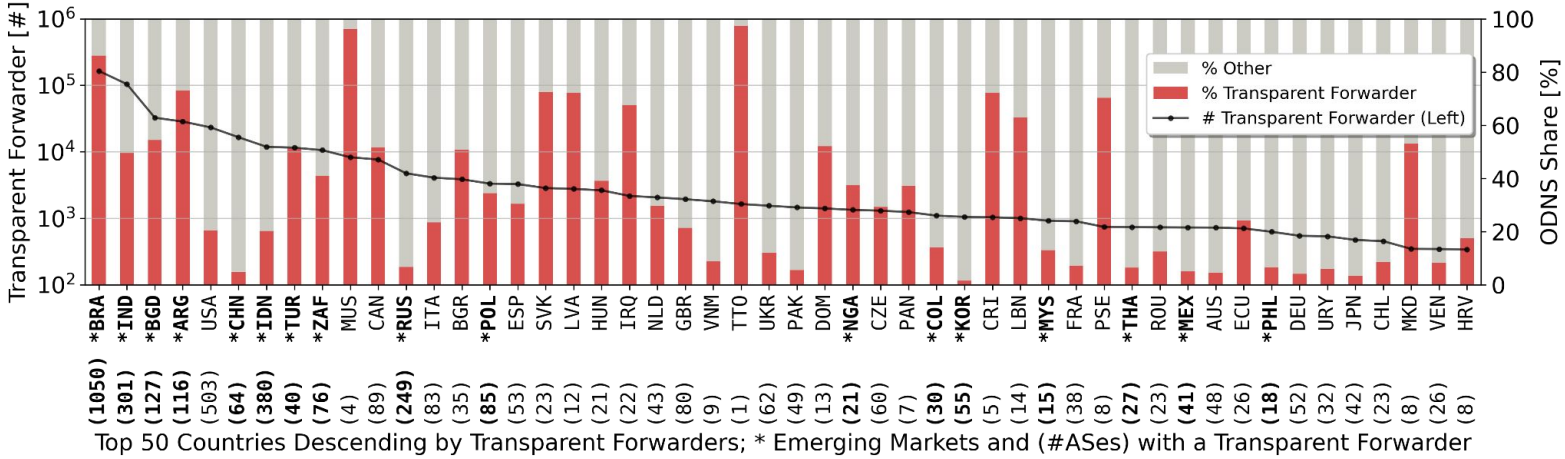
1. Countries classified as emerging markets are more likely to host transparent forwarders

Where is transparent forwarder deployment most popular?
Current results



1. Countries classified as emerging markets are more likely to host transparent forwarders
2. In each country, multiple ASes host forwarders.

Where is transparent forwarder deployment most popular?
Current results



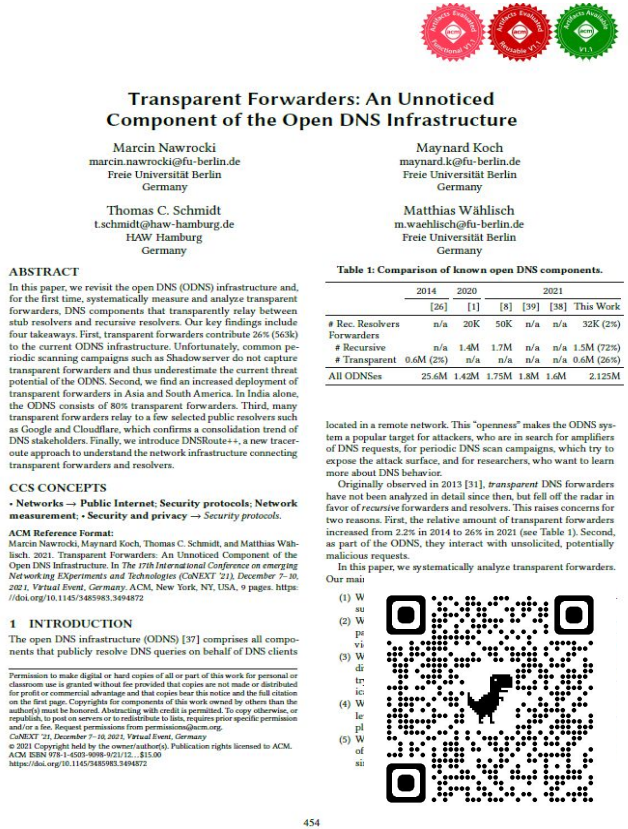
1. Countries classified as emerging markets are more likely to host transparent forwarders
2. In each country, multiple ASes host forwarders.
3. In some countries, the ODNS consists almost exclusively of transparent forwarders.

Outlook
Measuring transparent forwarders over…

	DoUDP	DoTCP	DoTLS	DoHTTPS	DoQUIC
# Transparent Forwarders	590K	2.4K			
Supported					

Outlook
Measuring transparent forwarders over…

	DoUDP	DoTCP	DoTLS	DoHTTPS	DoQUIC
# Transparent Forwarders	590K	2.4K	soon		
Supported	✓	✓	✓	✓	✓



Transparent Forwarders: An Unnoticed Component of the Open DNS Infrastructure

Marcin Nawrocki
marcin.nawrocki@fu-berlin.de
Freie Universität Berlin
Germany

Maynard Koch
maynard.k@fu-berlin.de
Freie Universität Berlin
Germany

Thomas C. Schmidt
t.schmidt@haw-hamburg.de
HAW Hamburg
Germany

Matthias Wählisch
m.waehlisch@fu-berlin.de
Freie Universität Berlin
Germany

ABSTRACT

In this paper, we revisit the open DNS (ODNS) infrastructure and, for the first time, systematically measure and analyze transparent forwarders, DNS components that transparently relay between stub resolvers and recursive resolvers. Our key findings include four takeaways. First, transparent forwarders contribute 26% (563k) to the current ODNS infrastructure. Unfortunately, common periodic scanning campaigns such as Shadowserver do not capture transparent forwarders and thus underestimate the current threat potential of the ODNS. Second, we find an increased deployment of transparent forwarders in Asia and South America. In India alone, the ODNS consists of 80% transparent forwarders. Third, many transparent forwarders relay to a few selected public resolvers such as Google and Cloudflare, which confirms a consolidation trend of DNS stakeholders. Finally, we introduce DNSRoute++, a new tracer-oute approach to understand the network infrastructure connecting transparent forwarders and resolvers.

CCS CONCEPTS

• **Networks** → **Public Internet**; **Security protocols**; **Network measurement**; • **Security and privacy** → *Security protocols*.

ACM Reference Format:
Marcin Nawrocki, Maynard Koch, Thomas C. Schmidt, and Matthias Wählisch. 2021. Transparent Forwarders: An Unnoticed Component of the Open DNS Infrastructure. In *The 17th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '21), December 7–10, 2021, Virtual Event, Germany.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3485983.3494872

1 INTRODUCTION

The open DNS infrastructure (ODNS) [37] comprises all components that publicly resolve DNS queries on behalf of DNS clients

ACM ISBN 978-1-4503-9098-9/21/12…$15.00
https://doi.org/10.1145/3485983.3494872

Table 1: Comparison of known open DNS components.

	2014	2020	2021			
	[26]	[1]	[8]	[39]	[38]	This Work
# Rec. Resolvers	n/a	20K	50K	n/a	n/a	32K (2%)
Forwarders						
# Recursive	n/a	1.4M	1.7M	n/a	n/a	1.5M (72%)
# Transparent	0.6M (2%)	n/a	n/a	n/a	n/a	0.6M (26%)
All ODNSes	25.6M	1.42M	1.75M	1.8M	1.6M	2.125M

located in a remote network. This "openness" makes the ODNS system a popular target for attackers, who are in search for amplifiers of DNS requests, for periodic DNS scan campaigns, which try to expose the attack surface, and for researchers, who want to learn more about DNS behavior.

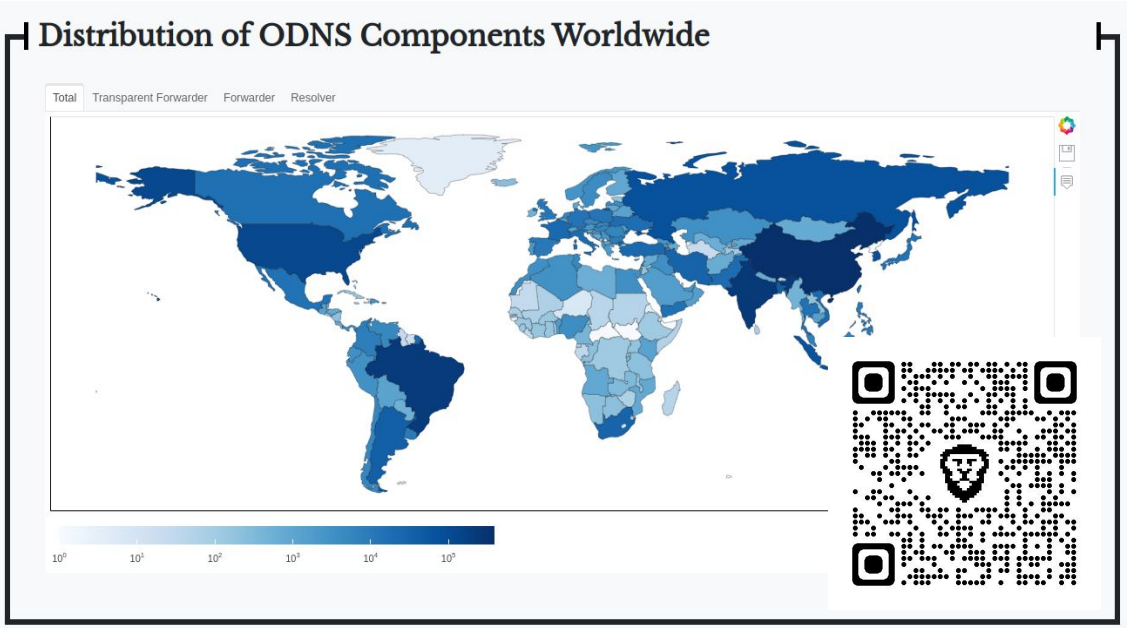
Originally observed in 2013 [31], *transparent* DNS forwarders have not been analyzed in detail since then, but fell off the radar in favor of *recursive* forwarders and resolvers. This raises concerns for two reasons. First, the relative amount of transparent forwarders increased from 2.2% in 2014 to 26% in 2021 (see Table 1). Second, as part of the ODNS, they interact with unsolicited, potentially malicious requests.

In this paper, we systematically analyze transparent forwarders. Our mai

(1) W
(2) W
(3) W
(4) W
(5) W

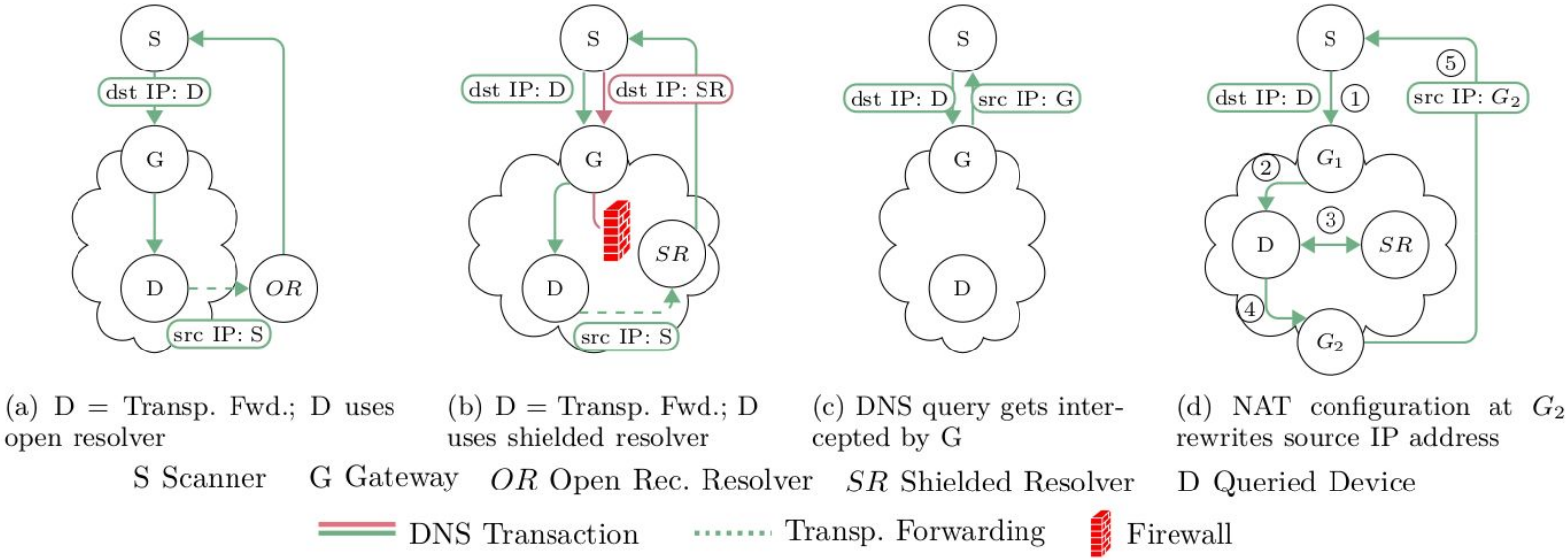
https://doi.org/10.1145/3485983.3494872

Weekly scan results and Open DNS classification: odns.secnow.net



Backup Slides

Transparent DNS Forwarders
Deployment scenarios



(a) D = Transp. Fwd.; D uses open resolver

(b) D = Transp. Fwd.; D uses shielded resolver

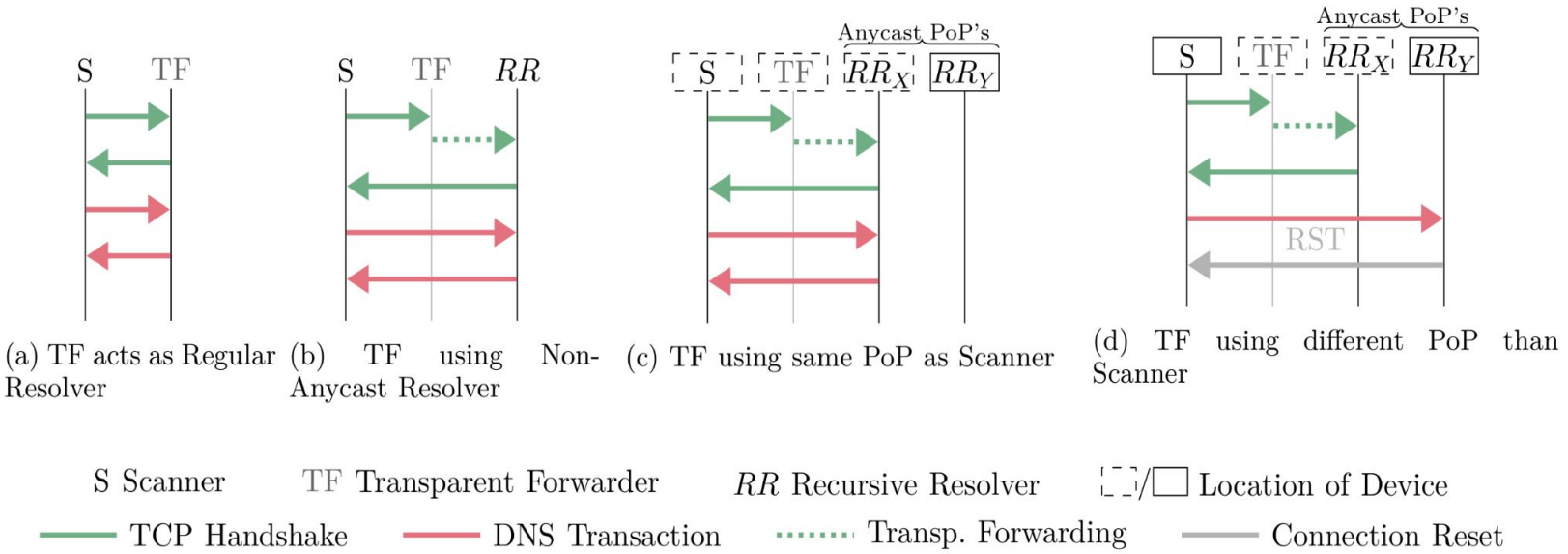
(c) DNS query gets intercepted by G

(d) NAT configuration at G_2 rewrites source IP address

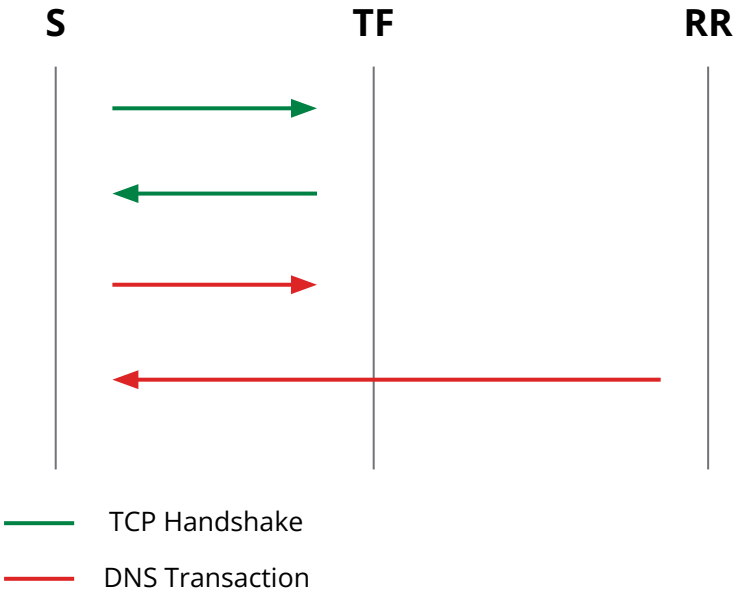
S Scanner G Gateway *OR* Open Rec. Resolver *SR* Shielded Resolver D Queried Device

DNS Transaction Transp. Forwarding Firewall

Transparent DNS Forwarders
Behavior over TCP

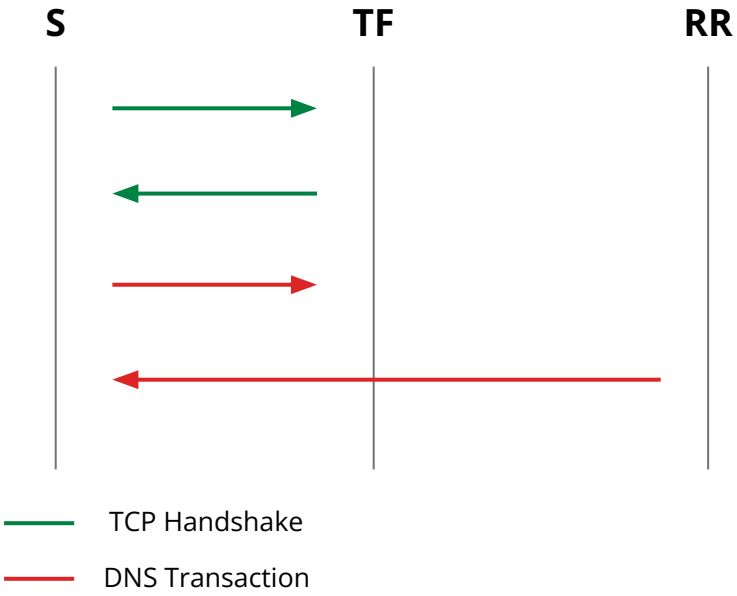


Transparent DNS Forwarders
Behavior over TCP



We receive a **SYN/ACK** from **TF** but the **DNS response** is sent by **RR.**

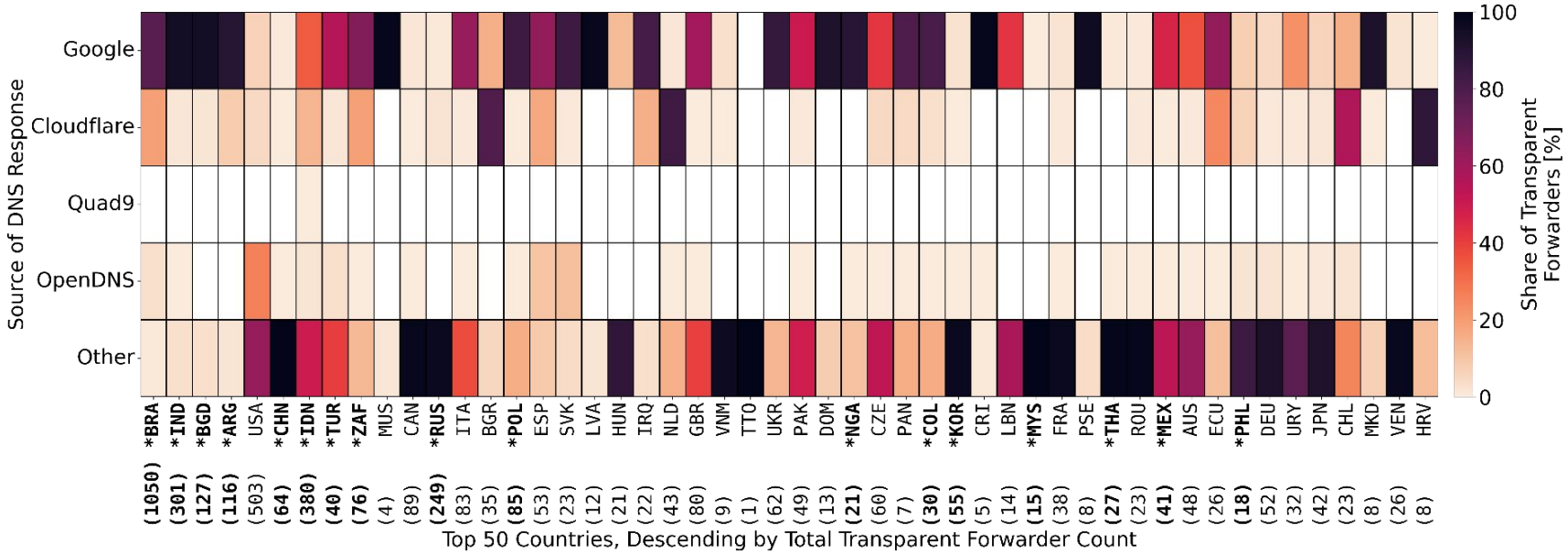
Transparent DNS Forwarders
Behavior over TCP



We receive a **SYN/ACK** from **TF** but the **DNS response** is sent by **RR.**

We are analyzing this case. Current results reveal that **RR is the router for TF**.

Transparent DNS Forwarders
Public resolver project share



You are (unintentionally) hosting transparent forwarders?

1. Open transparent forwarders facilitate **DNS amplification attacks**
   Even worse compared to recursive resolvers
2. Open transparent forwarders allow attackers to **exploit anycast deployments**
   Challenges PoP-based DDoS mitigation
3. Your AS forwards packets that look like **spoofed IP packets**
   Attribution is challenging because these packets are triggered outside your AS

Solutions:
(1) Update filter rules, or
(2) Update transparent forwarders.