Silent Leakage

A Forensic Analysis of Resolver Transparency Failures in Hardened DNS Environments **Published By © CoreNetSolution** Date: July 2025 Contact: corenetsolution.com@gmx.us
Website: https://www.corenetsolution.com

Executive Summary

Controlled DNS forensics tests uncovered a persistent and underreported phenomenon: DNS query traffic leaks silently to unauthorized resolvers—even in hardened environments with DNSSEC, DNS-over-TLS (DoT), strict ACLs, and segmented BIND 9.18 configurations.

Up to 65 resolvers responded to outbound queries despite no fallback, proxy, or tunneling enabled.

These findings challenge assumptions around DNS trust boundaries, privacy controls, and resolver exclusivity, and reveal behaviors invisible to traditional configuration audits.

Background & Purpose

DNS encryption has become mainstream, yet endpoint transparency and resolver predictability remain blind spots—particularly in enterprise-grade deployments.

This research tests whether locked-down configurations enforce query flow integrity, or merely simulate it. The goal: uncover behavioral drift and policy violations that occur below the surface.

Test Environment & Methodology

Software Stack:

- BIND 9.18 with DNSSEC validation
- Custom ACLs and recursion disabled
- No fallback, stub, or dynamic discovery (resolv.conf locked)

Networks Used:

- Three ISPs (US, EU, Asia)
- Clean network stacks — no VPNs, split DNS, proxies, or browser DoH

Protocols Enforced:

- DNS-over-TLS via trusted upstreams only (e.g., Cloudflare)

Tools Used:

- `tcpdump` for passive outbound DNS and TLS capture
- Third-party observables:
    - vpntesting.com – resolver telemetry
    - browserscan.net – fingerprinting

Session Duration: 3–5 hours per config, including TTL purge and reboots

Key Findings

1. Persistent Resolver Leakage

- 65+ unauthorized resolver IPs responded, spanning multiple ASNs
- CDN, ISP edge nodes, and unexpected IPv6 paths were observed
- Leakage occurred even with DoT pinned to a single upstream

2. CDN Injection & ISP-Assisted Re-Routing

- TCP connections exited via non-authorized networks
- Edge redirection detected via Akamai and Fastly IP ranges
- Redirection masked dig output — but traceable via packet capture

3. Metadata Exposure on Encrypted Paths

- Plaintext queries weren't exposed, but timing, resolver identity, and inferred hostnames were visible
- Leakage was behavioral — not payload-based

4. Behavior Resilient to Flushes & Reboots

- Persisted across DNS flushes, service restarts, TTL expiry cycles, and full system reboots

Case Highlight: IONOS Login Redirect Loop

Repeated login attempts to IONOS web builder failed with:

> *"auth.ionos.com redirected you too many times."*

Standard fixes (cookie purging, DNS flushes, browser resets) had no effect.

Inference: Session state was disrupted by invisible resolver shifts, CDN injection, or edge manipulation — undermining token-based authentication and SSO integrity.

Implications

Area	Concern
Security	Undetectable poisoned path responses; unauthorized resolvers intercepting queries
Privacy	Metadata leakage even over encrypted routes; resolver profiling possible
Operations	ACL/SLA assumptions invalidated by mid-path drift; audit blind spots for DoT/CDN systems

Recommendations

Stakeholder	Recommended Action
Sysadmins	Perform packet-level inspection, not just config audits
Vendors	Surface resolver ASN visibility in encrypted DNS products
ISPs/CDNs	Disclose DNS rewriting policies; offer opt-outs
Researchers	Treat resolver behavior as dynamic; capture runtime conditions

Future Work

This opens deeper questions around resolver enforcement under encryption and session stability across platforms. Upcoming tests will explore:

- IPv6-specific resolver path behavior
- Mobile OS divergence from desktop
- DoH/DoT bypass validation on Android hardware
- Collaborative research with transparency advocacy groups

Contact & Collaboration

For dataset access, media inquiries, or joint research proposals: Contact: corenetsolution.com@gmx.us Website: https://www.corenetsolution.com

[LinkedIn Article Link]