Heads-up Talk:

# Measurement of Systemic DNS Resolver Vulnerabilities

(Informing Six DNSOP I-Ds)

Xiang Li, Yuqi Qiu

Nankai University


IETF 125 · MAPRG · Lightning Talk · March 2026

# How Secure Are DNS Resolver Implementations?

# Short Answer: Widespread Exploitable Divergences

DNS specifications leave critical behaviors underspecified, ambiguous, or undefined. Implementations diverge — and attackers exploit these gaps.

| 90+ | 6 | 24–28 | >20,000× | 82% |
|---|---|---|---|---|
| CVEs assigned | novel attacks | software tested per study | amplification factor | software vulnerable |

## Who is affected?

Every major DNS implementation we tested: BIND, Unbound, Knot, PowerDNS, Microsoft DNS, Cloudflare, Google Public DNS, Quad9…

Tested up to 2.4M open resolvers per study — vulnerabilities found at every scale.

# Why? — RFC Ambiguity Creates a Systemic Attack Surface

**DNSBomb** S&P '24

**Correct mechanisms combined**

Timeout + aggregation + fast-return → each correct, dangerous combined
Draft proposes BCP

**RebirthDay** CCS '25

**Extension introduces new gap**

RFC 7871 (ECS): one-sentence gap → undefined interaction with query aggregation

**TsuKing** CCS '23

**RFC expression ambiguous**

“if RD=0, use local data” → 4 implementations, 4 behaviors (BIND, Unbound, Knot, PowerDNS)

**PHOENIX DOMAIN** NDSS '23

**Principles without algorithm**

RFC 1034 §5.3.3: cache trust levels defined, but no insert/expire algorithm
→ TOCTOU + deep subdomain exploits

**MaginotDNS** USENIX Sec '23

**Concept + deployment blind spot**

RFC 2181 §5.4.1: bailiwick defined but no checking algorithm; CDNS (41.8% of open DNS!) ignored by RFC

**TUDOOR** S&P '24

**True underspecification**

“discard malformed responses” — never defines what’s invalid
28 software, 28 different behaviors

# 6 Attacks, 6 Drafts

| Attack | Venue | Proposed Fix | Key Measurement | CVEs | Draft |
|---|---|---|---|---|---|
| **Area 1 — Cache & Delegation** | | | | | |
| **PHOENIX DOMAIN** | NDSS '23 | Scrutinize deep delegations; limit cache TTL for deep names | 210K resolvers; >25% still resolve after 1 month | 9 | deep-delegation-scrutiny |
| **MaginotDNS** | USENIX Sec '23 | Uniform bailiwick checks across modes; CDNS-specific rules | 41.8% open DNS are CDNS; 35.5% of CDNS vulnerable | 3 | enhanced-bailiwick |
| **Area 2 — Query Handling & Amplification** | | | | | |
| **TsuKing** | CCS '23 | RD=0: MUST NOT recurse or forward with RD=1 | 1.3M resolvers; 14.5% vuln.; PAF ≥ 3,700× | 3 | rd-flag-clarification |
| **DNSBomb** | S&P '24 | BCP: response pacing + shorter timeout (1.5–3s) | ALL resolvers; peak 8.7 Gb/s; BAF >20,000× | 10 | resolver-resilience |
| **RebirthDay** | CCS '25 | no-ECS-support tracking per zone (Updates RFC 7871) | 18/22 software; ~365K resolvers (~15%) | 35 | ecs-aggregation-fix |
| **Area 3 — Packet Pre-processing** | | | | | |
| **TUDOOR** | S&P '24 | Formalized response pre-processing state machine | 24/28 software; 23.1% of 1.8M resolvers | 33 | response-preprocessing |

# Highlight: DNSBomb



**Beneficial DNS mechanisms (timeout, aggregation, fast-returning) turned into a pulsing DoS weapon**

## Accumulate → Amplify → Concentrate

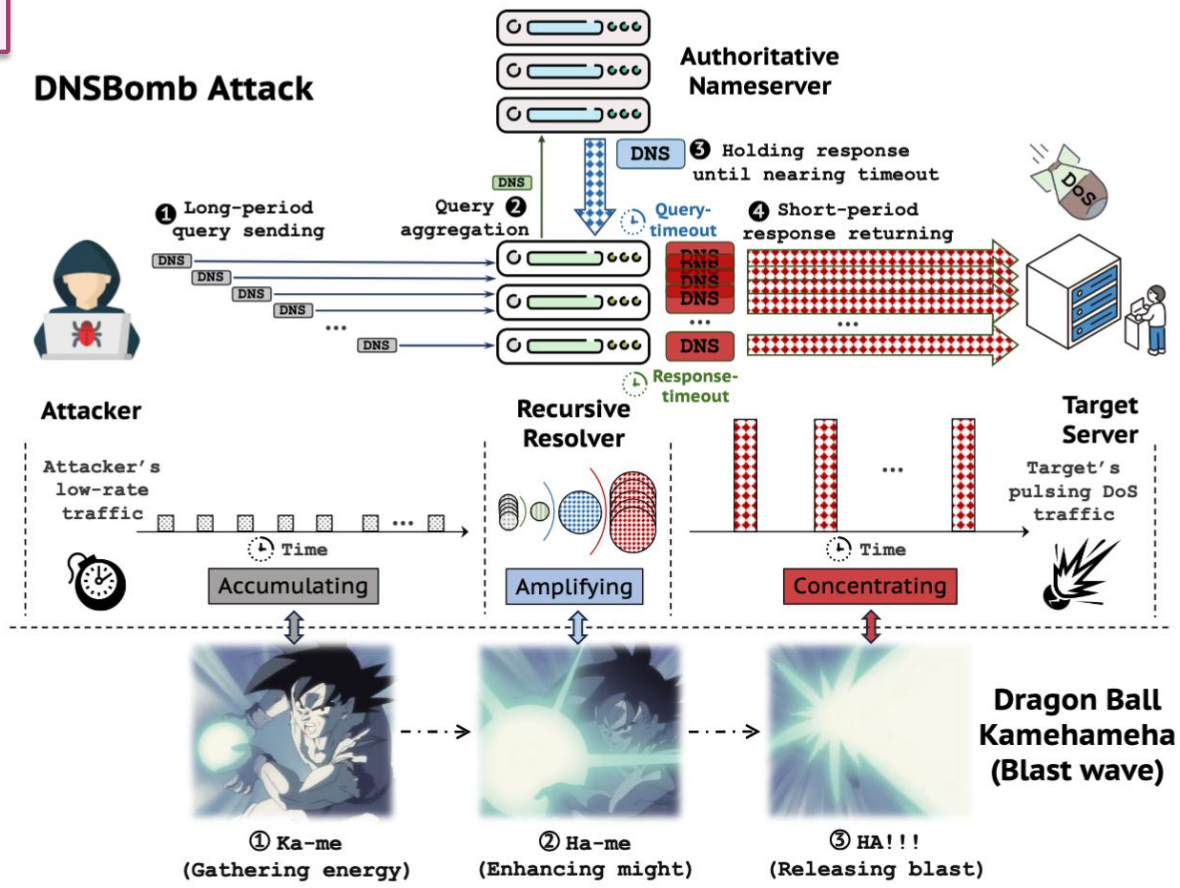
Low-rate queries held by timeout (1–15s), amplified by aggregation, then all responses released simultaneously

**8.7Gb/s**
peak pulse

**>20,000×**
BAF

**100%**
resolvers exploitable

Draft fix: response pacing + shorter timeout (1.5–3s)
Unbound BAF: 21,881× → 20.2× (99.9% reduction)



# Highlight: RebirthDay



**RFC 7871 (ECS) extension gap revives a 20-year-old cache poisoning attack**

**18/22** software vulnerable

**35** CVEs

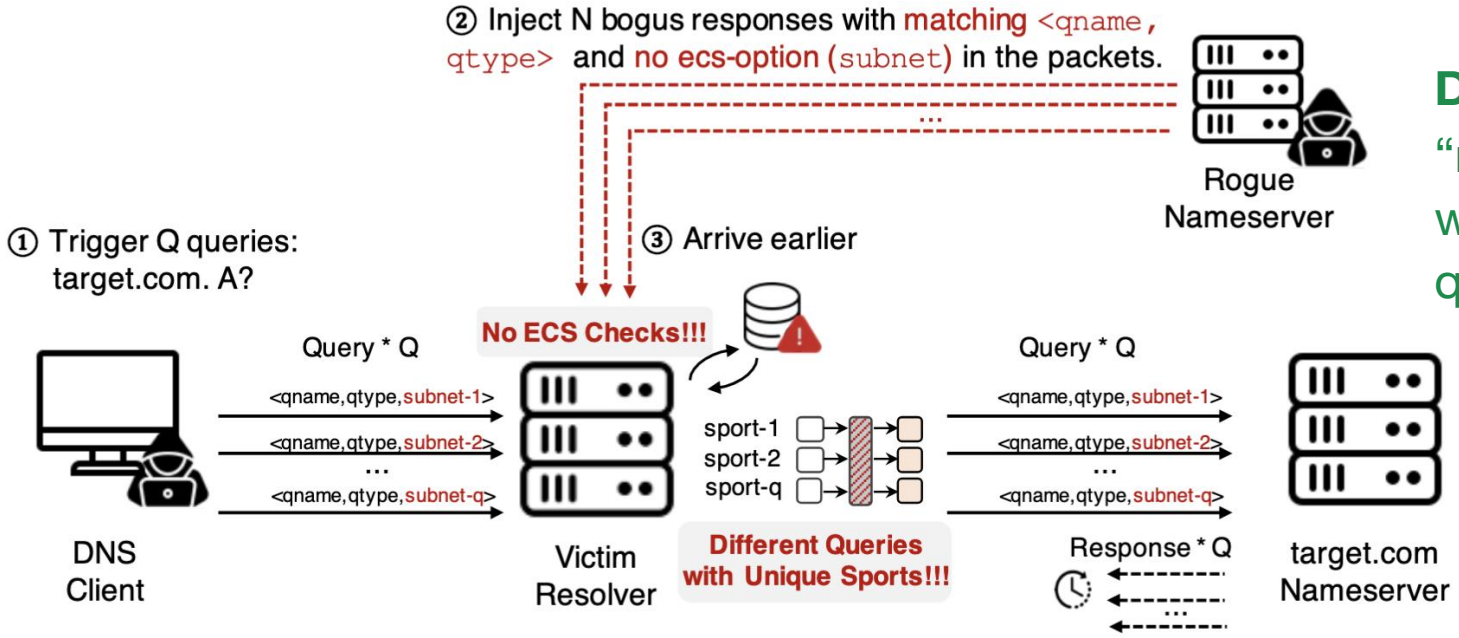
**~15%** of 2.4M resolvers

## Bypass → Multiply → Collide

① Different ECS prefix = different query → bypass aggregation

② N queries outstanding → spoofed responses to collide

③ RFC 7871: "response without ECS still valid" → matches any query




**Draft updates RFC 7871:**

"no-ECS-support" state tracking per zone — when zone doesn't support ECS, aggregate all queries regardless of ECS options

# Call to Action — We Welcome Your Review!

**These issues arise from underspecified RFCs, not careless implementations.**

Vendors are patching — but without standardized guidance, new implementations will face the same ambiguities.

6 drafts submitted to DNSOP working group

Each draft includes concrete, implementable fixes:

**Area 1 — Cache & Delegation**

deep-delegation-scrutiny (Phoenix Domain)
enhanced-bailiwick (MaginotDNS)

**Area 2 — Query Handling & Amplification**

rd-flag-clarification (TsuKing)
resolver-resilience (DNSBomb — BCP)
ecs-aggregation-fix (RebirthDay)

**Area 3 — Packet Pre-processing**

response-preprocessing (TUDOOR)

**Thank you! Questions → lixiang@nankai.edu.cn or qiuyuqi@mail.nankai.edu.cn**