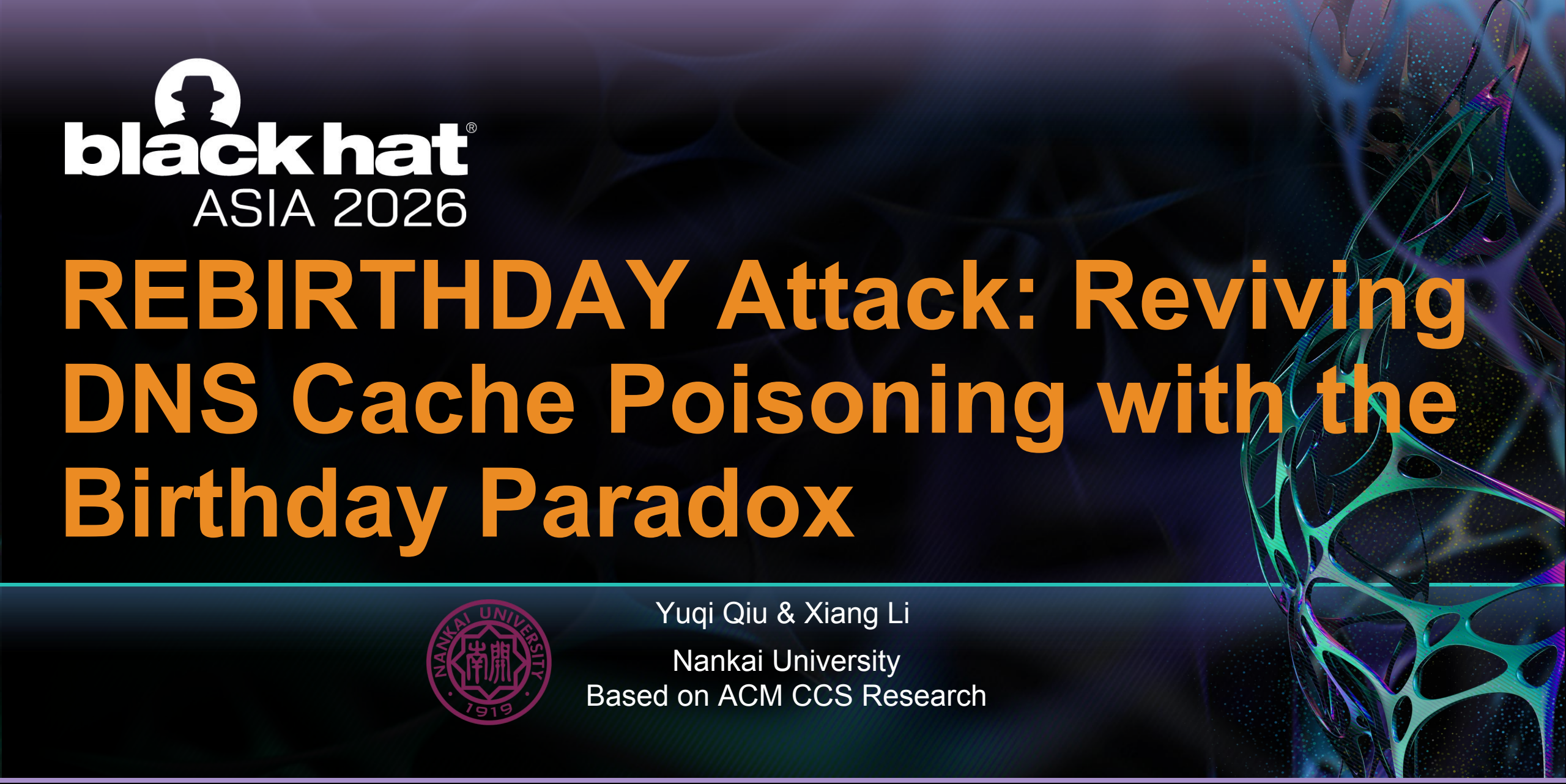

black hat®
ASIA 2026
APRIL 21-24, 2026
MARINA BAY SANDS / SINGAPORE



REBIRTHDAY Attack: Reviving DNS Cache Poisoning with the Birthday Paradox

Yuqi Qiu & Xiang Li

Nankai University

Based on ACM CCS Research

Attack Impact

- A classic, long-dead attack is back. The DNS Birthday Attack, mitigated since 2002, is exploitable again
- This vulnerability is widespread, affecting 18 of 22 major DNS software, including products from vendors like Unbound, PowerDNS, Cisco, and TP-Link

- **DNS Birthday Attack**
- **2002 - Defeated ==> Today - Revived!**

Cybersecurity

Protocol security

Vulnerability discovery

Large-scale model security.

Xiang Li

Associate Professor,

Nankai University

DNS security

Network measurement

Yuqi Qiu

PhD Student,

Nankai University

AGENDA

Talk Outline

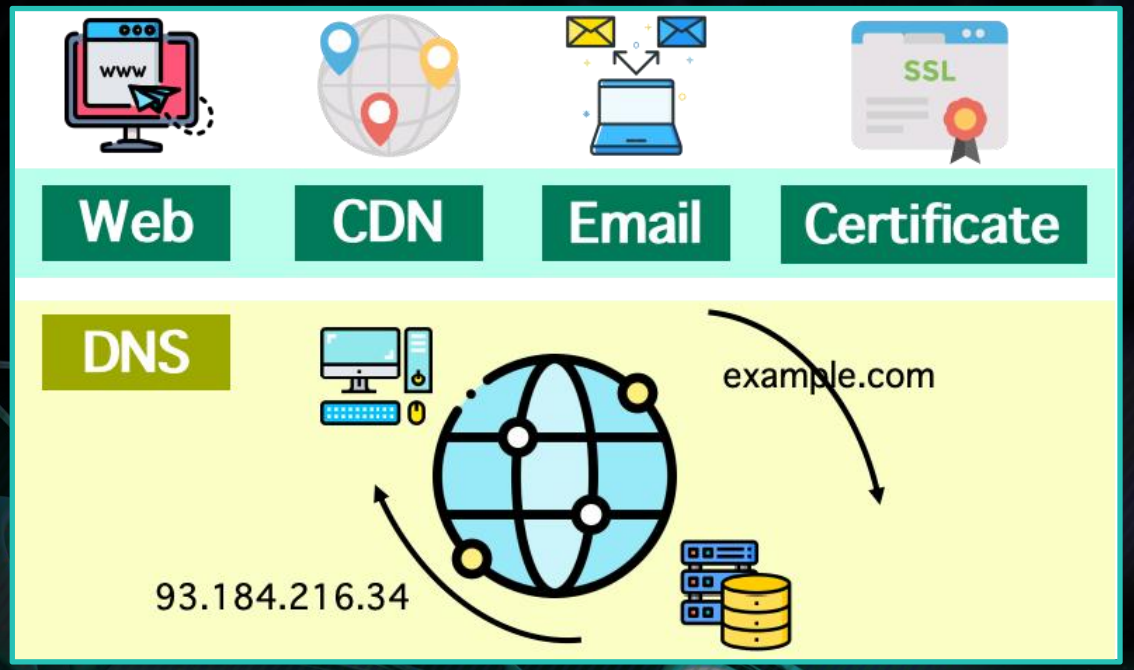
REBIRTHDAY: Reviving DNS Cache Poisoning	Time
DNS Background and the history of cache poisoning attacks	Part 1
The REBIRTHDAY Attack: exploiting ECS to bypass query aggregation	Part 2
Evaluation: end-to-end attack experiments on 4 DNS software	Part 3
Real-World Impact: routers, public DNS, and open resolvers	Part 4
Mitigation, Responsible Disclosure, and 35 CVEs	Part 5

BACKGROUND

DNS Resolution & Cache Poisoning

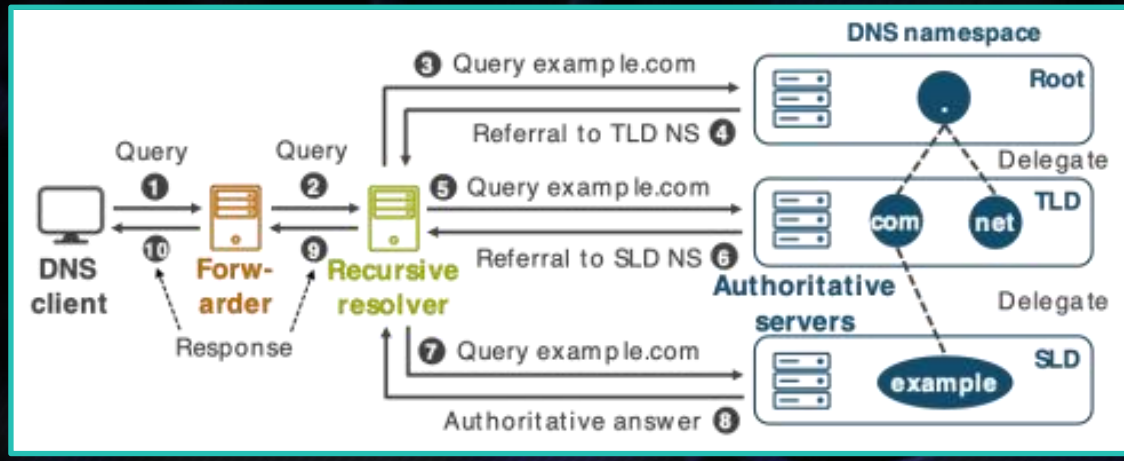
Domain Name System

- **DNS Overview**
  - Translates human-readable domain names to machine-readable IP addresses.
  - The entry point for nearly all Internet activities: Web, CDN, Email, Certificates.



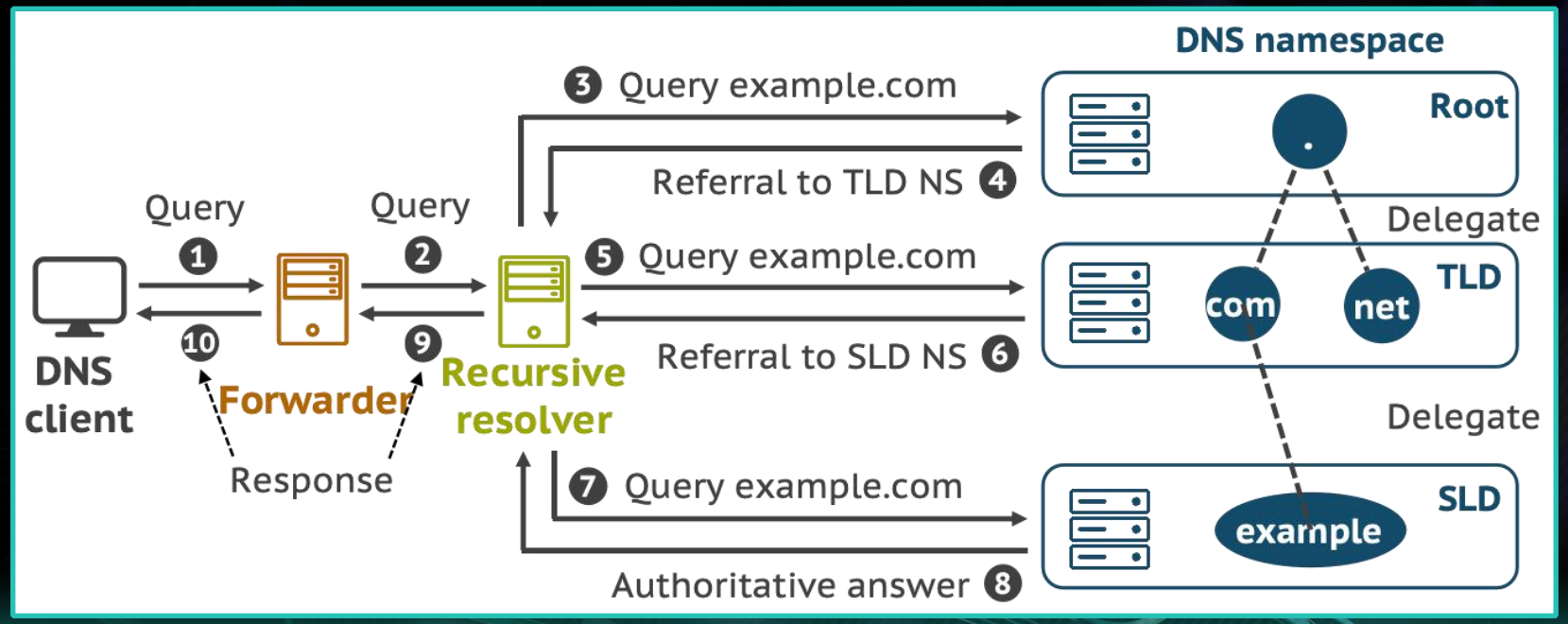
Domain Name System

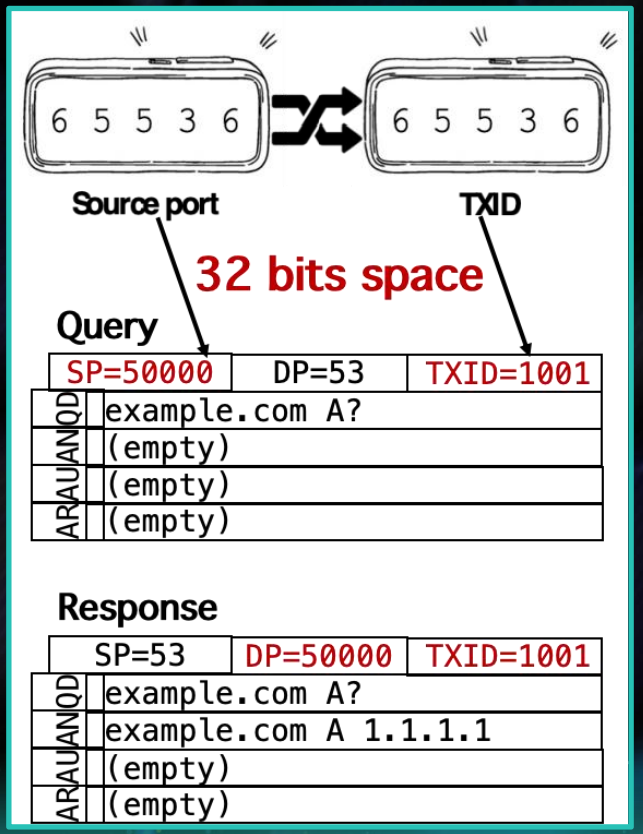
- **Hierarchical Name Space**
  - Authoritative zones: root, TLD, SLD → DNS records
  - Domain delegation → Domain registration
- **Multiple Resolver Roles**
  - Client, forwarder, recursive, authoritative
  - Caching
- **Iterative Resolution Process**
  - Client-server style



Domain Name System

- **DNS Resolution Process**
  - Primarily over UDP
  - Iterative and recursive
  - Caching





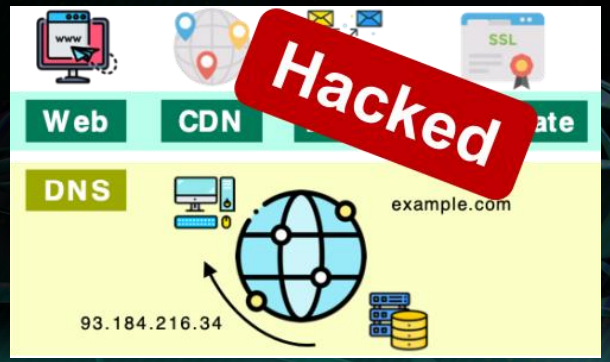
Takeaway

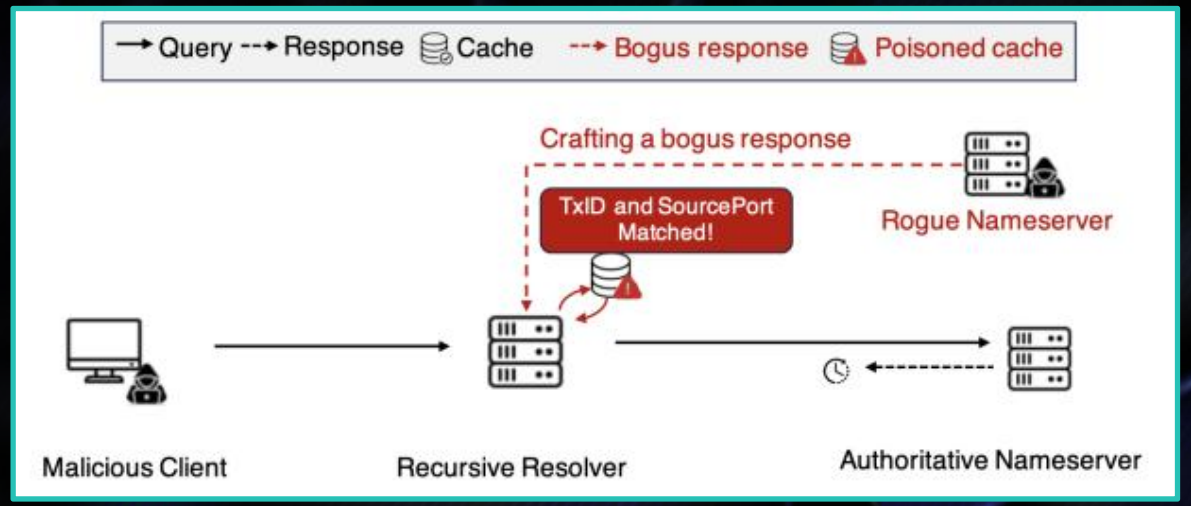
Since DNS is the cornerstone of the Internet, enabling multiple critical services and applications,

Attackers have long been trying to manipulate its response for hijacking via **cache poisoning attacks**.

DNS Cache Poisoning

- Objective
  - Injecting forged answers into resolvers' cache
- Goal
  - Hijack user traffic
  - Redirect to malicious destinations
- Technique
  - Cat-and-mouse game

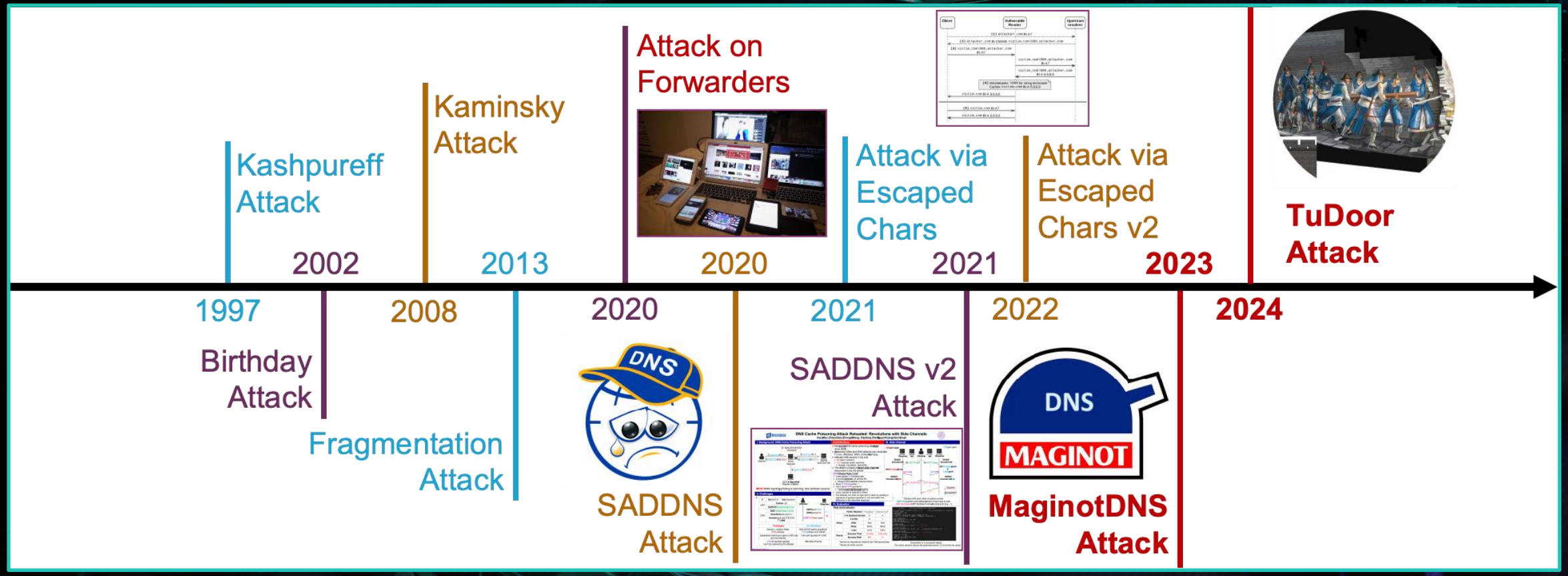




The Evolution of DNS Cache Poisoning

- From Brute-Force
  - Transaction IDs and source ports...
- To Sophisticated Techniques
  - Vulnerabilities, protocol flaws, and side channels.
- Defenses
  - TXID randomization, birthday protection, and DNSSEC

The Evolution of DNS Cache Poisoning

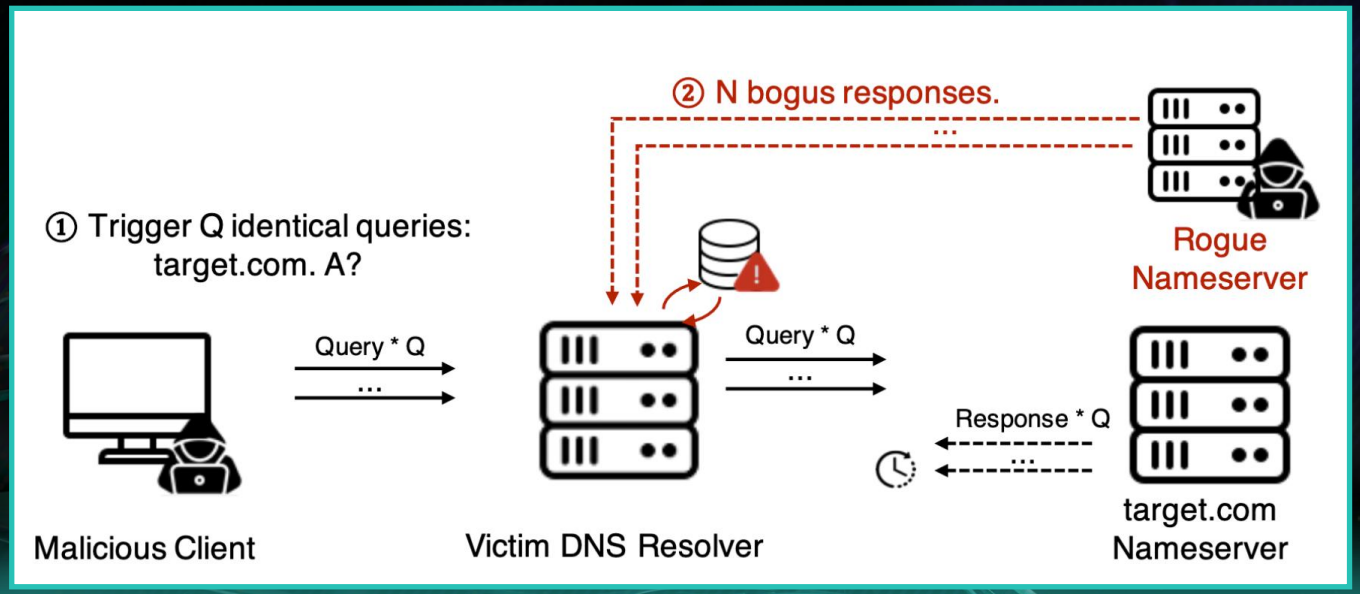


Question

Are all old threats truly gone?

The Classic DNS Birthday Attack (2002)

- Core Principle: statistical "Birthday Paradox"
- Method: forcing a resolver to issue multiple simultaneous queries for the same domain
- Vulnerability: creating a large set of valid, in-flight TXIDs for the attacker to target



The Classic DNS Birthday Attack (2002)

- The probability of a successful poisoning is not linear; it grows rapidly as the number of simultaneous queries, Q, increases.

Total size of the randomness (source port or TxID) space

Number of unique source port or TxID collisions

Total number of DNS queries

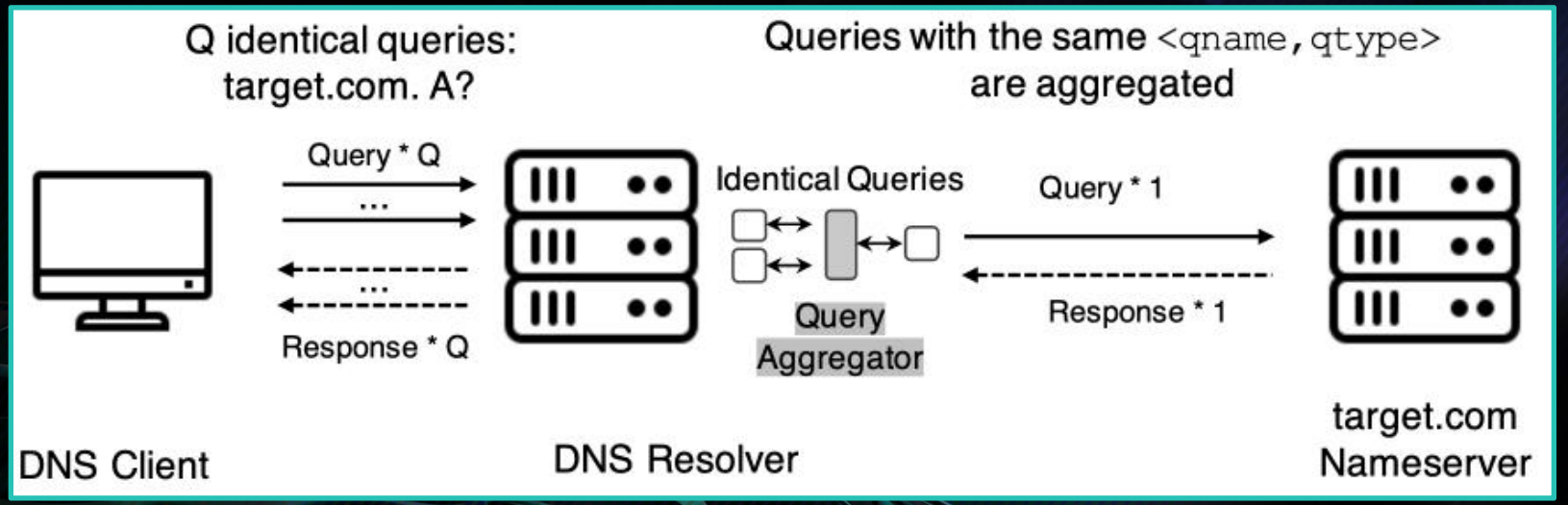
$$P_{\text{single}} = 1 - \prod_{i=0}^{n-1} \left(\frac{T - Q \cdot i}{T} \right)$$

Probability of a successful DNS Birthday attack after **r** attack rounds:

$$P_{\text{success}} = 1 - \left(1 - P_{\text{single}}\right)^{r}$$

The Defense: Query Aggregation

- **Mitigating the Birthday Attack**
  - Merging identical DNS requests for the same domain name into a single query
  - Requests are considered identical if they share the same key: <qname, qtype>

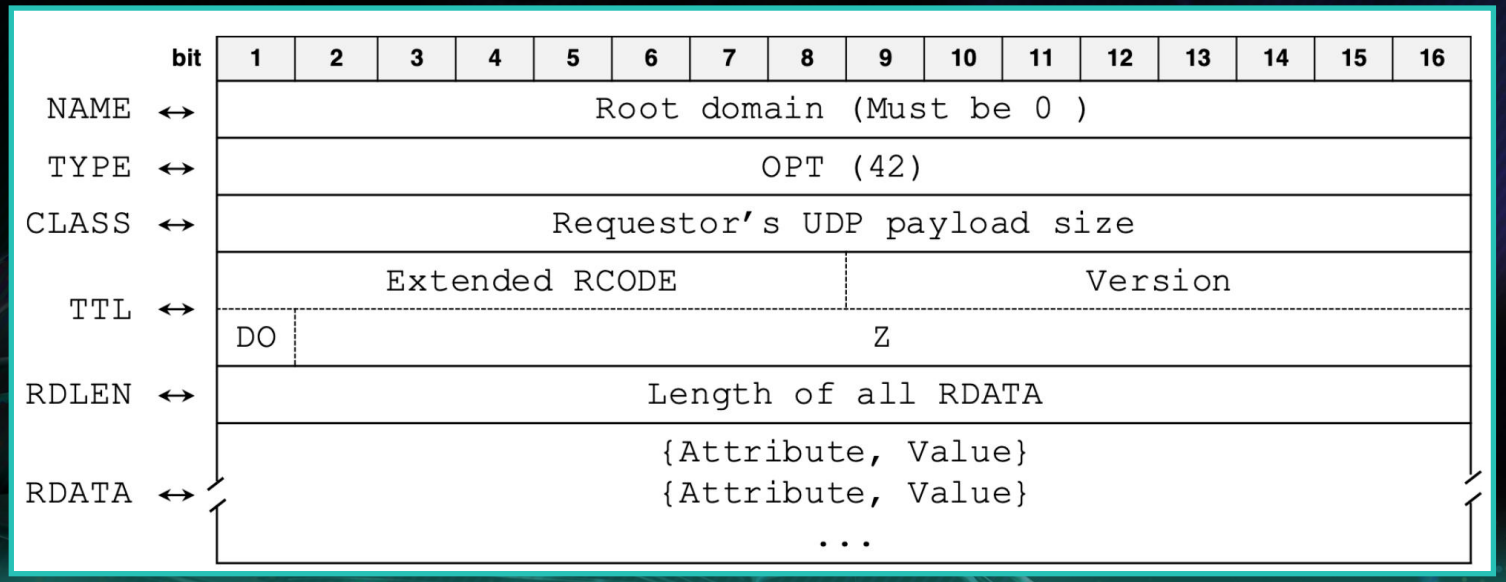


REBIRTHDAY ATTACK

Exploiting ECS to Bypass Query Aggregation

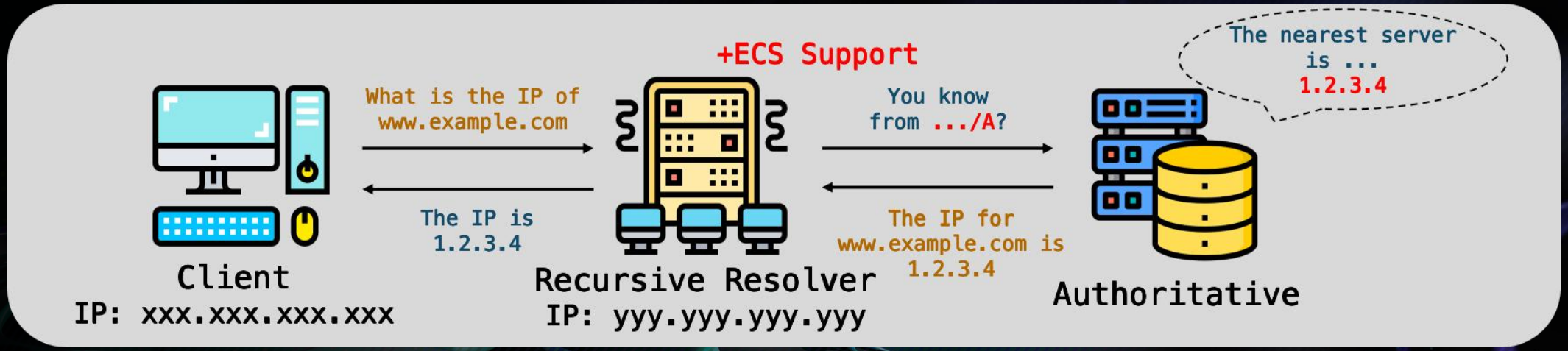
DNS Extensions EDNS(0)

- Purpose: Extension Mechanisms for DNS (RFC 6891) was introduced to overcome the original 512-byte DNS message size limit
- Mechanism: It adds an OPT pseudo-record to the additional section of a DNS message, allowing for new flags and data
- Importance: Foundation for almost all modern DNS features



EDNS Client Subnet (ECS)

- Purpose: ECS (RFC 7871) is an EDNS(0) option designed to optimize geo-located DNS responses (e.g., for CDNs)
- Mechanism: A resolver includes a portion of the client's IP address (the subnet) in the query it sends to an authoritative server
- Effect: Authoritative can provide a more optimal response



New Attack Surface

- Subnet-Specific Caching: When caching a response that was generated using ECS, the resolver associates the cached entry with the specific subnet used in the query.
- The Consequence: For a subsequent query from a different subnet, the resolver cannot use the existing cache entry. It must issue a new query upstream. This is a critical feature for correctness.

Vulnerability I: Aggregation is Bypassed

For resolvers that support ECS, the identifier for a unique query is a 3-tuple: <qname, qtype, subnet>

An attacker can send hundreds of queries for

the same domain with a different, spoofed subnet,

recreating the perfect environment for a Birthday Attack.

Vulnerability II: Weak Response Validation

The Rule (RFC 7871): a response without an ECS option is still a valid reply to a query that had an ECS option

Spoofed response packets can be simple DNS responses, relying only on **matching the <qname, qtype> tuple**

This dramatically **lowers the complexity of the attack**

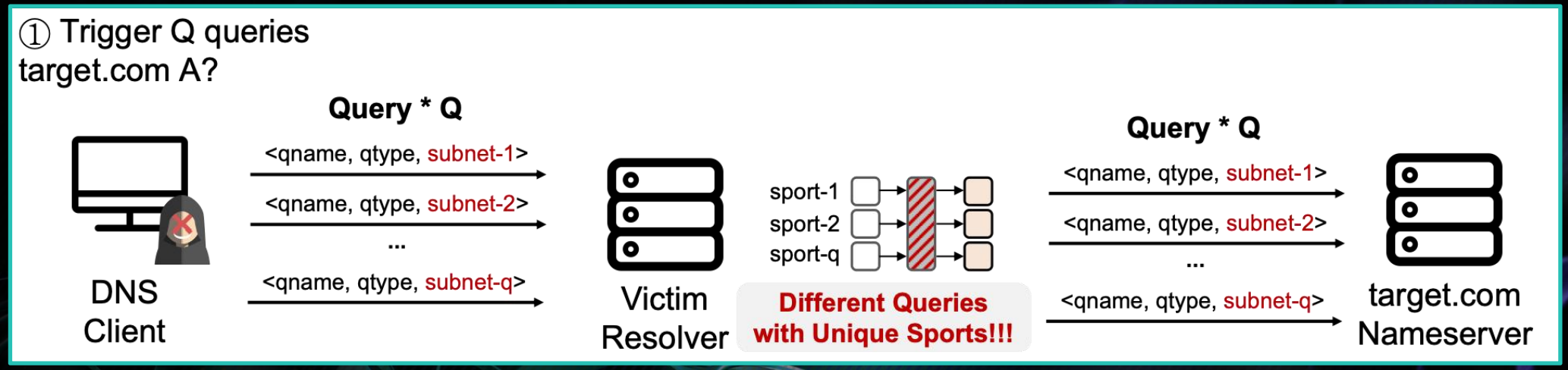
Attack Overview of REBIRTHDAY

- Attacker
  - An off-path DNS client
- Capabilities
  - Trigger domain queries
  - Learn the target resolver's egress IP
  - Spoof the source IP address
- Feasibility
  - IP spoofing is still feasible in over 19% of IPv4 ASes

Attack Steps

- Step 1: Triggering Multiple Queries

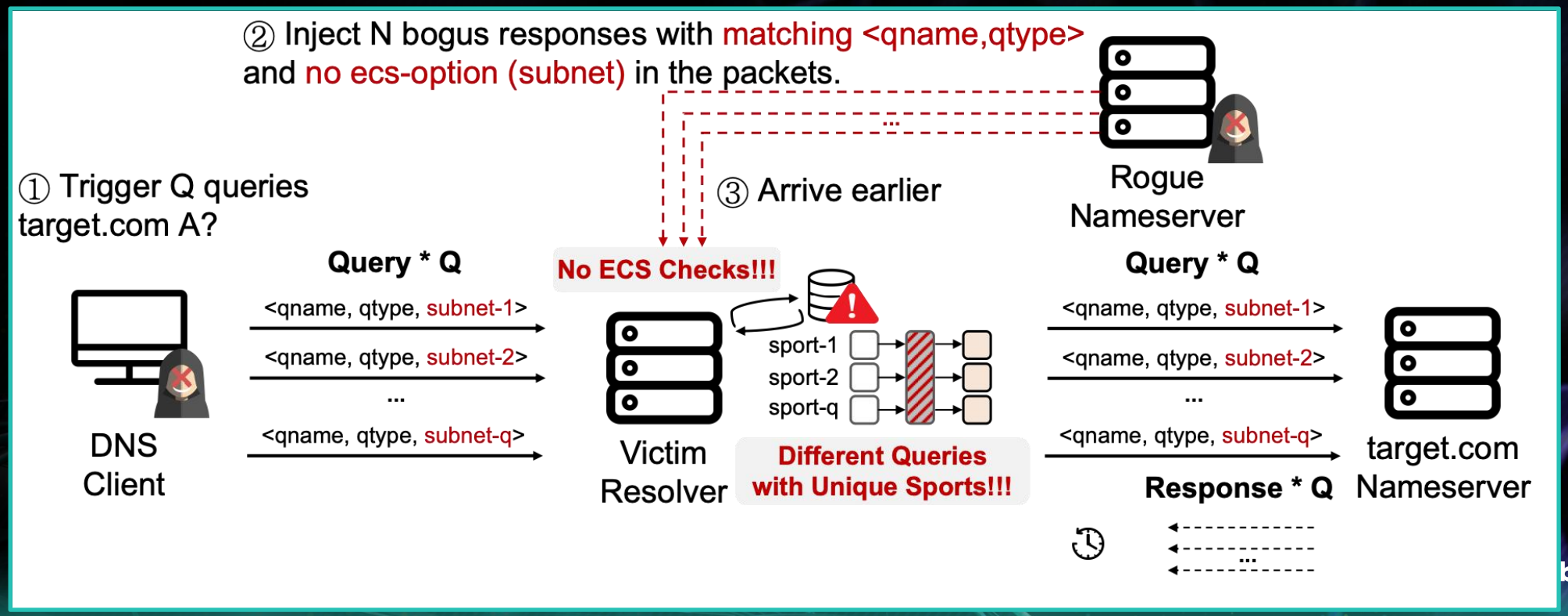
  Sends Q crafted DNS queries, each query contains a unique, forged client subnet



Attack Steps

- Step 2: Injecting Malicious Responses

  Guesses a small number of source ports and brute-forces all 65,536 possible TXIDs



EVALUATION

Testing the Attack on Real Software

VULNERABLE DNS SOFTWARE

- **22 DNS Software Analyzed: 18 Vulnerable**
  - 9 recursive resolvers + 13 forwarders tested
- **ECS Bypass Vulnerability (6 Software)**
  - BIND, Unbound, PowerDNS, Technitium, Dnsmasq, Pi-hole
  - Missing ECS coherence checks allow query aggregation bypass
- **No Query Aggregation (11 Software)**
  - HickoryDNS, CoreDNS, DNSDist, AdGuard, YogaDNS, and others
- **Poor Randomization (Additional Flaws)**
  - SmartDNS, DNSDist, Acrylic DNS: predictable ports/TxIDs

End-to-End Attack Experiment

- **Success Rate**
  - 100% success rate (20 out of 20 trials) against Unbound, PowerDNS Recursor, and CoreDNS
- **Average Time**
  - The average time to a successful poisoning was 358 seconds

Software	Average Round	Average Time	Success Rate
Unbound	263	593s	20/20
PowerDNS Recursor	328	237s	20/20
CoreDNS	20	245s	20/20

REAL-WORLD IMPACT

Measuring Vulnerable Resolvers at Scale

IMPACT: ROUTERS & PUBLIC DNS

- **Wi-Fi Routers: 16 of 21 Vulnerable**
  - ASUS, CISCO, D-Link, Linksys, TP-Link, ZTE, and more
  - 12 routers lack query aggregation entirely
  - 4 additional routers vulnerable due to predictable ports/TxIDs
- **Public DNS Services: 14 of 45 Vulnerable**
  - 8 services affected by ECS bypass, 3 by poor query aggregation

IMPACT: OPEN DNS RESOLVERS

- **Internet-Wide Scan: 2.4 Million Open Resolvers**
  - Scanned IPv4 UDP port 53 using XMap (Oct-Dec 2024)
  - 232 regions, 25,711 autonomous systems
- **Key Findings**
  - 14.1% support ECS queries upstream; 29% return ECS to clients
  - 80%+ show no significant query aggregation (less than 3 queries)
  - 15%+ make 25 or more queries (50% attack success in 1,800 rounds)
- **At least 365,000 (15%) open resolvers vulnerable to REBIRTHDAY**

MITIGATION

- **Root Cause**
  - RFC 7871 allows responses without ECS to be considered valid
- **Proposed Solutions**
  - Verify ECS consistency: reject responses missing ECS from ECS-aware servers
  - Aggregate queries within the same ECS scope
  - Enable 0x20 encoding to thwart case manipulation
  - Deploy DNSSEC for cryptographic response validation
  - Implement anomaly detection and rate limiting

RESPONSIBLE DISCLOSURE

- **35 CVEs Assigned**
  - Reported to all affected vendors and DNS service providers
- **Vendor Acknowledgments (7 Vendors)**
  - Unbound, PowerDNS, Technitium, Dnsmasq
  - YogaDNS, Quad9, AdGuard
- **Patches Deployed**
  - Unbound implemented patched version based on our suggestions
  - Ongoing discussions with remaining vendors

Wrap-up

Question?

Check our paper at IEEE S&P 2024

https://doi.org/10.1145/3719027.3744832

Xiang Li
Associate Professor, Nankai University
lixiang@nankai.edu.cn