

Maynard Koch <maynard.koch@tu-dresden.de>
Florian Dolzmann <florian.dolzmann@mailbox.tu-dresden.de>
Marcin Nawrocki <marcin.nawrocki@netscout.com>
Matthias Wählisch <m.waehlich@tu-dresden.de>
Thomas C. Schmidt <t.schmidt@haw-hamburg.de>

Transparent DNS Forwarders

A (still) unnoticed component of the ODNS infrastructure

OARC 43, Prague // October 27, 2024

Why should we care? Open DNS enables amplification attacks!

Leading to unwanted traffic and unexpected traffic shifts.



https://www.flaticon.com/free-icon/loupe_622669 | https://www.flaticon.com/premium-icon/dns_1183595
https://www.flaticon.com/free-icon/devil_725040 | https://www.flaticon.com/premium-icon/sad_3129281

Monitoring the Open DNS Infrastructure

Identify open resolvers to mitigate DDoS. Popular scanning campaigns.

The screenshot displays the SHODAN search interface with the following elements:

- Navigation:** SHODAN logo, Explore, Downloads, Pricing, port:53 Recursion: enabled, Account.
- Search Results:** 2,666 results for the query: `services.port: 53 AND services.service_name: 'dns'`.
- SHADOWSERVER Section:**
 - Logo and "UK Government" affiliation.
 - Navigation: Dashboard, General statistics, IoT device statistics, Attack statistics: Vulnerabilities, Attack statistics: Devices, Help.
 - Language notice: "The Shadowserver dashboard is available in [Deutsch](#) and 74 other languages. See the language menu in our footer for a full list."
 - Trending queries: `Progress MOVEit Transfer CVE-2024-5806 POST /guestaccess.aspx exploit attempts` (More details).
- Analytics Charts:**
 - Unique IP addresses per country:** World map showing high concentrations in India (3,435,996) and the United States (99,326).
 - Unique IP addresses per tag:** Donut chart for "avalanche andromeda" (683,326) with sub-categories like "indonesia", "usa", "china", "south america", "europe", "north america", "oceania", "africa", "asia".
 - Unique IP addresses over time:** Line chart from 2024-06-22 to 2024-07-20, showing activity across Asia, Africa, Europe, North America, South America, and Oceania.
- Left Sidebar:** Sinkholes, Scans, Honey pots, DDoS, ICS/OT, Web CVEs.
- About this data:** Sinkholing is a technique whereby a resource used by malicious actors to control malware is taken over and redirected to a benign listener that can (to a varying degree) understand network connections coming from infected devices. This provides visibility of the distribution of infected devices worldwide, as well as protecting victims by preventing botnet command and control (C2) from cybercriminals.

Monitoring the Open DNS Infrastructure

Our campaign, <https://odns.secnow.net>

SECNOW

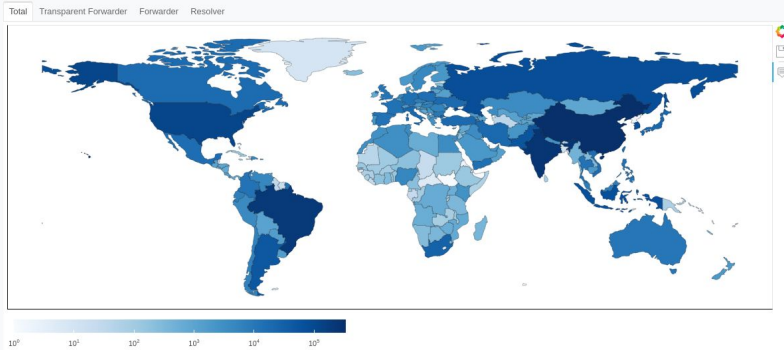
Open DNS (ODNS)

[Home](#) [DoUDP Measurements](#) [DoTCP Measurements](#) [CoNEXT'21 Artifacts](#) [Paper](#) [Contact](#)

DNS over UDP Scanning

Last successful measurement: 2024-07-19

Distribution of ODNS Components Worldwide



Why yet another scanning campaign?

Monitoring the Open DNS Infrastructure

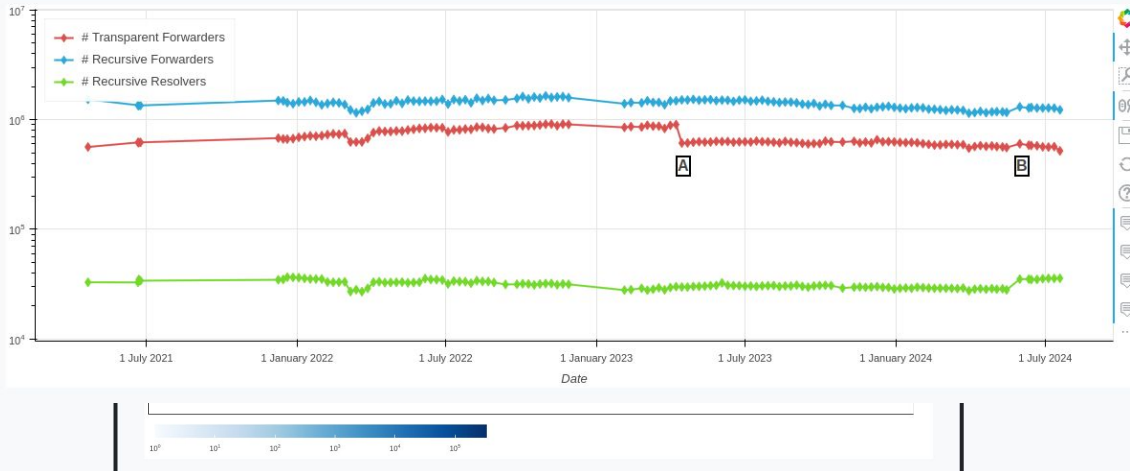
Our campaign, <https://odns.secnow.net>

SECNOW

Open DNS (ODNS)

Home DoUDP Measurements DoTCP Measurements CoNEXT'21 Artifacts Paper Contact

DNS over UDP Scanning



Why yet another scanning campaign?





We also monitor transparent DNS forwarders!

They account for ~30% of the ODNS infrastructure.

These devices are **missed completely** by other campaigns.

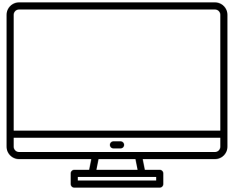
Our controlled experiment confirms that transparent DNS forwarders fell of the radar.

Details, see paper.

	Censys	Shadowserver	Shodan	Our Scans
# ODNS	1.75M	1.7M	1.6M	1.8M
Transparent forwarders detected				 (30% transp. fwd.)

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

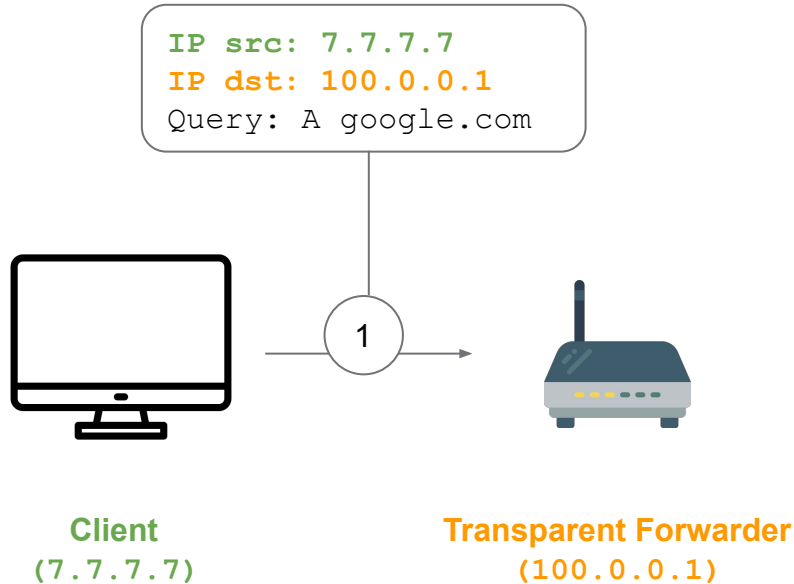
How do transparent forwarders work?



Client
(7.7.7.7)

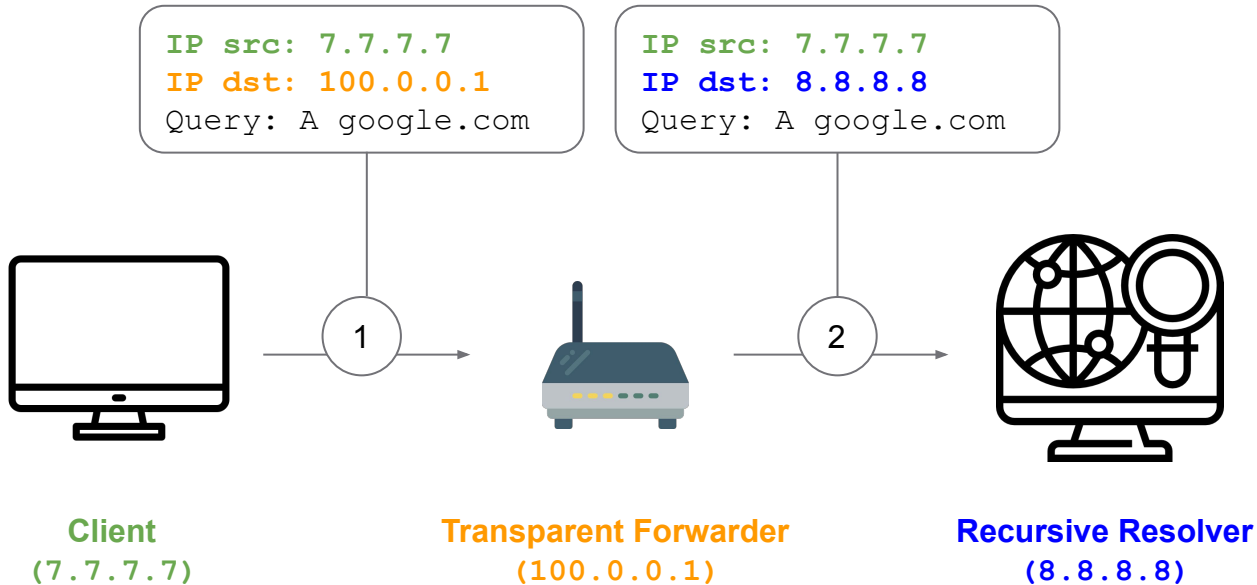
<https://www.flaticon.com/free-icons/computer> | <https://www.flaticon.com/free-icons/dns> | <https://www.flaticon.com/free-icons/router> | <https://www.flaticon.com/free-icons/server>

How do transparent forwarders work?



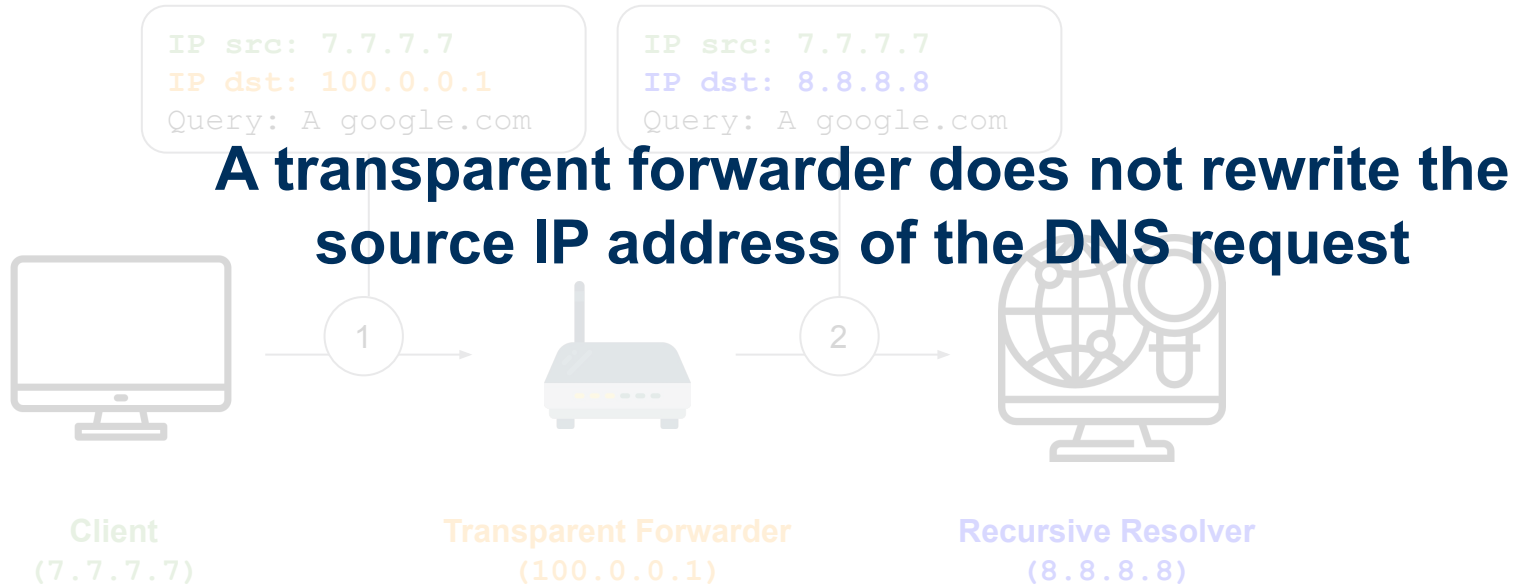
<https://www.flaticon.com/free-icons/computer> | <https://www.flaticon.com/free-icons/dns> | <https://www.flaticon.com/free-icons/router> | <https://www.flaticon.com/free-icons/server>

How do transparent forwarders work?



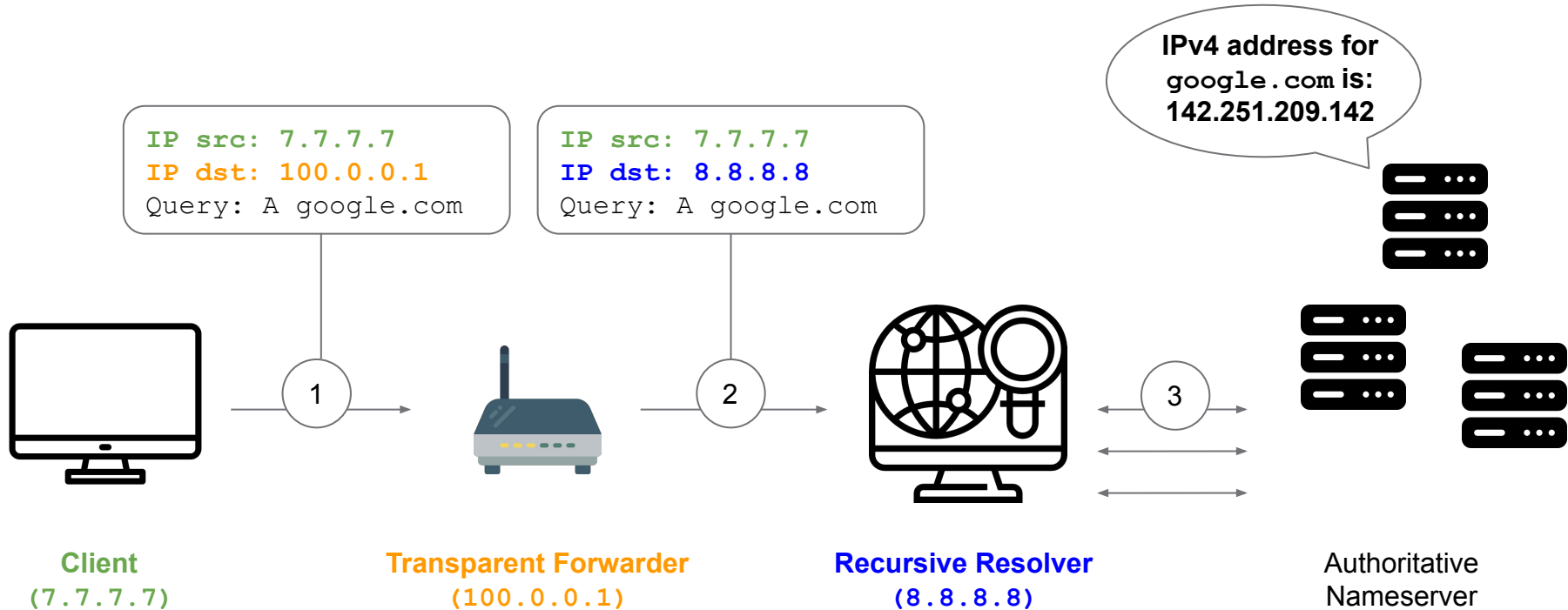
<https://www.flaticon.com/free-icons/computer> | <https://www.flaticon.com/free-icons/dns> | <https://www.flaticon.com/free-icons/router> | <https://www.flaticon.com/free-icons/server>

How do transparent forwarders work?



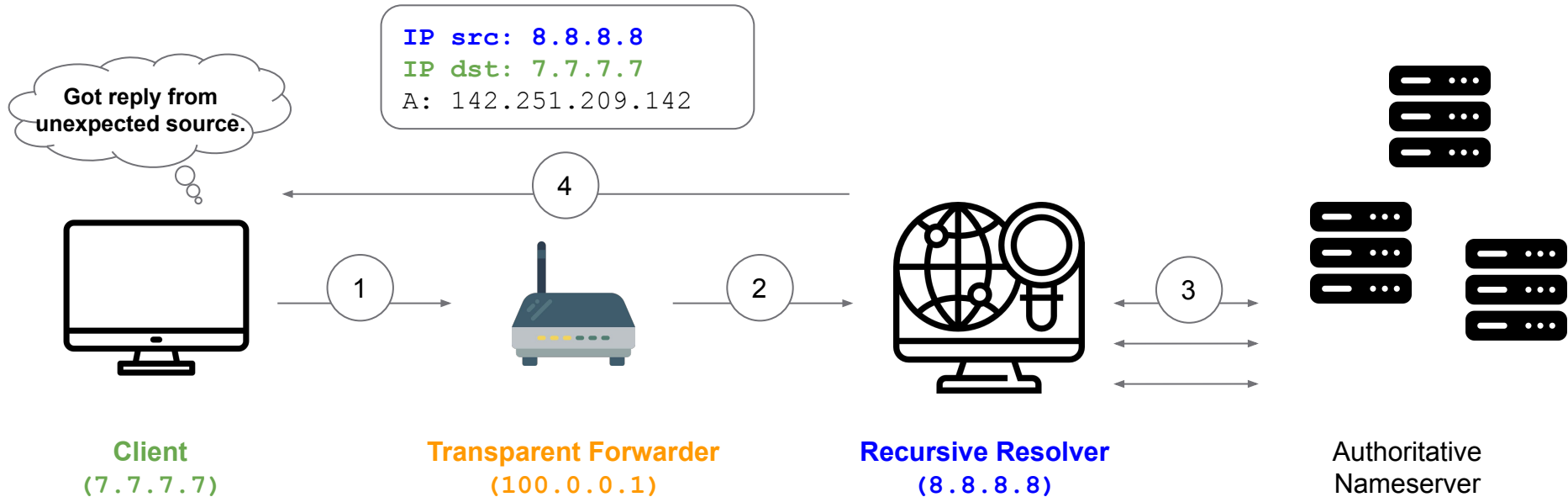
<https://www.flaticon.com/free-icons/computer> | <https://www.flaticon.com/free-icons/dns> | <https://www.flaticon.com/free-icons/router> | <https://www.flaticon.com/free-icons/server>

How do transparent forwarders work?



<https://www.flaticon.com/free-icons/computer> | <https://www.flaticon.com/free-icons/dns> | <https://www.flaticon.com/free-icons/router> | <https://www.flaticon.com/free-icons/server>

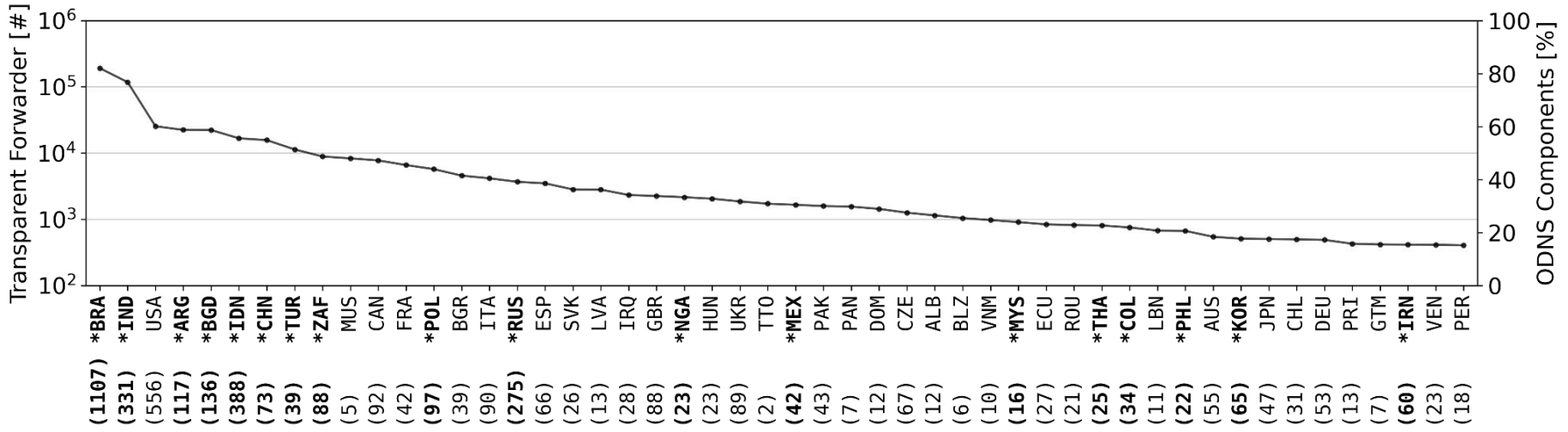
How do transparent forwarders work?



<https://www.flaticon.com/free-icons/computer> | <https://www.flaticon.com/free-icons/dns> | <https://www.flaticon.com/free-icons/router> | <https://www.flaticon.com/free-icons/server>

Where is transparent forwarder deployment most popular?

An overview of current results

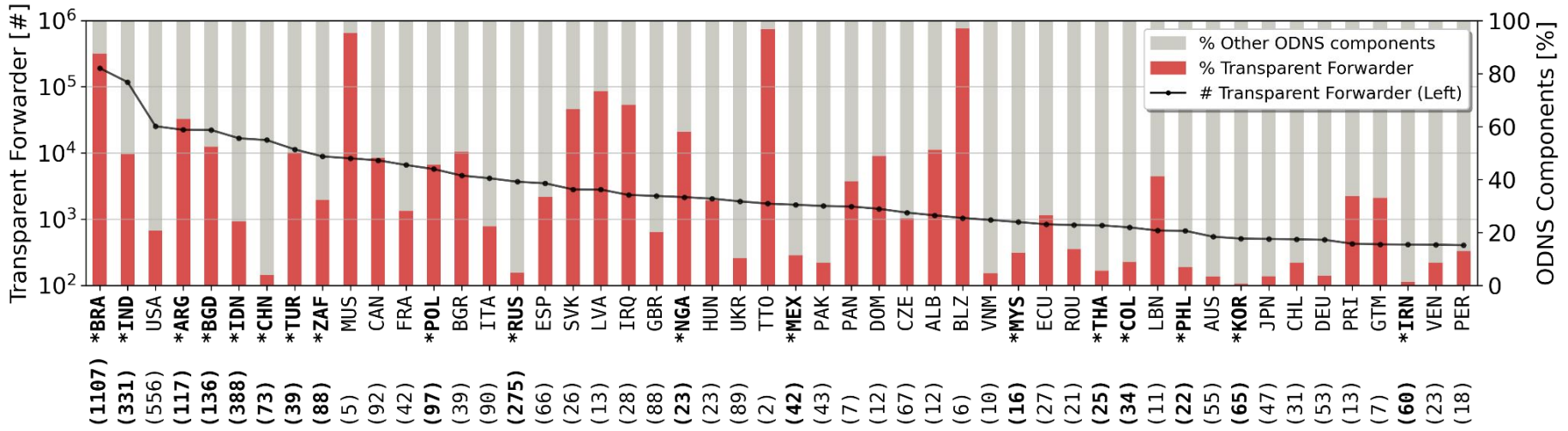


Top 50 Countries Descending by Transparent Forwarders; * Emerging Markets and (#ASes) with a Transparent Forwarder

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?

An overview of current results

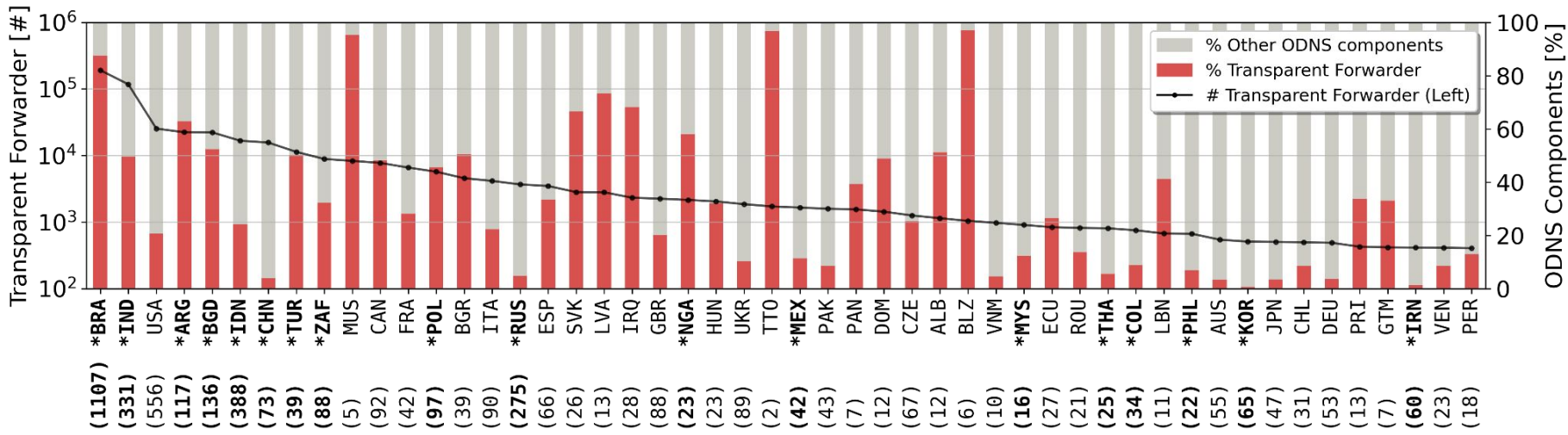


Top 50 Countries Descending by Transparent Forwarders; * Emerging Markets and (#ASes) with a Transparent Forwarder

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?

An overview of current results



Top 50 Countries Descending by Transparent Forwarders; * Emerging Markets and (#ASes) with a Transparent Forwarder

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.

Why do common scan campaigns miss transparent forwarders?

Due to efficiency reasons, scans use static queries and **only evaluate incoming traffic.**

This means that many scanning campaigns just consider the replying source address.

Why do common scan campaigns miss transparent forwarders?

Due to efficiency reasons, scans use static queries and **only evaluate incoming traffic.**

This means that many scanning campaigns just consider the replying source address.

“The consensus that we came to was that since these systems couldn’t do amplification on their own and merely forwarded packets, they were out of scope.” - Reply to our request why [scanning company] does not include transparent forwarders

Why do common scan campaigns miss transparent forwarders?

This is short sighted and here is a simple example why...

Due to efficiency reasons scans use static queries and only evaluate incoming traffic

This means that many scanning campaigns just consider the replying source address.

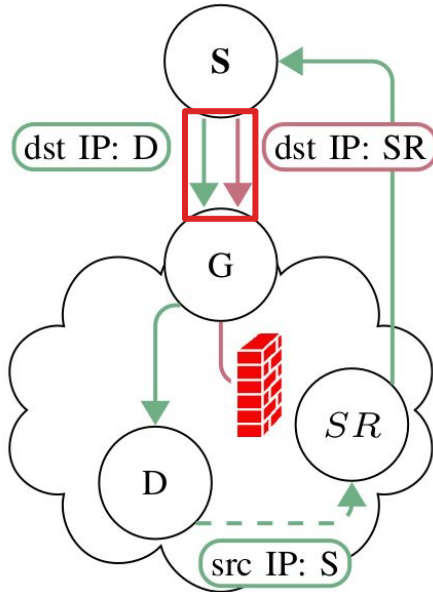
“The consensus that we came to was that since these systems couldn’t do amplification on their own and merely forwarded packets, they were out of scope.” - Reply to our request why [scanning company] does not include transparent forwarders



[http://bilder.hifi-forum.de/medium/610438/homer-simpson-doh_204826.gif]

Why should transparent forwarders be included in ODNS scans?

Transparent forwarders allow the use of restricted resolvers



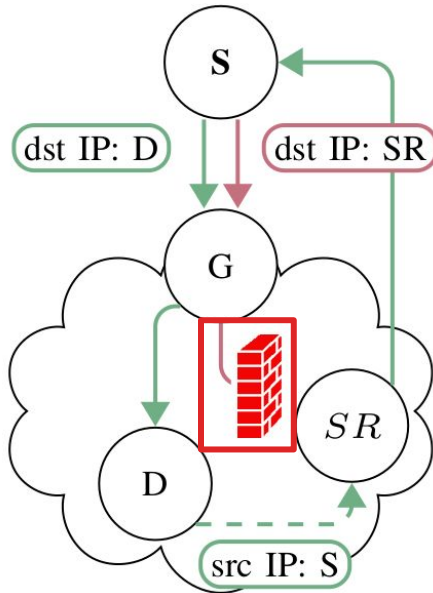
- Transparent forwarders **unveil access to restricted/shielded resolvers**

S Scanner **G** Gateway
D Queried Device **SR** Shielded Resolver

 DNS Transaction  Transp. Forwarding  Firewall

Why should transparent forwarders be included in ODNS scans?

Transparent forwarders allow the use of restricted resolvers



- Transparent forwarders **unveil access to restricted/shielded resolvers**

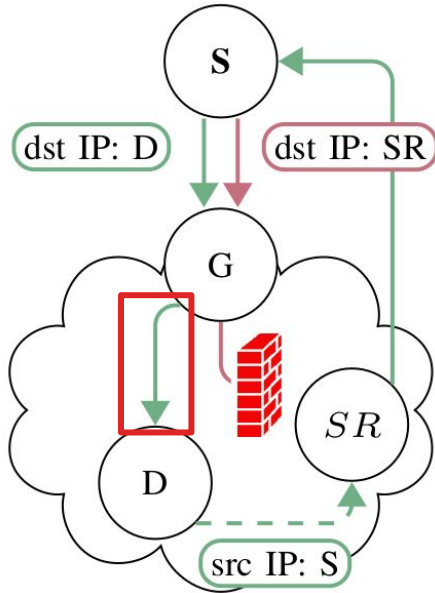
Firewall configuration at AS borders prohibit requests to their local resolvers

S Scanner **G** Gateway
D Queried Device **SR** Shielded Resolver

— DNS Transaction Transp. Forwarding Firewall

Why should transparent forwarders be included in ODNS scans?

Transparent forwarders allow the use of restricted resolvers



- Transparent forwarders **unveil access to restricted/shielded resolvers**

Firewall configuration at AS borders prohibit requests to their local resolvers

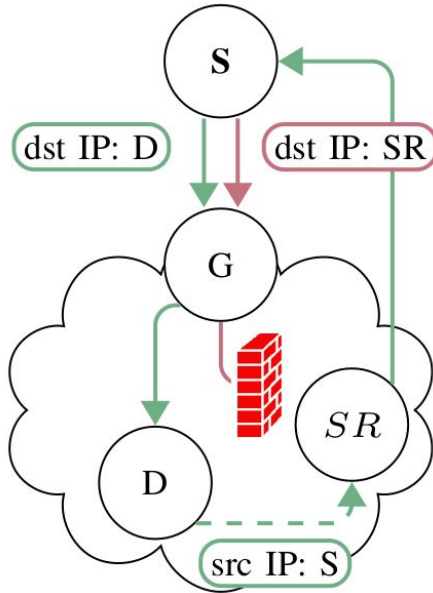
Querying a transparent forwarder circumvents the firewall!

S Scanner **G** Gateway
D Queried Device **SR** Shielded Resolver

— DNS Transaction Transp. Forwarding Firewall

Why should transparent forwarders be included in ODNS scans?

Transparent forwarders allow the use of restricted resolvers



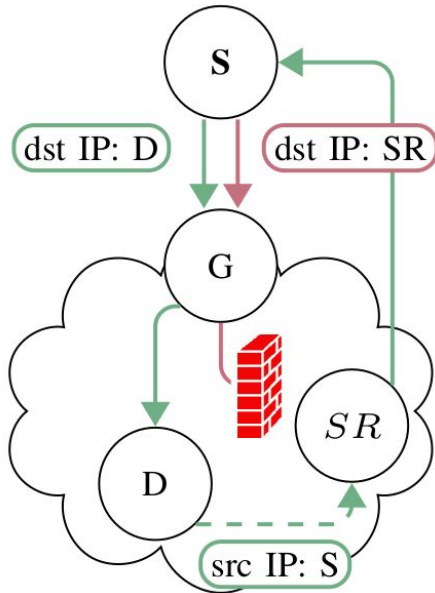
- Transparent forwarders **unveil access to restricted/shielded resolvers**
- Over **60%** of the resolvers used by transparent forwarders are **not publicly accessible**

S Scanner **G** Gateway
D Queried Device **SR** Shielded Resolver

 DNS Transaction  Transp. Forwarding  Firewall

Why should transparent forwarders be included in ODNS scans?

Transparent forwarders allow the use of restricted resolvers



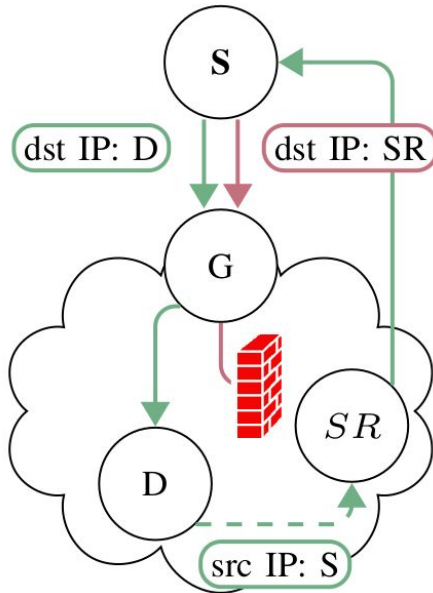
- Transparent forwarders **unveil access to restricted/shielded resolvers**
- Over **60%** of the resolvers used by transparent forwarders are **not publicly accessible**
- These resolvers are **distributed over hundreds of ASes** in multiple countries

S Scanner **G** Gateway
D Queried Device **SR** Shielded Resolver

— DNS Transaction Transp. Forwarding Firewall

Why should transparent forwarders be included in ODNS scans?

Transparent forwarders allow the use of restricted resolvers



S Scanner
D Queried Device
G Gateway
SR Shielded Resolver

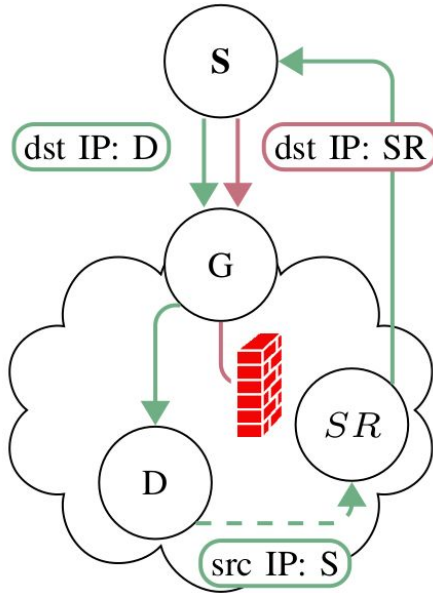
— DNS Transaction Transp. Forwarding

 Firewall

- Transparent forwarders **unveil access to restricted/shielded resolvers**
- Over **60%** of the resolvers used by transparent forwarders are **not publicly accessible**
- These resolvers are **distributed over hundreds of ASes** in multiple countries
- Some of these resolvers serve as **free reflectors/amplifiers** by replying with **millions of responses** to just a **handful of requests**

Why should transparent forwarders be included in ODNS scans?

Transparent forwarders allow the use of restricted resolvers



S Scanner
D Queried Device
G Gateway
SR Shielded Resolver

— DNS Transaction Transp. Forwarding Firewall

- Transparent forwarders unveil access to restricted/shielded resolvers

Transparent forwarders are, indeed, a threat and should be removed completely but at least monitored.

- These resolvers are distributed over hundreds of ASes in multiple countries

- Some of these resolvers serve as free reflectors/amplifiers by replying with millions of responses to just a handful of requests

In a nutshell

1. Open transparent forwarders facilitate **DNS amplification attacks**
Even worse compared to recursive resolver

In a nutshell

1. Open transparent forwarders facilitate **DNS amplification attacks**
Even worse compared to recursive resolver
2. Open transparent forwarders allow attackers to **exploit anycast deployments**
Challenges PoP-based DDoS mitigation

In a nutshell

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

In a nutshell

1. Open transparent forwarders facilitate **DNS amplification attacks**
Even worse compared to recursive resolver
2. Open transparent forwarders allow attackers to **exploit anycast deployments**
Challenges PoP-based DDoS mitigation
3. Affected ASes forward packets that look like **spoofed IP packets**
Attribution is challenging because these packets are triggered outside the ASes
4. Scanning for transparent forwarders is **not challenging**
No scalability issues. Extending setup requires minimal changes.

In a nutshell

1. Open transparent forwarders facilitate **DNS amplification attacks**
Even worse compared to recursive resolver
2. Open transparent forwarders allow attackers to **exploit anycast deployments**
Challenges PoP-based DDoS mitigation
3. Affected ASes forward packets that look like **spoofed IP packets**
Attribution is challenging because these packets are triggered outside the ASes
4. Scanning for transparent forwarders is **not challenging**
No scalability issues. Extending setup requires minimal changes.

Solutions:

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

In a nutshell

1. Open transparent forwarders facilitate **DNS amplification attacks**
Even worse compared to recursive resolver
2. Open transparent forwarders allow attackers to **exploit anycast deployments**
Challenges PoP-based DDoS mitigation
3. Affected ASes forward packets that look like **spoofed IP packets**
Attribution is challenging because these packets are triggered outside the ASes
4. Scanning for transparent forwarders is **not challenging**
No scalability issues. Extending setup requires minimal changes.

Solutions:

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

...and also include
transparent forwarders in
your scanning campaigns!



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 traceroute 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

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions.acm.org.
CoNEXT '21, December 7–10, 2021, Virtual Event, Germany
© 2021 Copyright held by the owner(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9098-0/21/12...\$15.00
<https://doi.org/10.1145/3485983.3494872>

Table 1: Comparison of known open DNS components.

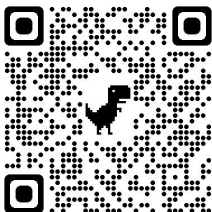
	2014	2020	2021		
	[26]	[1]	[8]	[39]	This Work
# Rec. Resolvers	n/a	20K	50K	n/a	n/a
Forwarders					32K (2%)
# Recursive		n/a	1.4M	1.7M	n/a
# Transparent	0.6M (2%)	n/a	n/a	n/a	1.5M (72%)
All ODNSes	25.6M	1.42M	1.75M	1.8M	1.6M
					2.125M

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 main contributions read as follows:

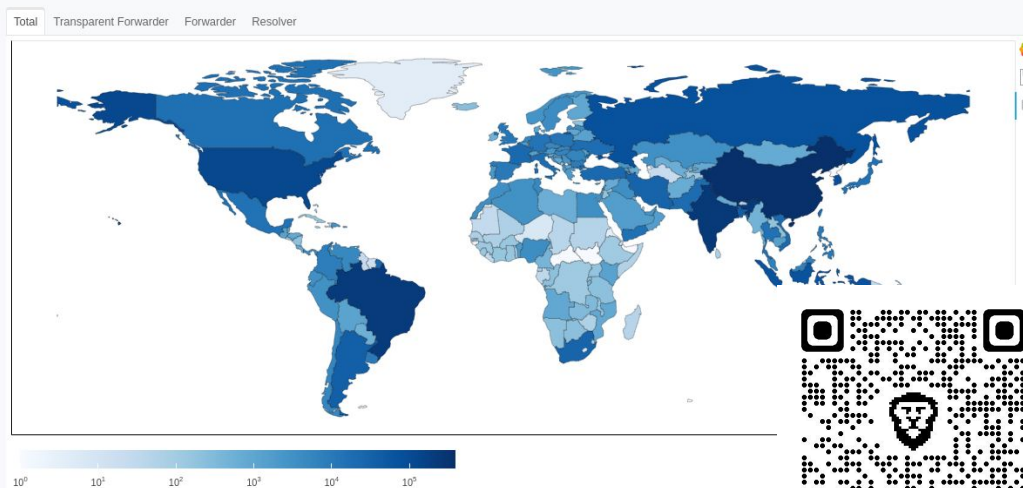
- (1) We ensure
- (2) We provide
- (3) We dive into
- (4) We leverage
- (5) We discuss



Weekly scan results and Open DNS classification:

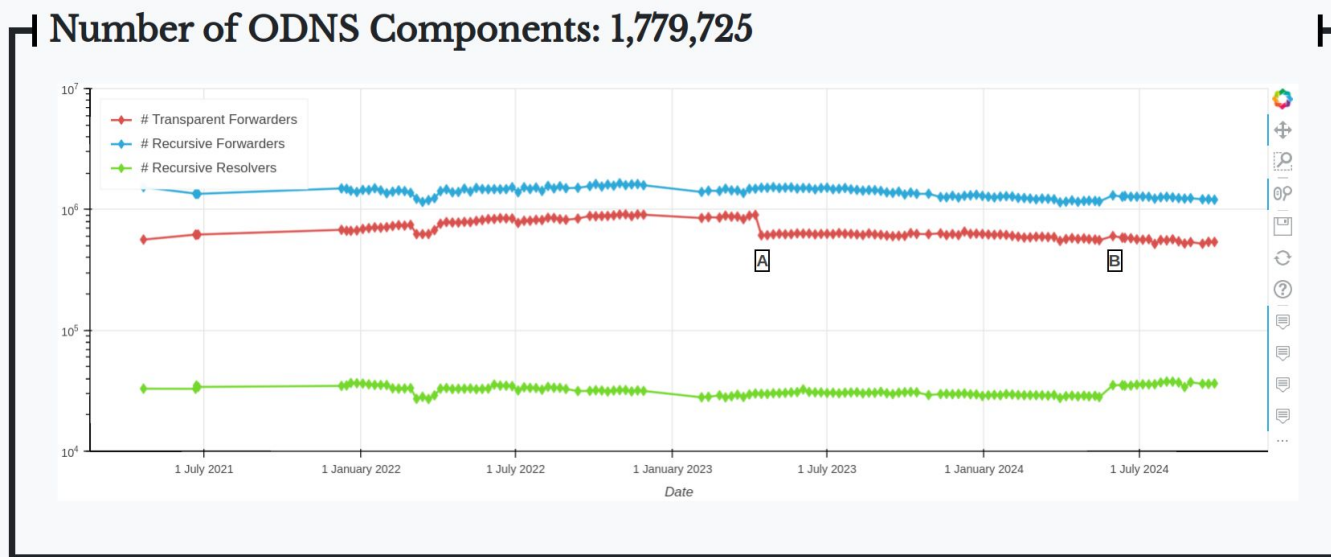
odns.secnow.net

Distribution of ODNS Components Worldwide



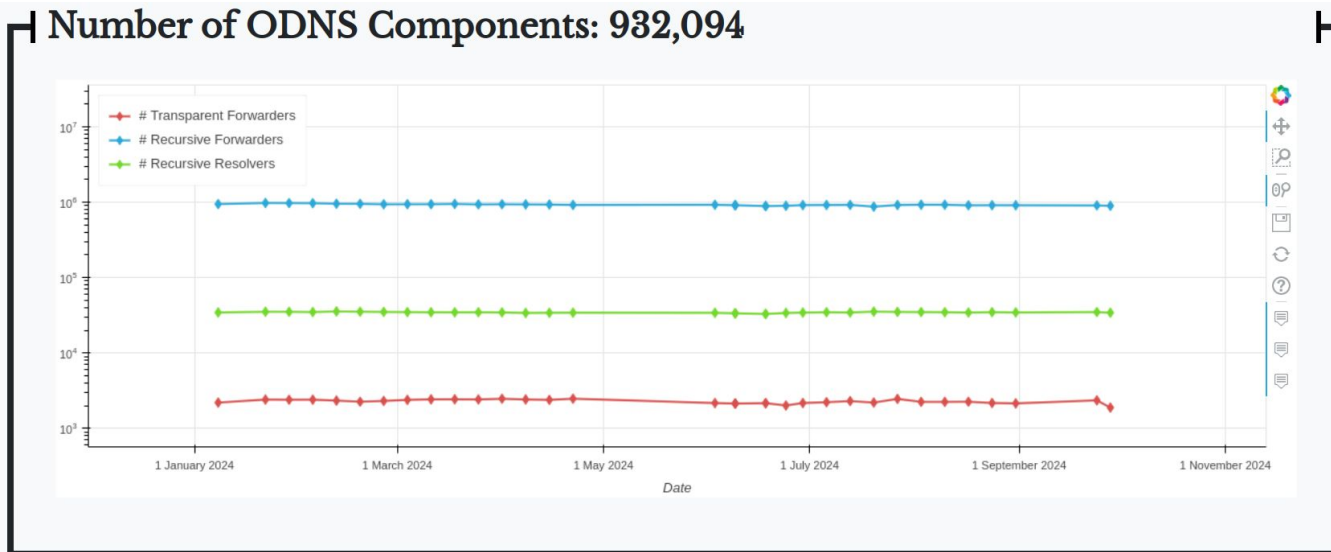
Backup

DNS over UDP



1. There is a slight decreasing trend for transp. and rec. forwarders
2. We were able to reduce the amount of transparent forwarders by approx. 250K (event A)
 - a. How? We got in contact with a telecom. company that was responsible for more than 250K transp. fwd.
 - b. They updated their packet filter rules.

DNS over TCP



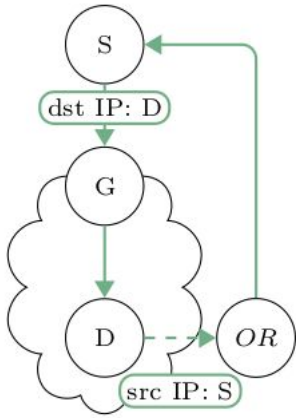
1. Transparent forwarders are rarely deployed over DoTCP
2. Connection-oriented nature of TCP reduces the threat potential significantly

You ship transparent forwarders?

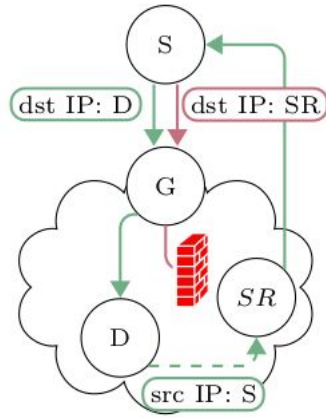
Please, talk to us. We would like to understand your implementations better.

We have identified **MikroTik** and **Cisco** devices that are misconfigured by default.

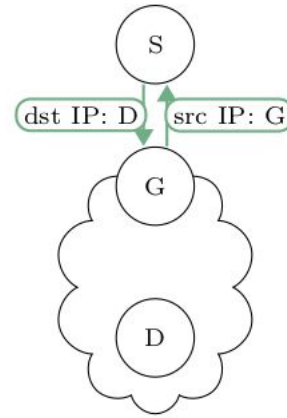




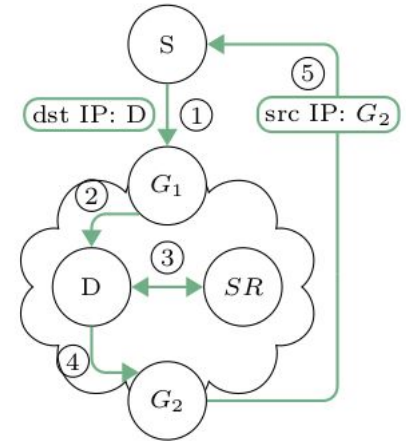
(a) D = Transp. Fwd.; D uses open resolver



(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

Regarding CPE devices that act as transparent forwarders

[<https://seclists.org/nanog/2013/Aug/132>]

- (1) Some CPE devices provide DNS resolution by just **forwarding** DNS requests to a predefined resolver, i.e., they do not implement a full resolver.
- (2) CPE devices usually implement NAT, i.e., at the **LAN interface**, they rewrite the source IP address and forward the incoming packet. This includes DNS requests.
- (3) CPE devices do not rewrite source IP addresses of incoming packets from a **WAN interface**.
- (4) Combining (1), (2), (3) means that (faulty) implementations also forward DNS requests received from the WAN interface without rewriting the source IP address.

Understanding which type of CPE devices are affected will help to approach vendors and fix this bug.