Summarizing DNS & Security Academic Papers Published in 2024

Chaoyi Lu

March 2025

https://chaoyi.lu

About me

Postdoctoral researcher

Research interests: *Internet measurement, network security*

SSAC member @ ICANN

Research & publication records

Full publication list at: https://chaoyi.lu/publications.html

DNS Protocol & operations measurement	Encrypted DNS, DNS root, Protective DNS, IDN
Large-scale DNS data analysis	WHOIS & privacy, traffic manipulation, DNS zones
New DNS security threats	Denial-of-service (DoS), DNS cache poisoning
Other infrastructure	Web PKI, Email, Mobile

Collecting papers

Academic conferences surveyed: 12

Security, tier-1

IEEE Symposium on Security and Privacy ***(IEEE S&P)***

NDSS

Network and Distributed System Security Symposium ***(NDSS)***

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

USENIX *Security Symposium*

acm SIGSAC

ACM Conference on Computer and Communications Security ***(CCS)***

Security, tier-2

Annual Computer Security Applications Conference ***(ACSAC)***

RAID

International Symposium on Research in Attacks, Intrusions and Defenses ***(RAID)***

IEEE/IFIP International Conference on Dependable Systems and Networks ***(DSN)***

ESORICS

European Symposium on Research in Computer Security ***(ESORICS)***

Networks, tier-1

ACM ***SIGCOMM***

ACM Internet Measurement Conference ***(IMC)***

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

USENIX Symposium on Networked Systems Design and Implementation ***(NSDI)***

THE WEB CONFERENCE ACM

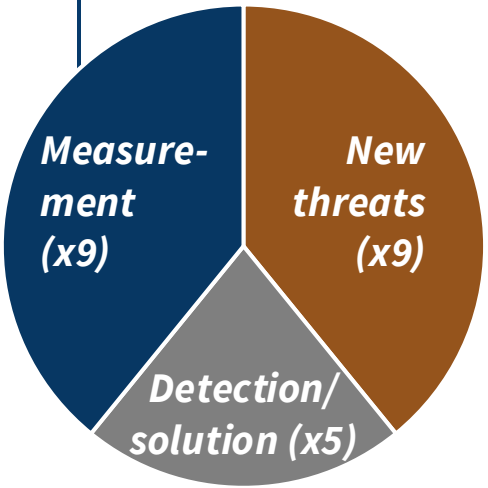
The Web Conference ***(WWW)***

Having fun with numbers

23 papers about DNS/Security

23 papers about DNS/Security

Measurement of DNS servicing and security (x9)



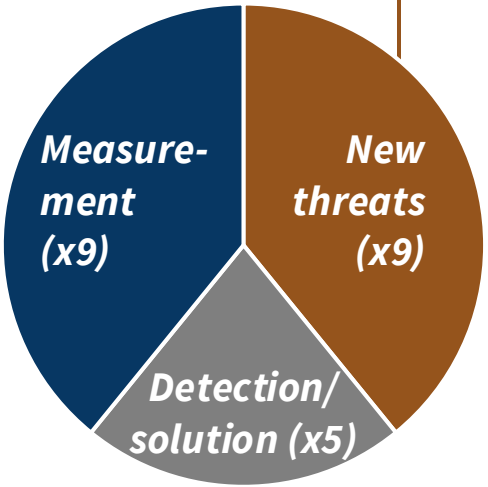
Of DNS servicing / DNS data (x6)

- [IMC] Zeros Are Heroes: **NSEC3** Parameter Settings In The Wild
- [IMC] Exploring the Ecosystem of DNS **HTTPS Resource Records**: An End-to-End Perspective
- [IMC] The **Roots** Go Deep: Measuring '.' Under Change
- [NDSS] Understanding the Implementation and Security Implications of **Protective DNS** Services
- [WWW] A Worldwide View on the Reachability of **Encrypted DNS** Services
- [ESORICS] From Fingerprint to Footprint: Characterizing the Dependencies in **Encrypted DNS** Infrastructures

Of DNS security (x3)

- [IMC] DarkDNS: Revisiting the Value of **Rapid Zone Update**
- [IMC] Yesterday Once More: Global Measurement of Internet **Traffic Shadowing** Behaviors
- [WWW] Discovering and Measuring CDNs Prone to **Domain Fronting**

23 papers about DNS/Security



New DNS security threats / attack vectors (x9)

DoS leveraging / targeting DNS (x4)

- [CCS] The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on **DNSSEC**
- [S&P] DNSBomb: A New Practical-and-Powerful **Pulsing** DoS Attack Exploiting DNS Queries-and-Responses
- [USENIX] Loopy Hell(ow): Infinite **Traffic Loops** at the Application Layer
- [USENIX] CAMP: Compositional **Amplification Attacks** against DNS

Caching (x2)

- [S&P] TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with **Malformed Packets**
- [USENIX] A **Flushing** Attack on the DNS Cache

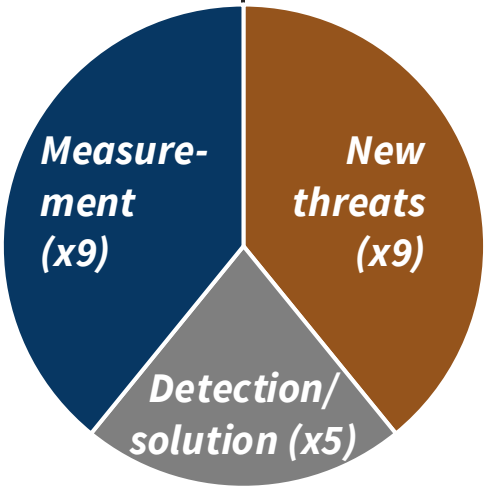
Delegation and infrastructure (x2)

- [USENIX] Rethinking the Security Threats of Stale DNS **Glue Records**
- [USENIX] Cross the Zone: Toward a Covert Domain Hijacking via **Shared DNS Infrastructure**

Others (x1)

- [S&P] Practical Attacks against **DNS Reputation Systems**

23 papers about DNS/Security



DNS detection and solution (x5)

- [SIGCOMM] Topaz: Declarative and Verifiable **Authoritative DNS** at CDN-Scale
- [NDSS] Information Based Heavy Hitters for Real-Time DNS **Data Exfiltration Detection**
- [DSN] Sensitive information **leakage prevention in DNSSEC Zone-Walking** - A Practical Solution
- [RAID] Blocklist-Forecast: Proactive **Domain Blocklisting** by Identifying Malicious Hosting Infrastructure
- [RAID] Down to earth! Guidelines for **DGA-based Malware Detection**

Before digging in...

Measurement:
Obtaining data about the DNS

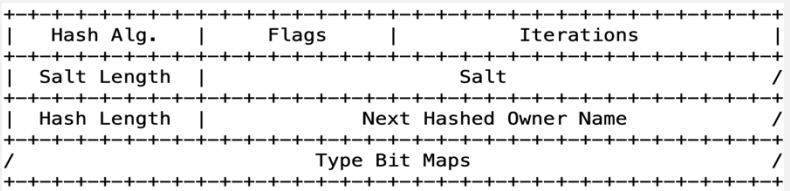
Getting data about DNS operation

[IMC] Zeros Are Heroes: NSEC3 Parameter Settings In The Wild

Authors: Cordian Daniluk, Yevheniya Nosyk, Andrzej Duda, Maciej Korczynski

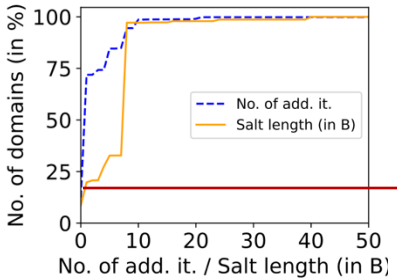
RFC 9276: Guidance for NSEC3 Parameter Settings

- Number of additional iterations MUST be set to 0 ***(zero!)***
- SHOULD NOT use a salt
- Recommendations to zones & validating resolvers



Domains

- 15.5M of 302M registered domains enables NSEC3
- **87.8% of them do not comply with RFC 9276**

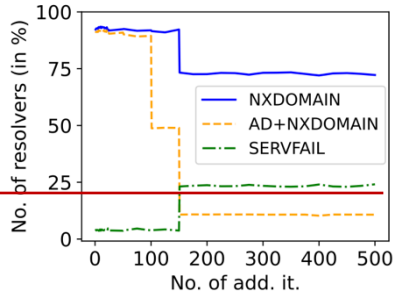


Only 12.2% NSEC3-enabled domains have 0 additional iterations

Validating resolvers

- 78.3% of resolvers limit # of iterations processed
- 18.4 do not accept any additional iterations

Chance of getting SERVFAIL rises when using more rounds of additional iterations



Getting data about DNS operation

[IMC] Exploring the Ecosystem of DNS HTTPS Resource Records: An End-to-End Perspective

Authors: Hongying Dong, Yizhe Zhang, Hyeonmin Lee, Shumon Huque, Yixin Sun

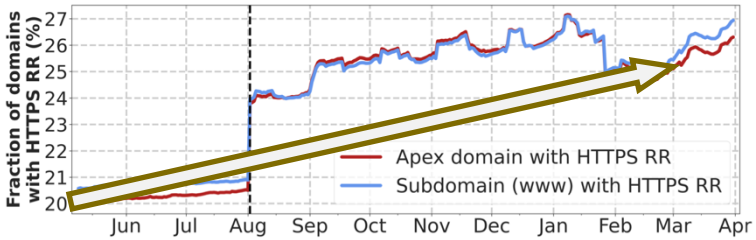
HTTPS Resource Record (RFC 9460)

```
@ 7200 IN HTTPS 1 . alpn=h3
```

- Clients replace the scheme with “https” when loading “https://@”
- “https://@” supports QUIC and HTTP/1.1 over TLS.

Server-side deployment (Tranco Top 1M)

- ~25% by the end of 2024, still growing
- **Cloudflare** remains as the major adopter
- Over 90% are **missing DNSSEC**



Client-side (browsers) support

- Proper **failover** mechanisms are in need

		Chrome		Safari	Edge	
OS		macOS	Windows	macOS	macOS	Windows
Browser Version		120.0.6099		17.2.1	120.0.2210	
HTTPS RR Utilization	{apex}	●	●	◐	●	●
	http://{apex}	●	●	◐	●	●
	https://{apex}	●	●	●	●	●
AliasMode	TargetName	○	○	●	○	○
ServiceMode	TargetName	○	○	●	○	○
	port	○	○	●	○	○
	alpn	●	●	●	●	●

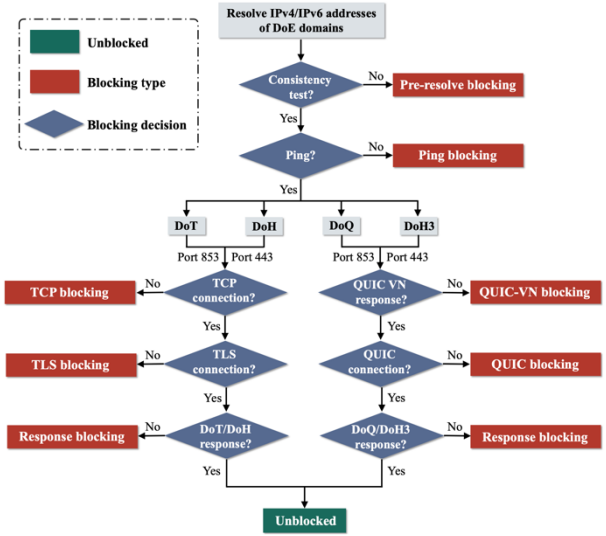
Knowing how emerging services perform

[WWW] A Worldwide View on the Reachability of Encrypted DNS Services

Authors: Ruixuan Li, Baojun Liu, Chaoyi Lu, Haixin Duan, Jun Shao

Encrypted DNS (DoE) protects privacy, but may not be reachable (e.g., is blocked) sometimes

- DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), DNS-over-QUIC (DoQ)



Probe for open DoE resolvers:

- **~1.7k domains** (from TLS certificates) point to DoE services (resolvers using self-signed certs are removed)

Test if encrypted DNS is available from global VPs:

- Most blocking happens at **IP layer** (can't even ping), then at **TCP connection establishment** (e.g., timeout, connection reset)
- DoE queries fail more from Internet-not-free countries
- DoE queries fail more (~30%) from China, except DoQ
- DoE is better reached over **IPv6** than IPv4

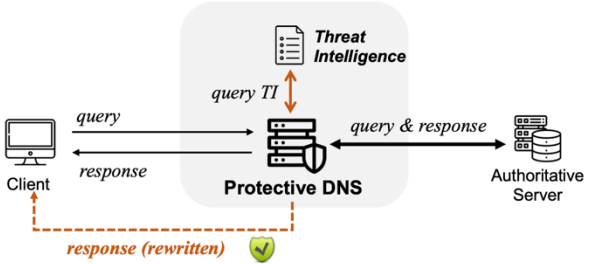
Knowing how emerging services perform

[NDSS] Understanding the Implementation and Security Implications of Protective DNS

Authors: Mingxuan Liu, Yiming Zhang, Xiang Li, Chaoyi Lu, Baojun Liu, Haixin Duan, Xiaofeng Zheng

Protective DNS: resolvers rewrite DNS for active filtering

- Supported by large DNS services: Cloudflare, Quad9, etc.
- National PDNS initiatives: EU (DNS4EU), US, Canada

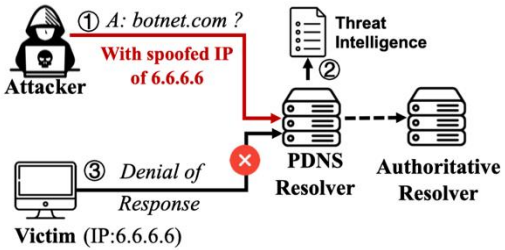


PDNS adoption: ~17k open resolvers are actively filtering malicious domains

Rewriting policies

# Rewriting Policy	# PDNS
Secure IP	9,935 (56.45%)
Special-use IP	7,209 (40.96%)
No Data	822 (4.67%)
Secure CNAME	449 (2.55%)
Error Response Code	408 (2.32%)

Find implementation flaws that allow:



- **Denial of response:** attacker query blocked domains with spoofed IP of victim, causing resolver to refuse serving victim's queries
- **Domain takeover:** resolver use dangling IPs that are available to public

Measuring impact of security problems

[IMC] DarkDNS: Revisiting the Value of Rapid Zone Update

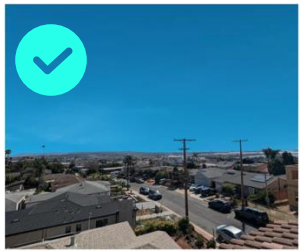
Authors: Raffaele Sommese, Gautam Akiwate, Antonia Affinito, Moritz Muller, Mattijs Jonker, KC Claffy

TLD zone snapshots (e.g., CZDS) offer visibility into registered domains at some point every day

- Is it enough? Will it miss detection opportunities?

Day 1
Snapshot 1 at 6 p.m.

Day 1
Event at 8 p.m.
Missed it from snapshots!



Day 2
Snapshot 2 at 6 p.m.

Find newly-registered domains from CT logs:

- ~76k domains per day
- 42% can be detected before they appear in CZDS
- **1% never appear in the next snapshot *(invisible!)***

Why do this happen, and what domains are these?

- These domains do not last for over 24 hours
- Early removal by registrars under **abuse**
- **So we *are* missing early detection opportunities**

Where next?

- Call to resurrect **Rapid Zone Updates**: finer-grained visibility of changes to zone files

Measuring impact of security problems

[IMC] Yesterday Once More: Global Measurement of Internet Traffic Shadowing Behaviors

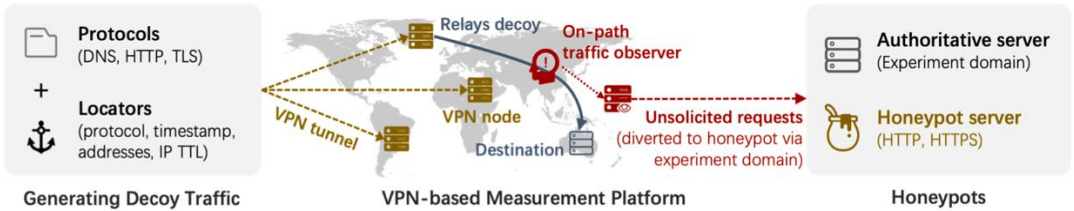
Authors: Yunpeng Xing, Chaoyi Lu, Baojun Liu, Haixin Duan, Junzhe Sun, Zhou Li

"Traffic shadowing": past queries are recorded on-path and come again when original client is no longer waiting for response

- APNIC pilot study: 1/4 of DNS queries from experiments are unexpectedly captured again, **hours or days later**

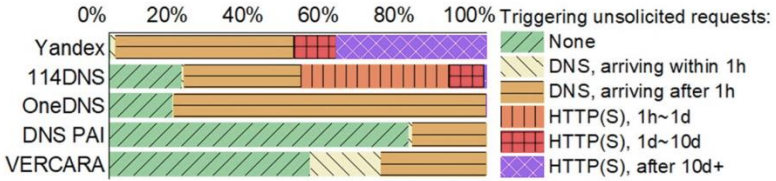
Send "decoys" to lure observers

- Bear query names that were never used or ever used again
- Capture **unsolicited requests** ***(yesterday once more!)***



DNS queries can be observed and recorded

- When the destination is public DNS resolvers
- Can trigger unsolicited requests over **other protocols** (e.g., HTTP/S, meaning additional probes to the website)



DNS threats:
New attack vectors & methods

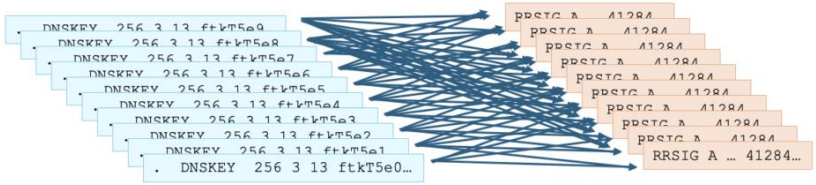
Let's try bringing DNS servers down

[CCS] The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC

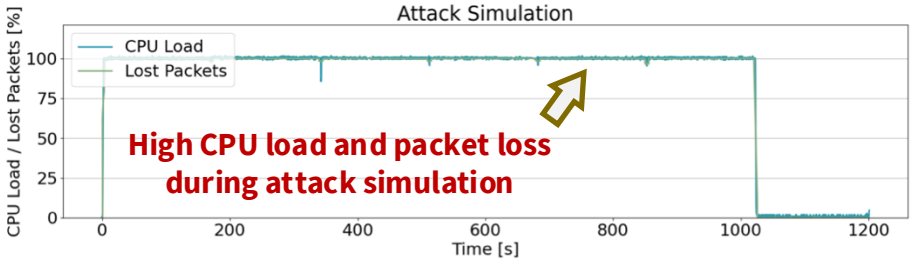
Authors: Elias Heftrig, Haya Schulmann, Niklas Vogel, Michael Waidner

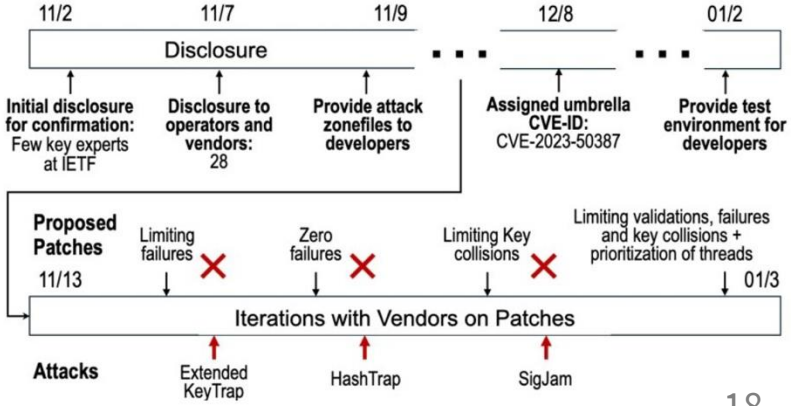
DNSSEC validation under multiple keys and signatures

- Specifications recommend trying them all ➔ potentially costs lots of computing resources



Attackers setup such domains, trying to cost resolvers lots of resources during validation



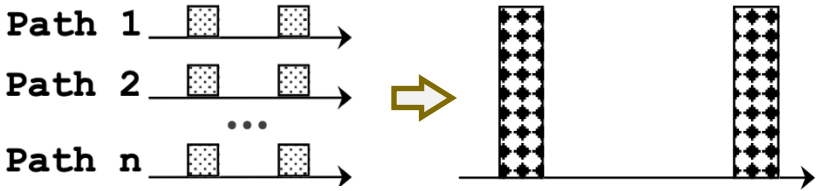


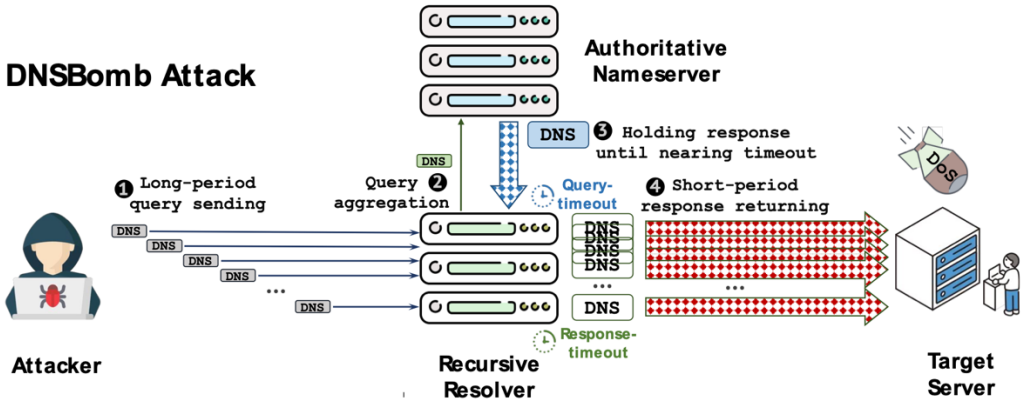
Let's try bringing DNS servers down

[S&P] DNSBomb: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses

Authors: Xiang Li, Dashuai Wu, Haixin Duan, Qi Li

Pulsing attacks:
low rate, high peaks, hard to detect by IDS





Using resolvers to make pulses:

- **Gather** queries with timeouts
- **Amplify** response size
- **Fast-direct** responses to victim

Simulation results:

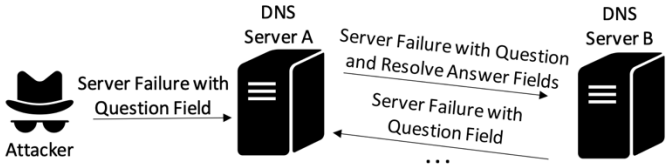
- Up to **20,000x** amplification factor
- Causing packet loss to normal queries

Let's try bringing DNS servers down

[USENIX] Loopy Hell(ow): Infinite Traffic Loops at the Application Layer

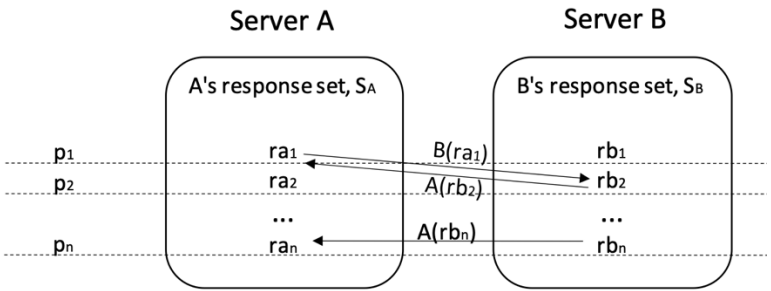
Authors: Yepeng Pan, Anna Ascheman, Christian Rossow

Creating traffic loops between (DNS and beyond) servers to exhaust their resources



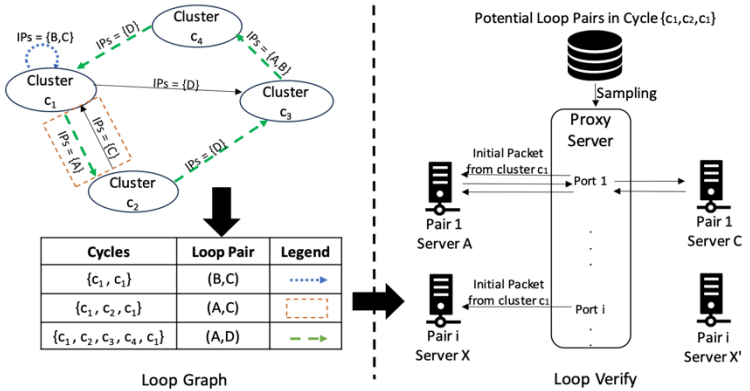
Build "response functions" for each server

- For server **A**, the response to query q is denoted **A**(q)
- **Find loops:** e.g., if **B**(**A**(q))=q, this creates a simple loop between **A** and **B**



Loop graphs and loop verify

- Find **140k DNS servers** that can be involved in a loop

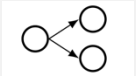


Let's try bringing DNS servers down

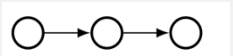
[USENIX] CAMP: Compositional Amplification Attacks against DNS

Authors: Huayi Duan, Marco Bearzi, Jodok Vieli, David Basin, Adrian Perrig, and Si Liu

Taxonomy of DNS amplification (primitives)



Fan-out



Chaining

Self-probing

Compositional amplification vulnerabilities

- Combine **multiple primitives** to produce multiplicative amplification effects

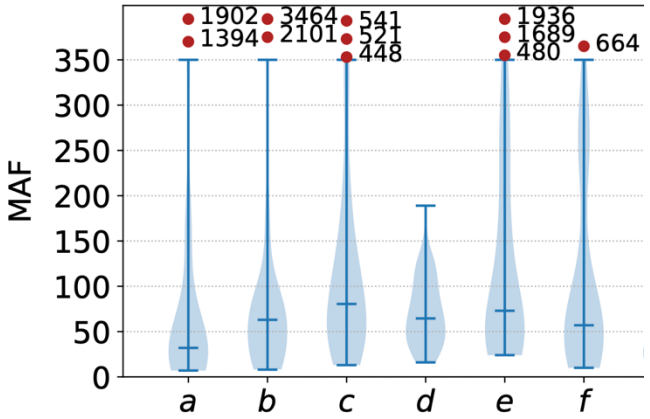
1 query for q.a fans out into 3 to nx.a

then chain to domain b

Fan-out x chaining

>zone a.com@1.2.3.4			>zone b.com@1.2.3.4		
q.a	NS	n1.a	-v1		
q.a	NS	n2.a	n11.b	NS	n12.b
q.a	NS	n3.a	n12.b	NS	n13.b
-v1: secd. referral			n21.b	NS	n22.b
n1.a	NS	n11.b	n22.b	NS	n23.b
n2.a	NS	n21.b	...		
n3.a	NS	n31.b	-v2		
-v2: secd. rewrite			r11.b	CNAME	r12.b
n1.a	CNAME	r11.b	r12.b	CNAME	r13.b
n2.a	CNAME	r21.b	r21.b	CNAME	r22.b
n3.a	CNAME	r31.b	...		

Evaluation on DNS software & public resolvers



Produces hundreds to thousands times of traffic amplification

Meddling with DNS cache

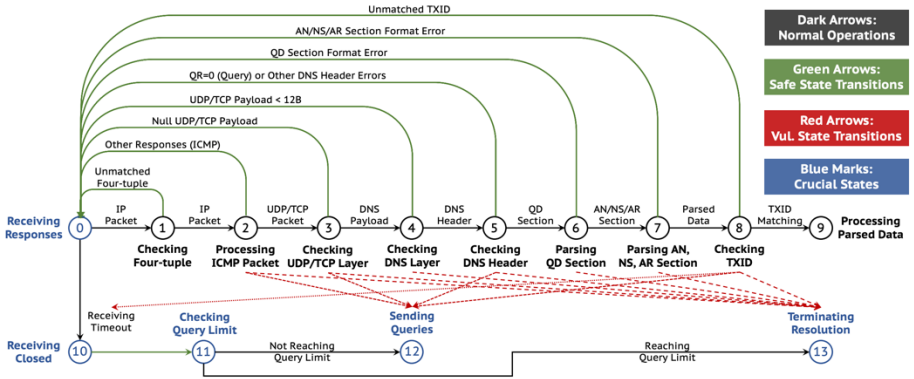
[S&P] TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets

Authors: Xiang Li, Wei Xu, Baojun Liu, Mingming Zhang, Zhou Li, Jia Zhang, et al.

DNS cache poisoning: inserting false data into resolver cache, thus hijacking domains

- Long history: bailiwick circumvention (’97), metadata guessing (’08), fragmentation (’20), side channels (’20), …

Vulnerabilities in DNS response processing opens a “side door”



Find vulnerabilities from state transitions of DNS software

E.g., Microsoft DNS

- Opens side channel where attacker can probe to discover source port, leaving only TXID to guess
- **Can inject false data in <0.5s**

Delegation & TLD management

[USENIX] Rethinking the Security Threats of Stale DNS Glue Records

Authors: Yunyi Zhang, Baojun Liu, Haixin Duan, Min Zhang, Xiang Li, Fan Shi, Chengxi Xu

"Stale" glue records in TLD zone files

- Providing IP addresses that do not agree with SLD authoritative data
- Server name in glue is not used as authoritative by any domain under this TLD

; .com zone file

example.com	NS	ns.example.com
ns.example.com	A	1.2.3.4 **(Correct)**
stale.com	NS	ns.stale.com
ns.stale.com	A	4.5.6.8 **(Stale)**
ns-old.stale.com	A	8.8.9.9 **(Expired)**

; example.com nameserver

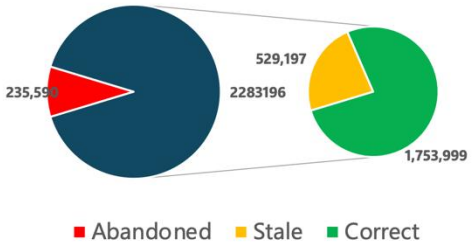
example.com	NS	ns. example.com
ns.example.com	A	1.2.3.4

; stale.com nameserver

ns.stale.com	A	2.3.4.5

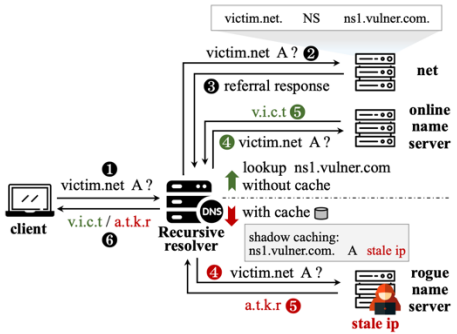
Find stale glue in TLD zones

- Over 1,000 TLDs and 2M+ glue records inspected



23% of all glue records provide stale information

Inappropriate use of glue by DNS software



Trusting and caching stale glue without verification

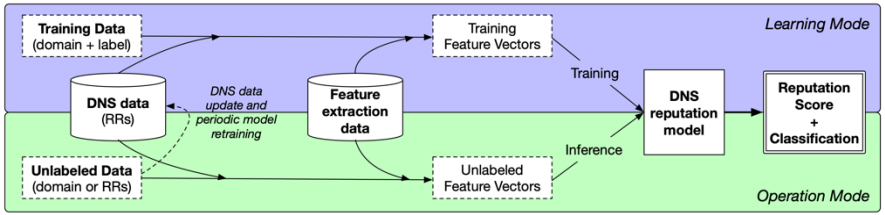
Enables stealthy domain takeover

DNS reputation systems

[S&P] Practical Attacks Against DNS Reputation Systems

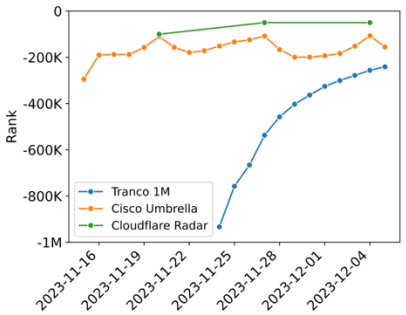
Authors: Tillson Galloway, Kleanthis Karakolios, Zane Ma, Roberto Perdisci, Angelos Keromytis, Manos Antonakakis

DNS reputation systems are "black boxes"; their adversarial robustness is less known.



Popularity list manipulation

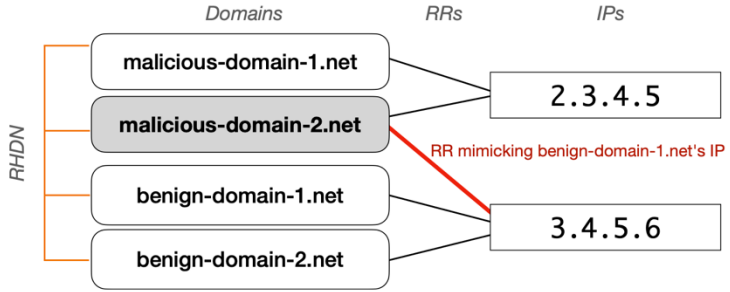
- Attacker can perform **a small number of DNS lookups from many IP addresses** for high rank



Manipulating Cisco and Cloudflare lists with just 12k queries a day, using VPN nodes

Mimicry attacks

- Adversaries create new RRs for malicious domain that **resolve to IP addresses from benign RRs**



Detection & solution

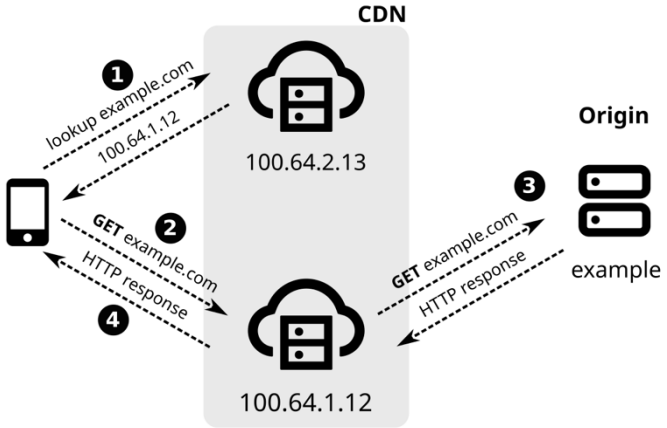
When DNS is used for load balancing

[SIGCOMM] Topaz: Declarative and Verifiable Authoritative DNS at CDN-Scale

Authors: Tillson Galloway, Kleanthis Karakolios, Zane Ma, Roberto Perdisci, Angelos Keromytis, Manos Antonakakis

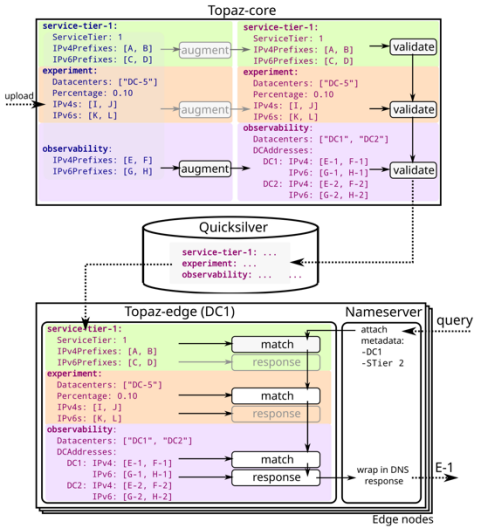
CDN resolver decides which CDN IP a live domain query will map to

- Traditionally: rely on **centralized** assignment systems – ***potentially obfuscates DNS behavior***



New architecture that prevents possible conflicts

- Encode distinct objective as a ***policy***
- Executed directly to ***live DNS queries*** by CDN edge service



Detect possible conflicts before deployment

Handles ~1M DNS queries per second at a global CDN

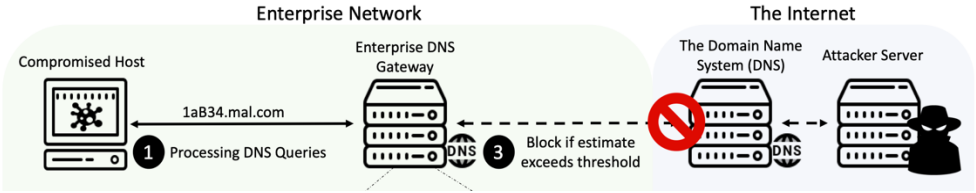
Detecting bad behaviors over DNS

[NDSS] Information-Based Heavy Hitters for Real-Time DNS Data Exfiltration Detection

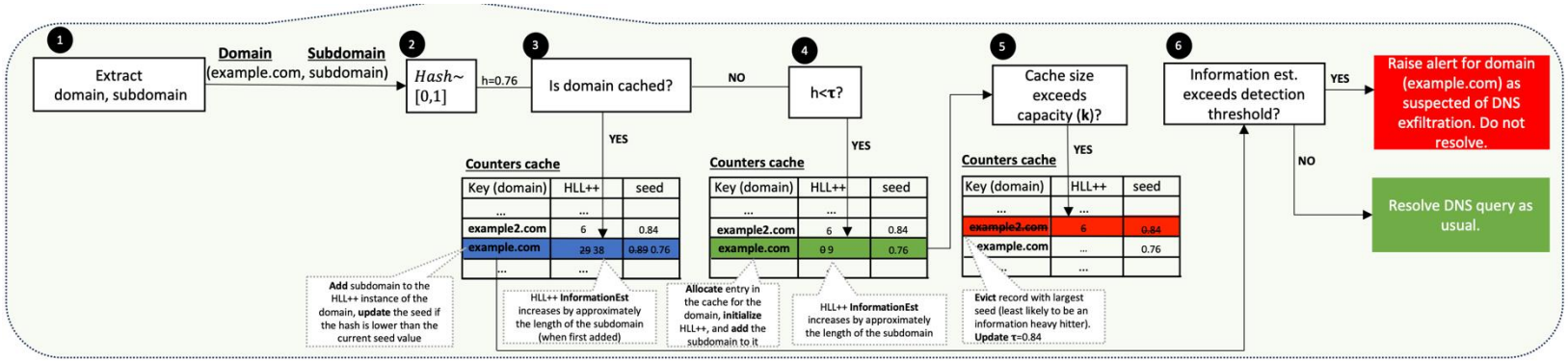
Authors: Yarin Ozery, Asaf Nadler, Asaf Shabtai

Detection of data exfiltration over DNS

- Traditionally focused on **offline detection methods** - allow a large amount of data to be exfiltrated before attack mitigation



Real-time DNS exfiltration detection method



Enhancing blocking efficiency with DNS

[RAID] Blocklist-Forecast: Proactive Domain Blocklisting by Identifying Malicious Hosting Infrastructure

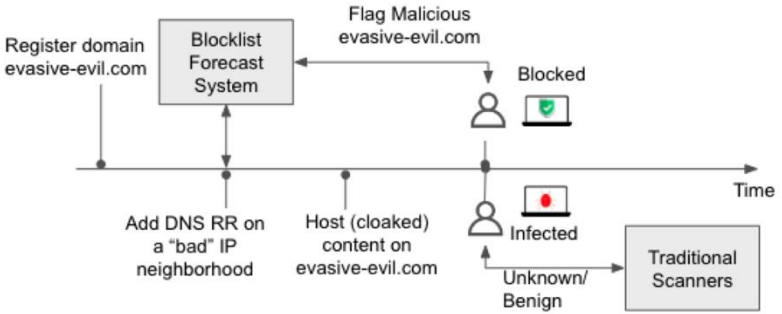
Authors: Udesh Kumarasinghe, Mohamed Nabeel, Charitha Elvitigala

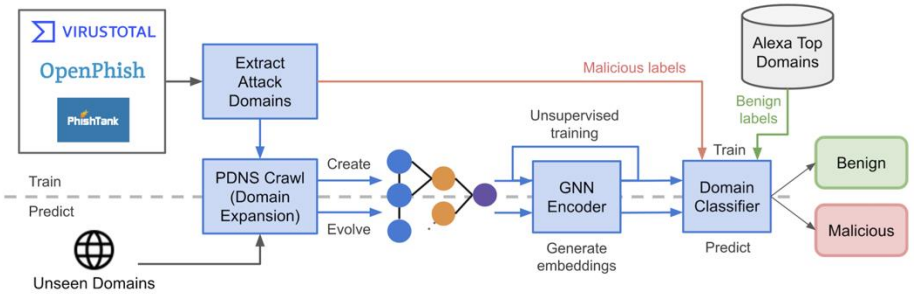
Existing domain blocklists are slow to react to attacks

- They rely on website content or user interactions to ascertain if a website is malicious

Build a "blocklist forecast system"

- To ***proactively predict*** and flag more malicious domains from those already blocked ***("seeds")***
- Crawl passive DNS data to identify domains in the **"neighborhood"** of seed malicious domains from blocklists
- Predict **4.7x** more malicious domains with **94.3%** accuracy





Summarizing DNS & Security Academic Papers Published in 2024

Chaoyi Lu

March 2025

https://chaoyi.lu