



REBIRTHDAY Attack: Reviving DNS Cache Poisoning with the Birthday Paradox

Xiang Li, Mingming Zhang, Zuyao Xu, Fasheng Miao, Yuqi Qiu, Baojun Liu, Jia Zhang, Xiaofeng Zheng, Haixin Duan, Zheli Liu, Yunhai Zhang, Dunqiu Fan

Presenter: **Yuqi Qiu**, Nankai University

qiuyuqi@mail.nankai.edu.cn

Oct 2025



Attack Impact

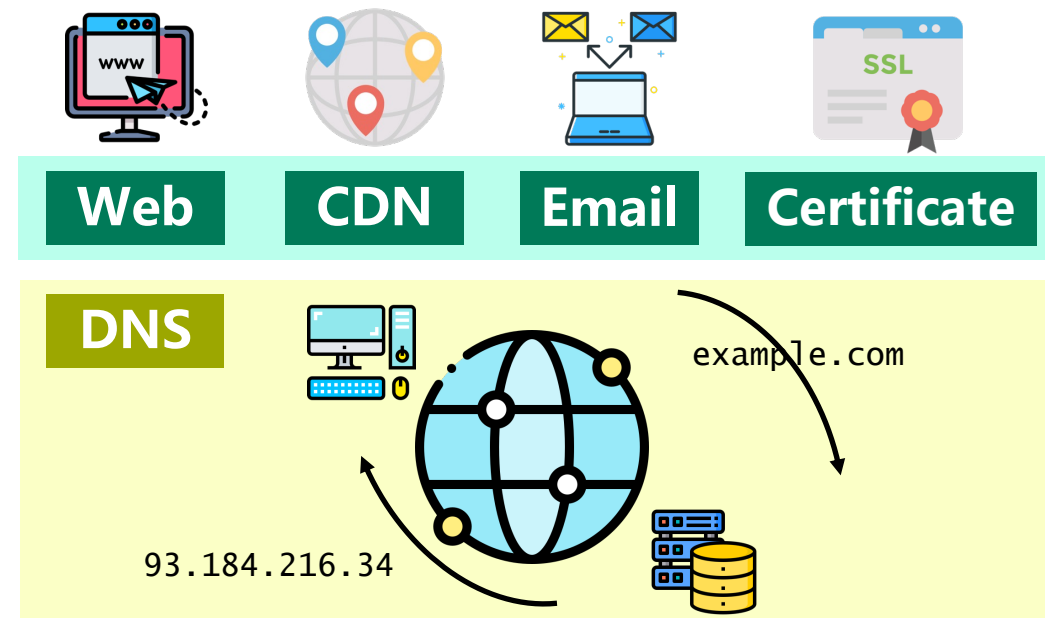
- **A classic, long-dead attack is back. The DNS Birthday Attack, mitigated since 2002, is exploitable again**
- **This vulnerability is widespread, affecting 18 of 22 major DNS software, including products from vendors like Unbound, PowerDNS, Cisco, and TP-Link**

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

Domain Name System (DNS)

➤ 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 (DNS)

➤ Hierarchical Name Space

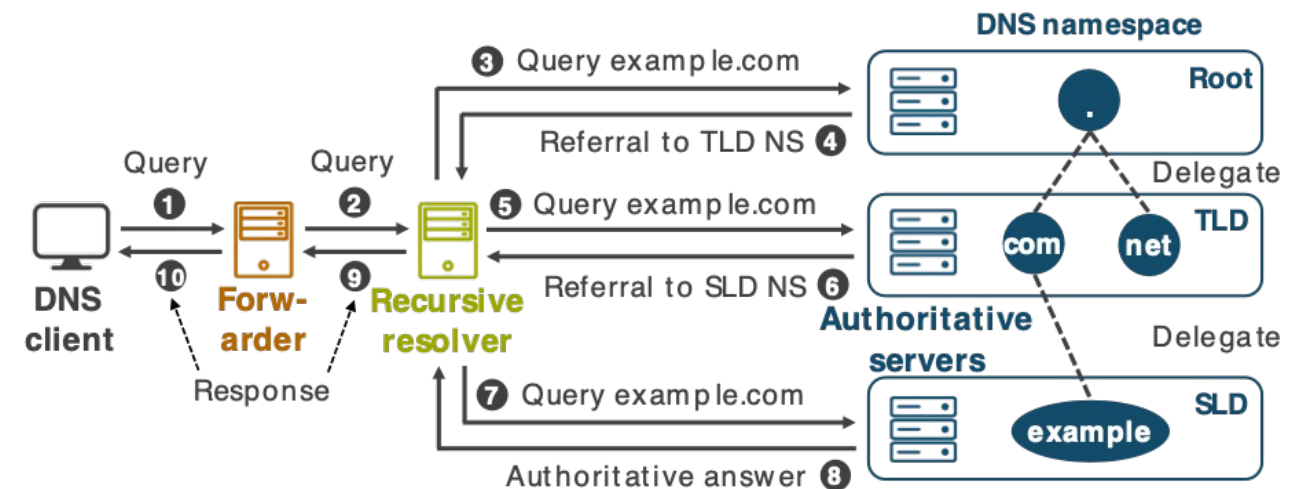
- ❑ Authoritative zones: root, TLD, SLD → DNS records
- ❑ Domain delegation → Domain registration

➤ Multiple Resolver Roles

- ❑ Client, forwarder, recursive, authoritative
- ❑ Caching

➤ Iterative Resolution Process

- ❑ Client-server style

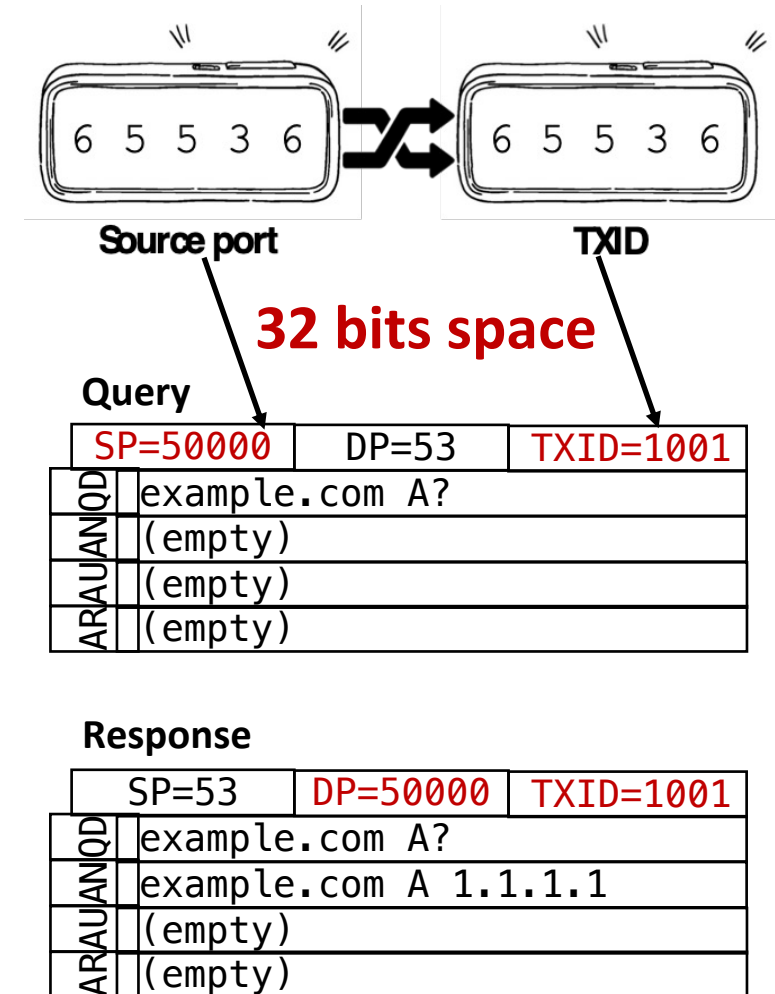
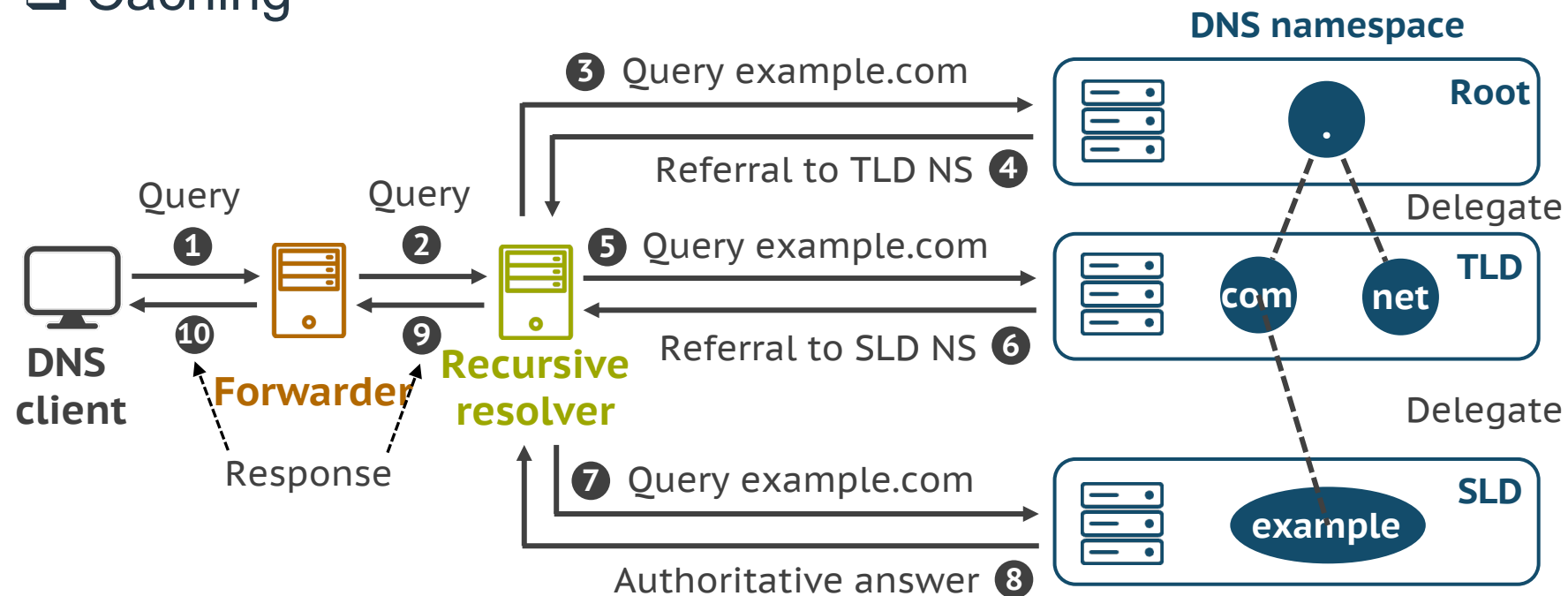


REBIRTHDAY

Domain Name System (DNS)

➤ 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**.

Question

What is DNS cache poisoning?

Since DNS is primarily over UDP, attackers want to **inject forged answers into resolvers' cache.**

REBIRTHDAY

The Threat of DNS Cache Poisoning

➤ Objective

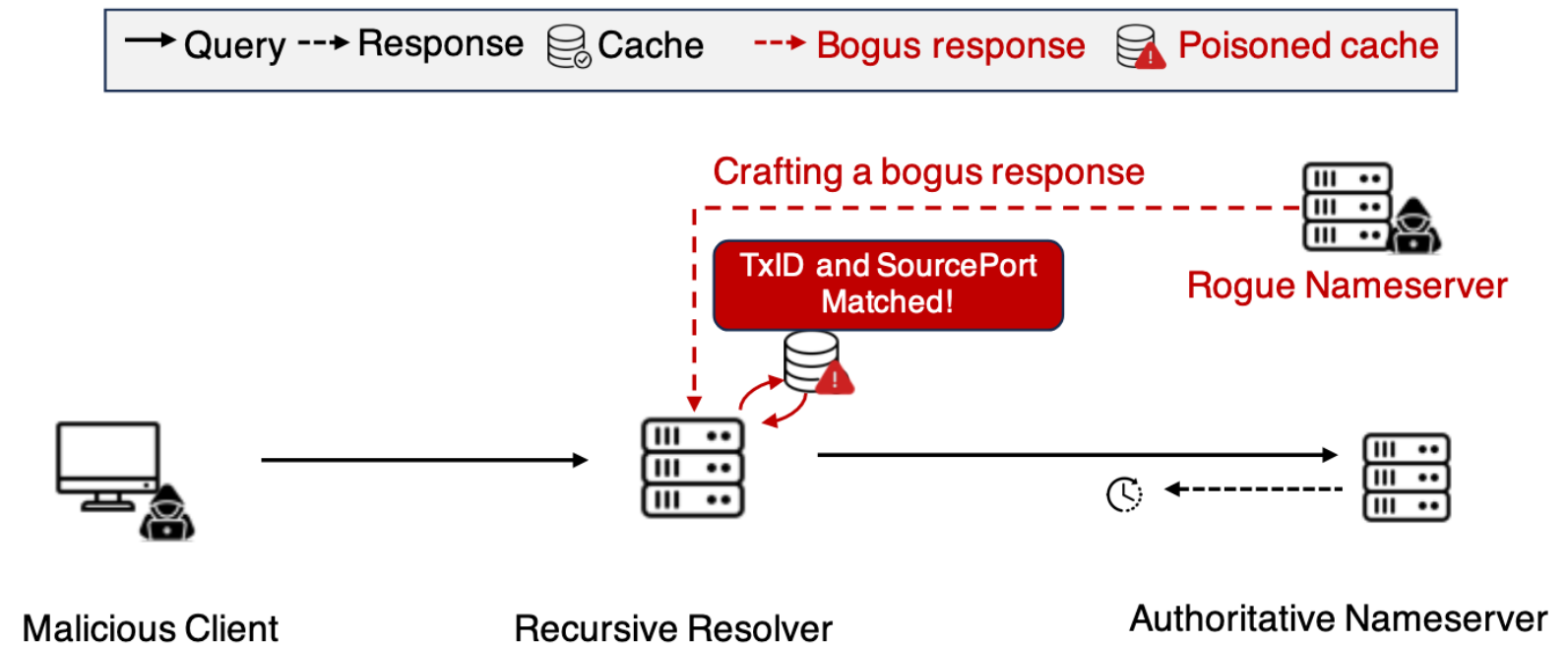
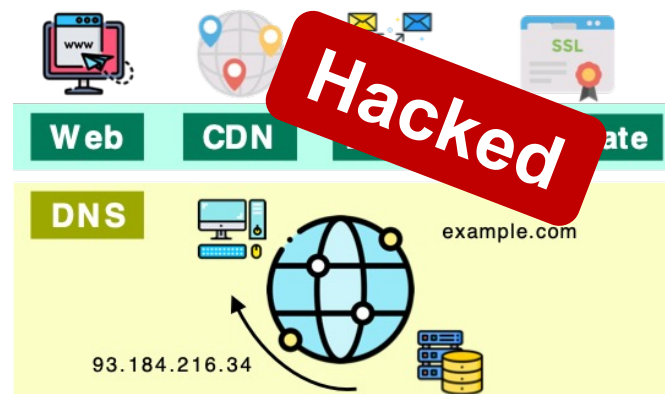
- ❑ Injecting forged answers into resolvers' cache

➤ 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

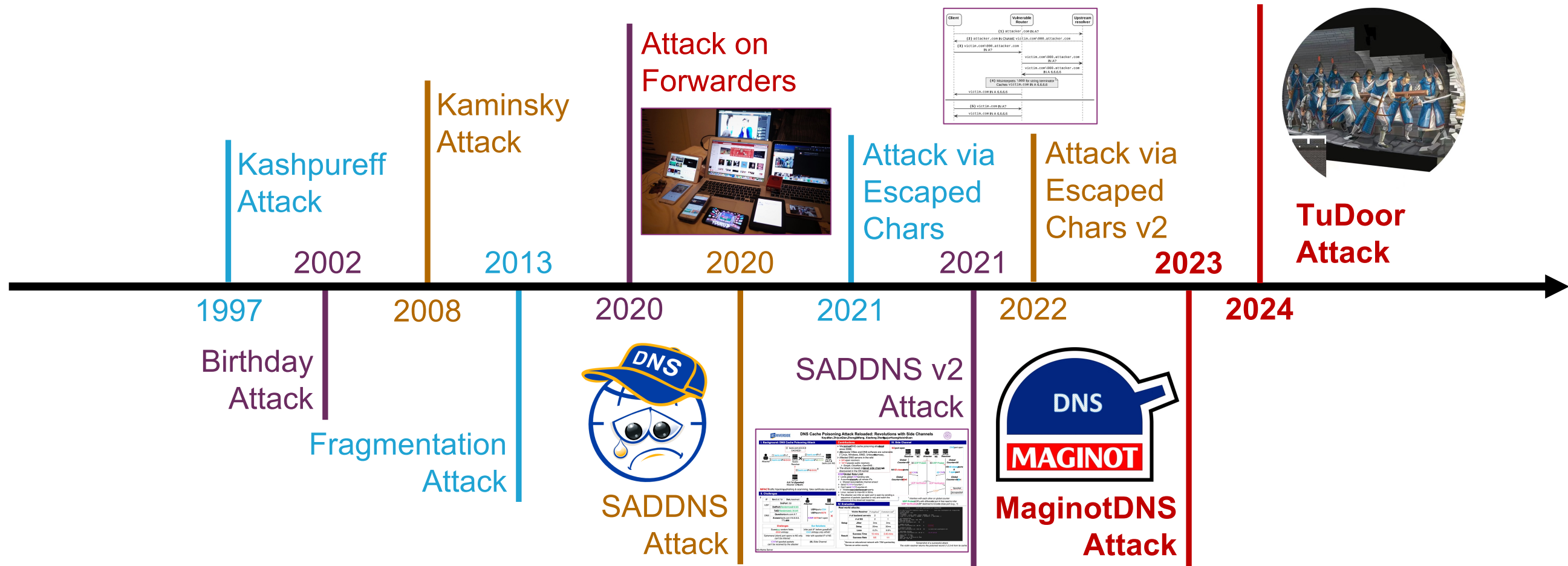
- ❑ Vulnerabilities, protocol flaws, and side channels.

➤ Defenses

- ❑ TXID randomization, birthday protection, and DNSSEC

REBIRTHDAY

The Evolution of DNS Cache Poisoning



Question

Are all old threats truly gone?

Motivation

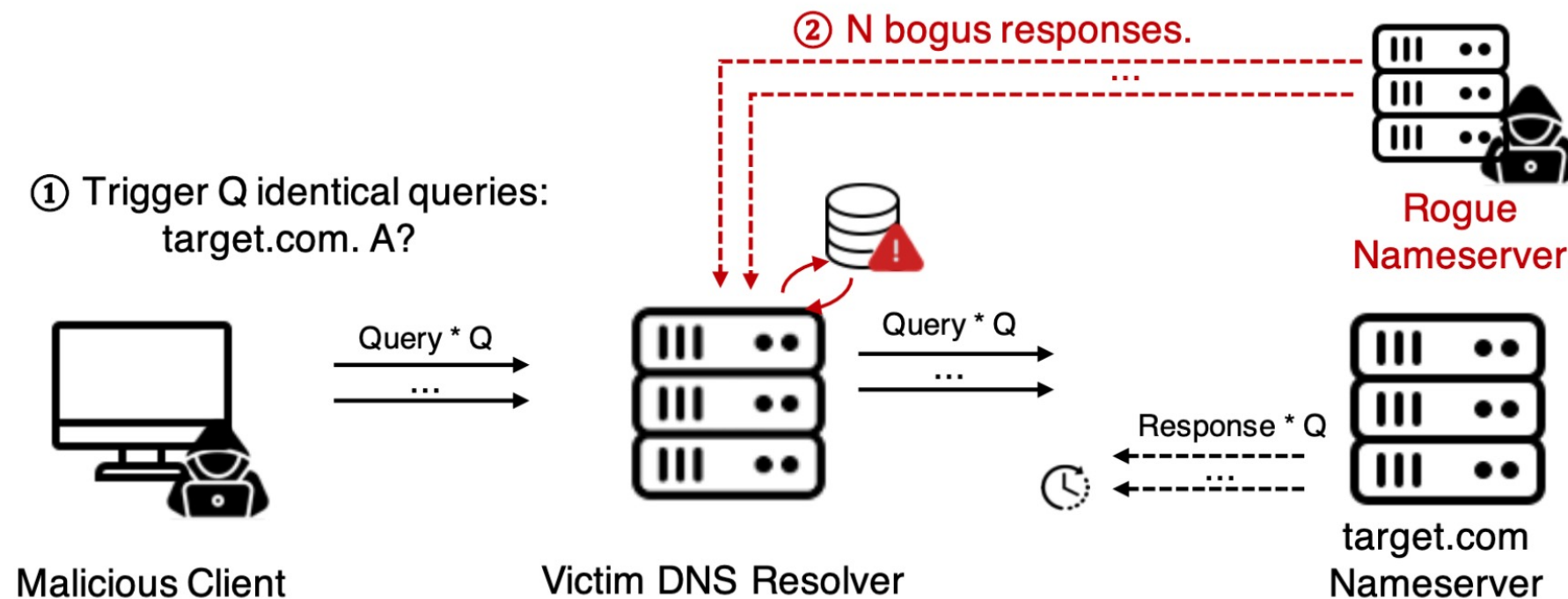
It is necessary to systematically re-examine the long-term effectiveness of the attack vector in the context of the modern DNS protocol

What we did in this paper. And we found,

DNS Birthday Attack

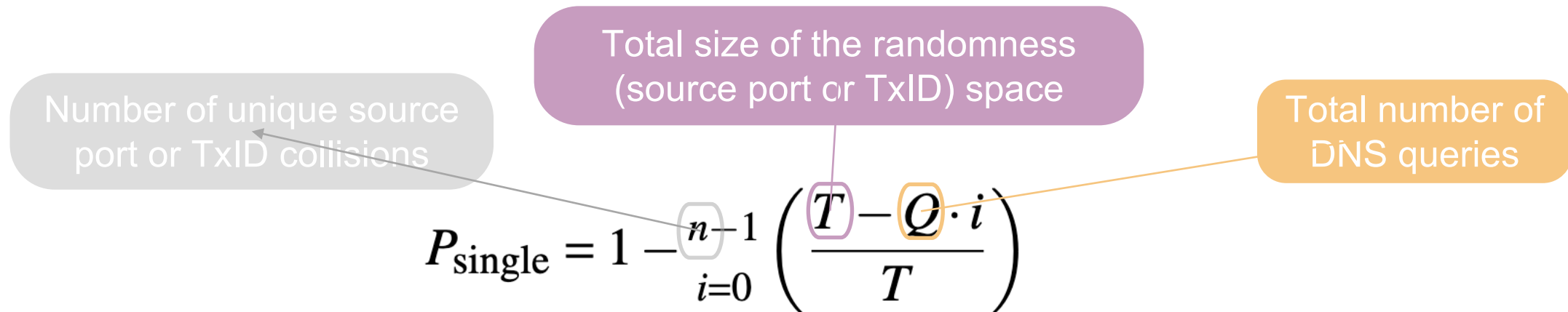
➤ The Classic DNS Birthday Attack (2002)

- ❑ **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



Takeaway

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



Number of unique source port or TxID collisions

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

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:

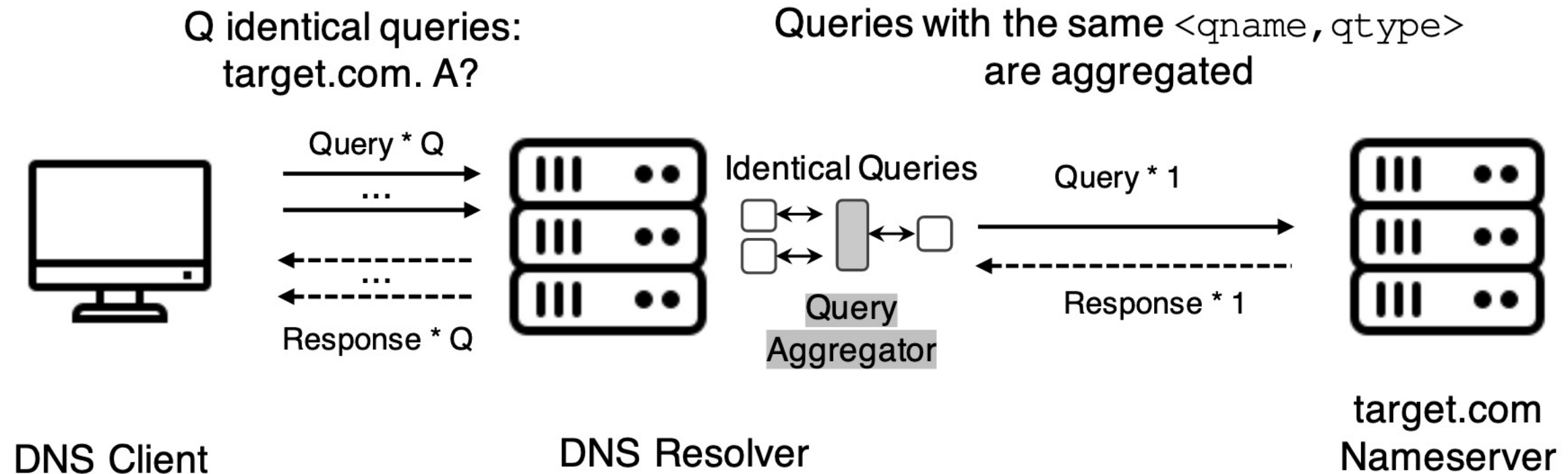
$$P_{\text{success}} = 1 - (1 - P_{\text{single}})^r$$

REBIRTHDAY

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>**

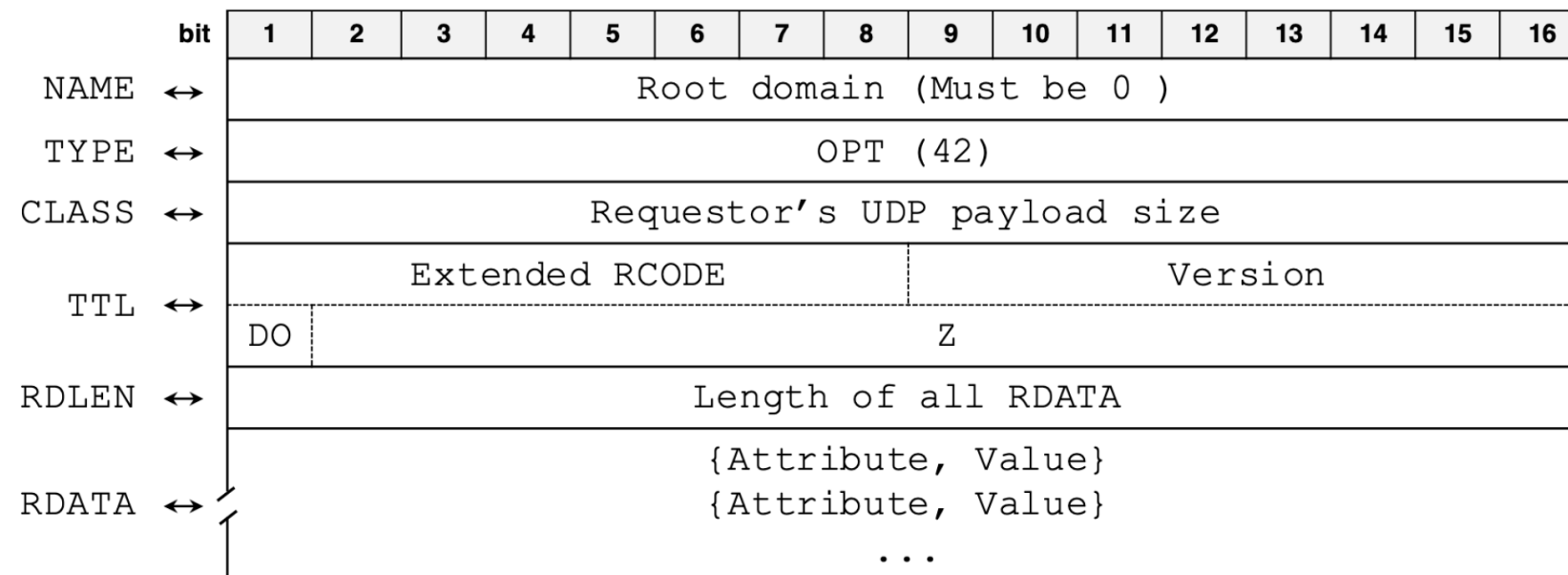


REBIRTHDAY

New Attack Surface

➤ DNS Extensions EDNS(0)

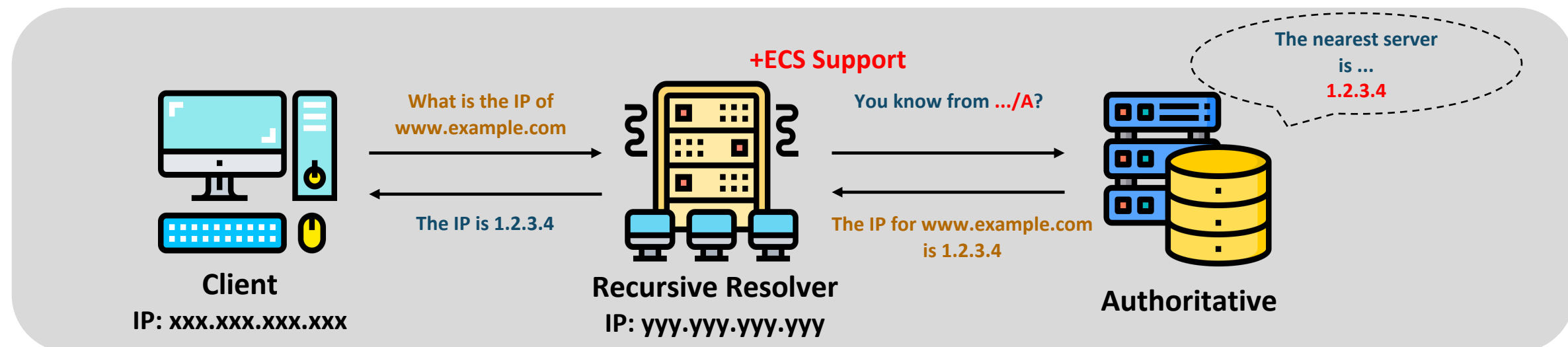
- ❑ **Purpose:** Extension Mechanisms for DNS (RFC 6891) was introduced to overcome the original 512-byte DNS message size limit
- ❑ **Mechanism:** It adds an OPT pseudo-record to the additional section of a DNS message, allowing for new flags and data
- ❑ **Importance:** Foundation for almost all modern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



New Attack Surface

➤ 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

➤ ECS Processing: The Caching Decision

- ❑ **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: $\langle \text{qname}, \text{qtype}, \text{subnet} \rangle$

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

Spoofered response packets can be simple DNS responses, relying only on **matching the <qname, qtype> tuple**
This dramatically **lowers the complexity of the attack**

REBIRTHDAY

Vulnerable DNS Software

➤ 18/22 Software

❑ Vulnerable to a revived Birthday Attack

Resolver		ECS		No Query Aggregation		Vulnerable
Actor	Software	Reply	Request	Without ECS	With ECS	
Recur- sive	BIND	✓	✓	X	✓	✓
	Unbound	✓	✓	X	✓	✓
	PowerDNS Recursor	✓	✓	X	✓	✓
	Knot Resolver	X	X	X	X	X
	Microsoft DNS	X	X	X	X	X
	Technitium DNS	✓	✓	X	✓	✓
	Simple DNS Plus	X	X	X	X	X
	MaraDNS	X	X	X	X	X
	HickoryDNS	X	X	✓	✓	✓

REBIRTHDAY

Vulnerable DNS Software

➤ 18/22 Software

❑ Vulnerable to a revived Birthday Attack

Resolver		ECS		No Query Aggregation		Vulnerable
Actor	Software	Reply	Request	Without ECS	With ECS	
Forw- sarder	Dnsmasq	✓	✓	X	✓	✓
	CoreDNS	X	X	✓	✓	✓
	DNSSDist	✓	✓	✓	✓	✓
	SmartDNS	✓	✓	X	X	✓
	Pi-hole	✓	✓	X	✓	✓
	pdnsd	✓	X	✓	✓	✓
	Acrylic DNS	✓	✓	✓	✓	✓
	AdGuard	✓	✓	✓	✓	✓
	AdGuard Home	✓	✓	✓	✓	✓
	DNS Safety	✓	✓	✓	✓	✓
	Dual DHCPDNS	✓	✓	✓	✓	✓
	NxFilter	X	✓	✓	✓	✓
	YogaDNS	✓	✓	✓	✓	✓

REBIRTHDAY

Attack Overview of REBIRTHDAY

➤ Attacker

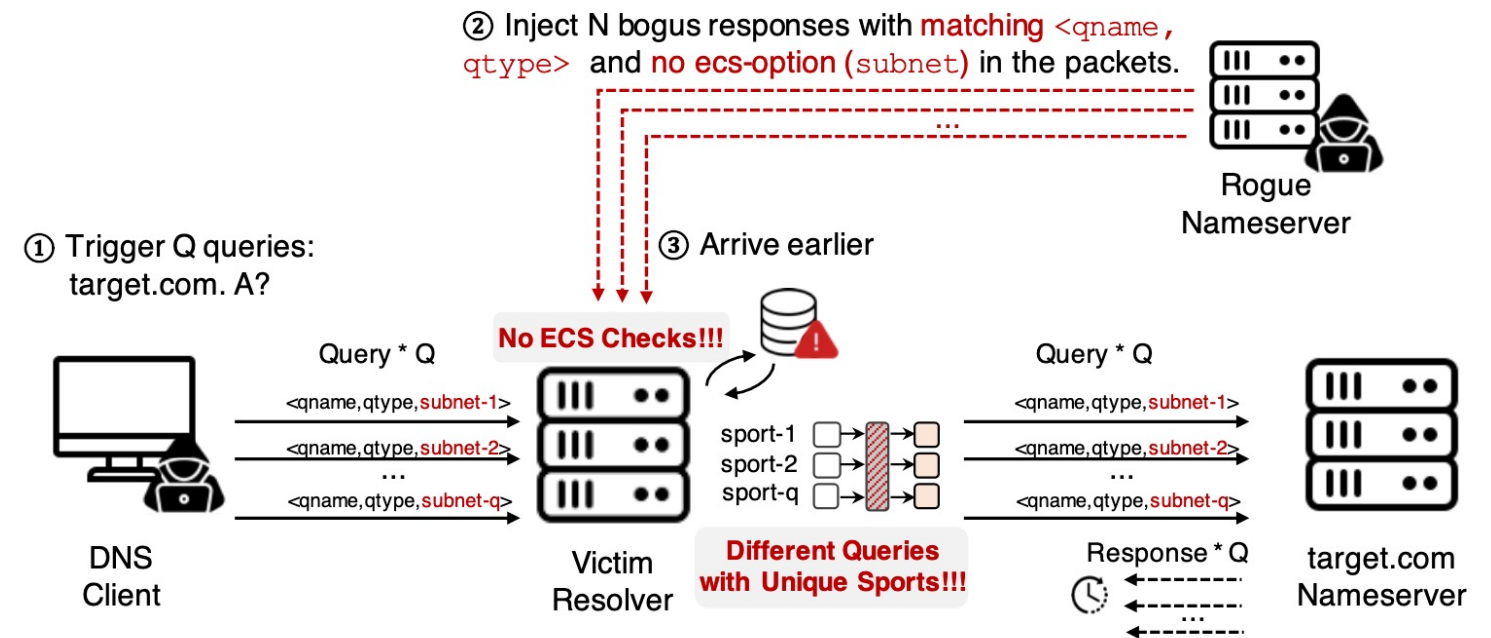
- ❑ An off-path DNS client

➤ 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



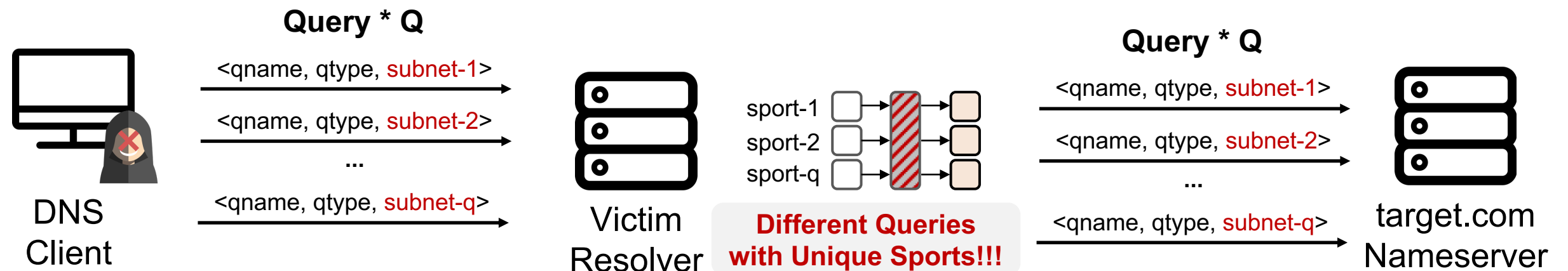
REBIRTHDAY

Attack Steps

➤ Step 1: Triggering Multiple Queries

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

① Trigger Q queries
target.com A?



REBIRTHDAY

Attack Steps

➤ Step 2: Injecting Malicious Responses

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

② Inject N bogus responses with **matching <qname,qtype>** and **no ecs-option (subnet)** in the packets.

① Trigger Q queries
target.com A?



DNS
Client

Query * Q

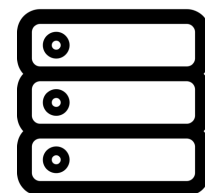
<qname, qtype, subnet-1>

<qname, qtype, subnet-2>

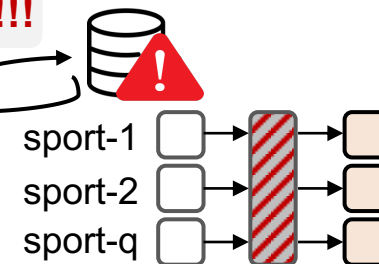
...

<qname, qtype, subnet-q>

No ECS Checks!!!

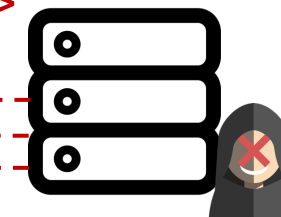


Victim
Resolver



Different Queries
with Unique Sports!!!

③ Arrive earlier



Rogue
Nameserver

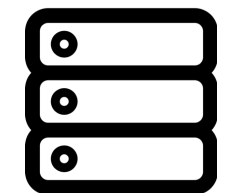
Query * Q

<qname, qtype, subnet-1>

<qname, qtype, subnet-2>

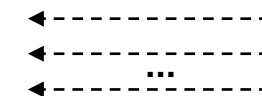
...

<qname, qtype, subnet-q>



target.com
Nameserver

Response * Q



Success Probability & Resource Requirements

➤ Scenario

- ❑ Assume **Q=200** queries per round

➤ Probability

- ❑ The success probability after 1,800 rounds of attack is approximately 99.6%

➤ Bandwidth

- ❑ The maximum bandwidth required to inject 65,536 packets (one full TXID scan) is about **119 Mbps**, which is well within the capabilities of a modern attacker

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

Vulnerable Wi-Fi Routers and OSes

➤ 16/27

- ❑ 12 routers (from vendors like ASUS, CISCO, TP-Link) did not perform query aggregation.
- ❑ Others (from vendors like Fiberhome, Netgear) were vulnerable due to predictable randomization.

Vendor	Version	No Q. Agg.	Vul.
ASUS RT-AC66U	384.18	✓	✓
CISCO Router	1.2.1.7	✓	✓
D-Link 7001	17.01.11A1	✓	✓
Fast FAC1200R	1.0.0	✓	✓
Fiberhome SR4201SA	RP0100	X	✓
Linksys	2.0.4.215745	✓	✓
Mercury D191G	2.0.2	✓	✓
Netgear AX5	1.0.8.82_1	X	✓
Redmi AX3000	1.0.68	✓	✓
Skyworth WR9651X	1.1.0	✓	✓
TendaV1	16.03.29.50	✓	✓
TP-Link XDR3230	1.0.22	✓	✓
TP-Link XDR5430	1.0.14	✓	✓
ZTE E2633	1.0.4	✓	✓
iKuai OS	3.7.17	X	✓
RouterOS	7.16.2	X	✓

REBIRTHDAY

Vulnerable Public DNS Services

➤ 14/45 Public DNS Services




REBIRTHDAY

Vulnerable Open Resolvers

➤ Real-World Impact

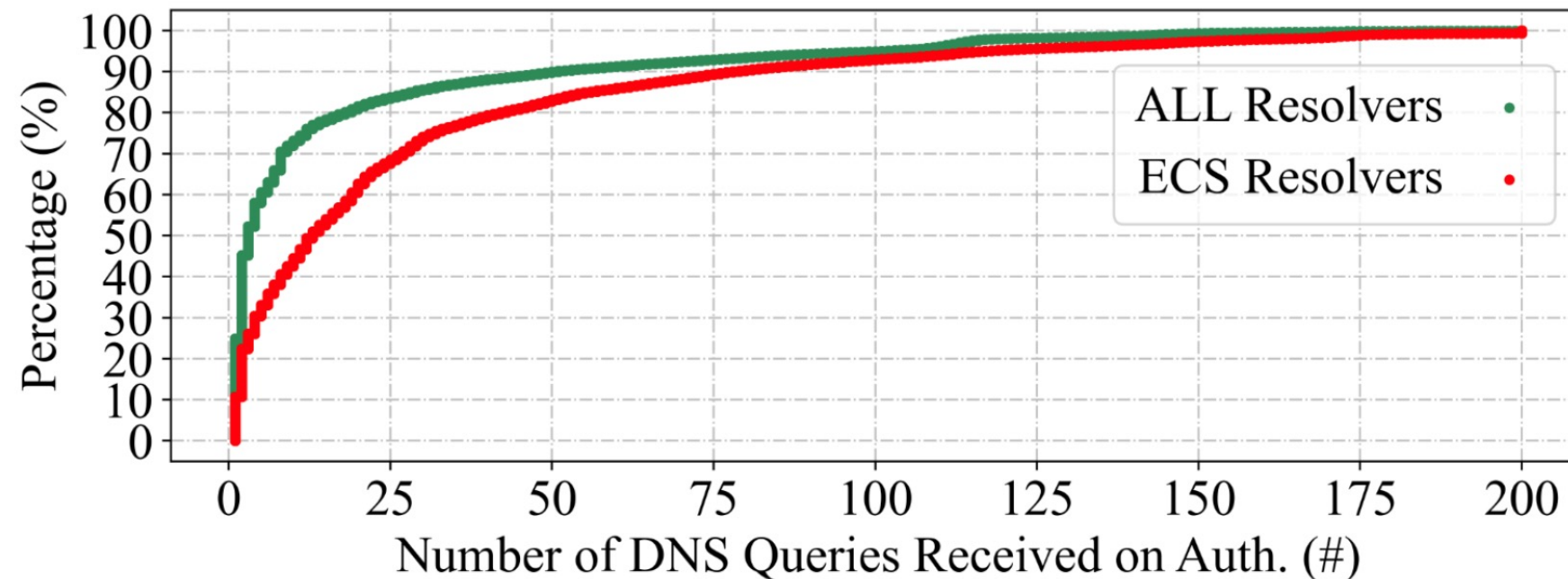
❑ Using XMap (Open-sourced tool)

❑ **365k (15%) out of 2.4M vulnerable (made 25 or more queries)**

 **xmap** Public

XMap is a fast network scanner designed for performing Internet-wide IPv6 & IPv4 network research scanning.

● C ☆ 316 🗑️ 47



REBIRTHDAY

Core Contributions

- **Provided a comprehensive survey of DNS cache poisoning and identified new vulnerabilities**
- **Proposed the REBIRTHDAY threat model, which revives the classic DNS Birthday Attack**
- **Uncovered vulnerabilities in DNS extension implementations across 18 DNS software**
- **Demonstrated prevalent real-world threats, affecting 16 router vendors, 14 public DNS services, and ~365K open resolvers**
- **Introduced protocol-level mitigations and conducted responsible disclosure**

Discussion & Mitigation

➤ Vulnerability Disclosure

- ❑ Acknowledged by 7 vendors, including Unbound and Quad9
- ❑ **35 CVE-ids** assigned

➤ Root Cause

- ❑ Permissive validation in RFC 7871
- ❑ Inconsistent implementation of query aggregation in the presence of DNS extensions

➤ Mitigation Solution

- ❑ Resolvers must enforce strict ECS consistency.
- ❑ Authoritative servers that don't support ECS should be marked, and all subsequent queries (with any ECS) to them should be aggregated.

Wrap-up

Thanks for listening!
Any question?

Xiang Li

Associate Professor, Nankai University

lixiang@nankai.edu.cn

