OARC 43

DNSBomb: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses

[Published at IEEE S&P 2024]

Speaker: Xiang Li, Associate Professor

Nankai University

Oct. 2024

@NKU

Attack Impact

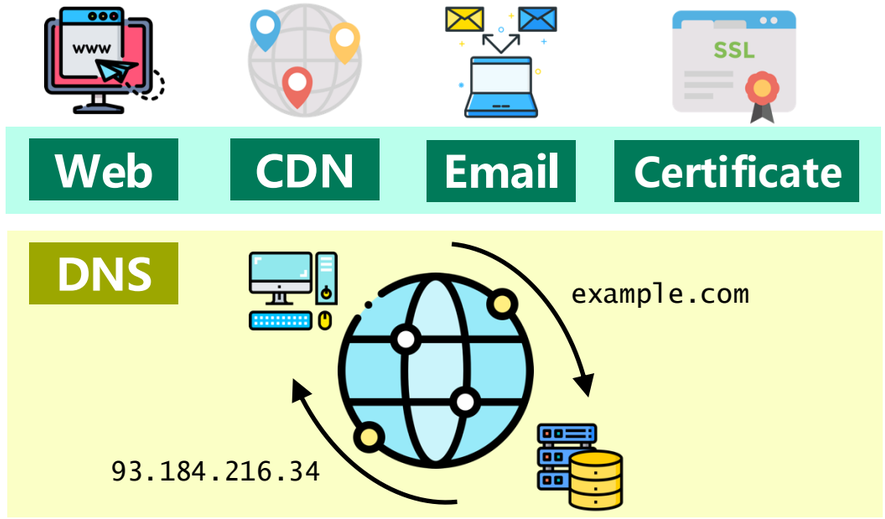
Our DNSBomb attack could be exploited to DoS arbitrary targets with pulsing traffic.

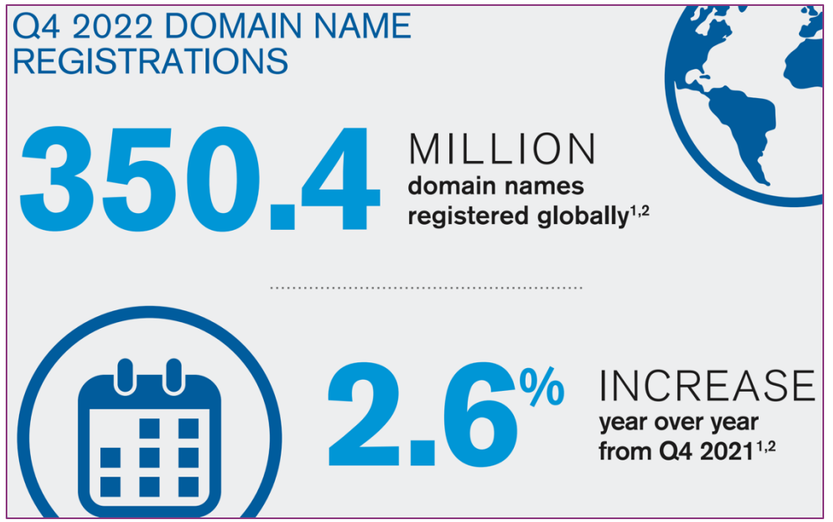
The bandwidth amplification factor could be >20,000x.

Domain Name System (DNS)

➢ DNS Overview

- ❑ Translating domain names to IP addresses
- ❑ Entry point of many Internet activities
- ❑ Domain names are widely registered



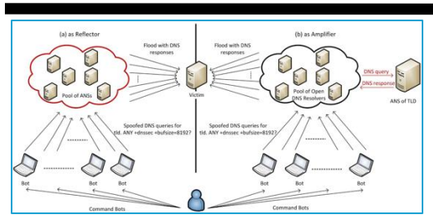


verisign.com/dnib

DNS Amplification Attack

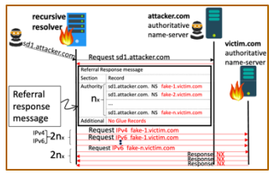
- **Target**
  - To flood a target with amount of DNS traffic
- **Taxonomy**
  - Bandwidth amplification attack
  - Packet amplification attack

2014



DNS reflection amplification attack by ANY/TXT/DNSSEC

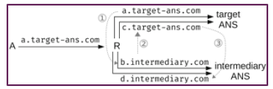
2018



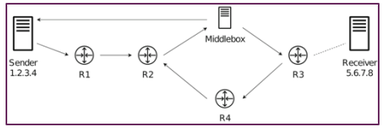
NXNSAttack

2020

DNS Unchained



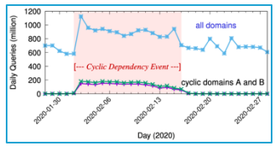
2021



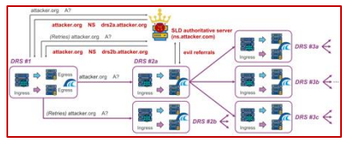
Routing Loops as mega Amplifiers

2022

TsuNAME



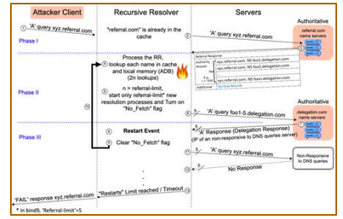
2023



TsuKing

2023

NRDelegationAttack



Takeaway

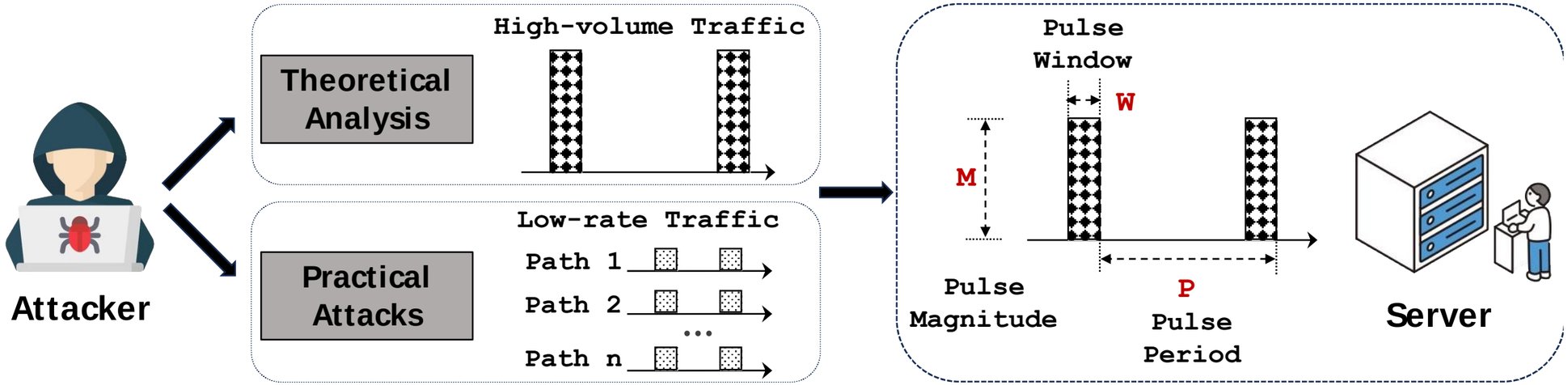
However, the traditional DNS amplification attack could be easily detected by the amount of traffic.

Researchers have proposed new amplification attacks with the **hard-to-detect pulsing DoS traffic**.

Pulsing DoS Attack

➢ Summary of Pulsing DoS Attack

- ❑ Concentrating a low-bandwidth traffic into a high-bandwidth pulsing
- ❑ **Cannot be detected by traditional IDS** (low-rate among a while)
- ❑ Impact is hugely causing pkts loss



Takeaway

However, previous pulsing DoS attacks could only yield a low amplification factor or require a large pulse period. (Not practical and powerful enough)

In this paper, we observe the capacity of DNS resolvers to **concentrate traffic has never been studied in depth**.

DNSBomb Attack

- **What is the DNSBomb attack**
  - Proposed by our **NISL** lab, published at **[IEEE S&P 2024]**
  - **A new practical and powerful DNS-based pulsing DoS attack**
    - Concentrating a low-rate query traffic into a high-rate response pulsing
  - **Exploiting three inherent DNS mechanisms (defense) to DoS (attack)**
    - **timeout**, **query aggregation**, and **response fast-returning**

Dragon Ball Kame Hame Ha (Blast wave)

① Kame (Starting)

② Hame (Gathering energy)

③ Ha (Releasing blast)

DNSBomb Attack

➢ Threat Model

❑ Step 1: Ka-me

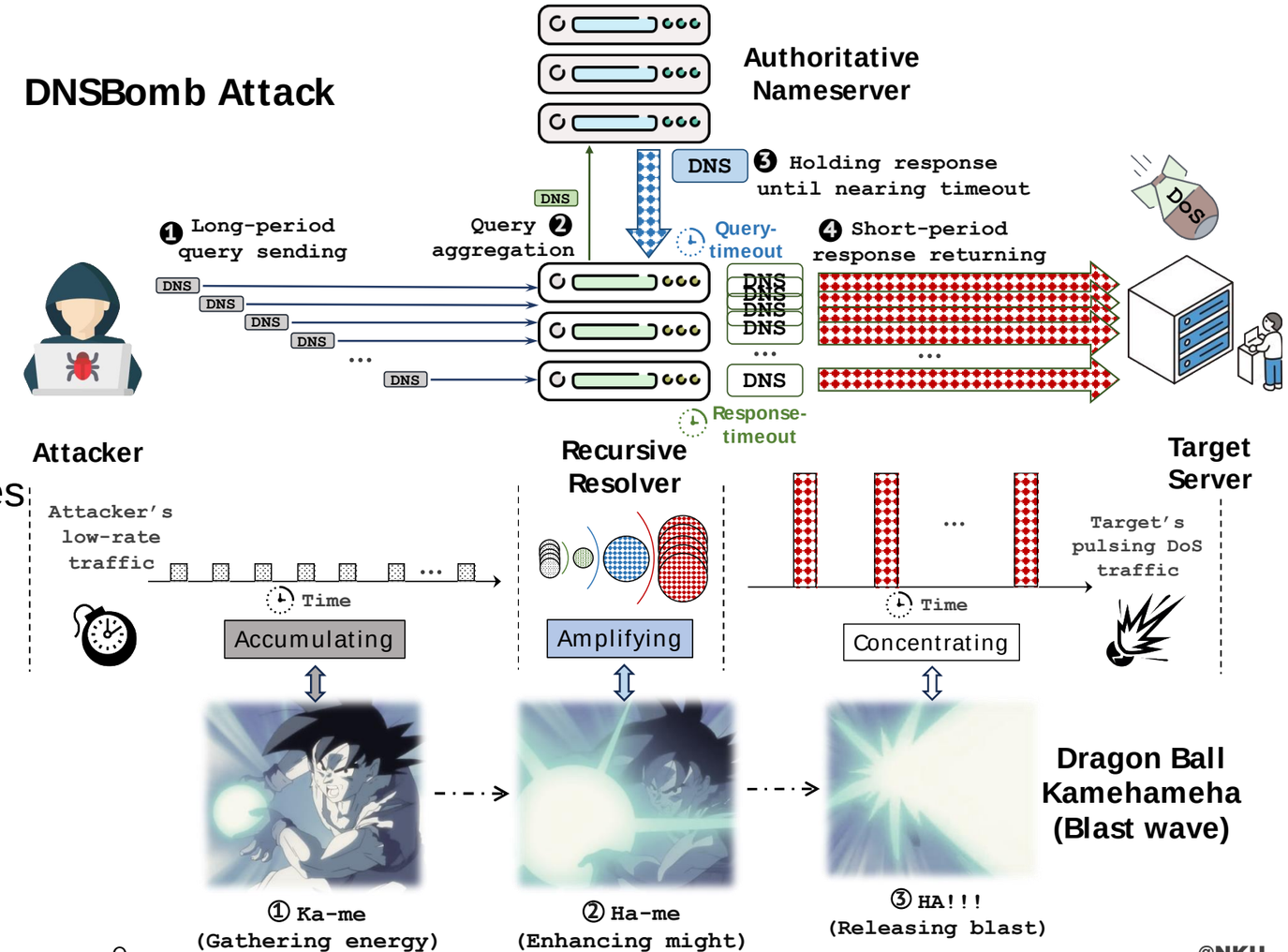
- Accumulating DNS Queries
- **(DNS Resolution Timeout)**

❑ Step 2: Ha-me

- Amplifying DNS Queries into Responses
- **(DNS Query Aggregation & EDNS0)**

❑ Step 3: HA!!!

- Concentrating DNS Responses
- **(DNS Response Fast-returning)**



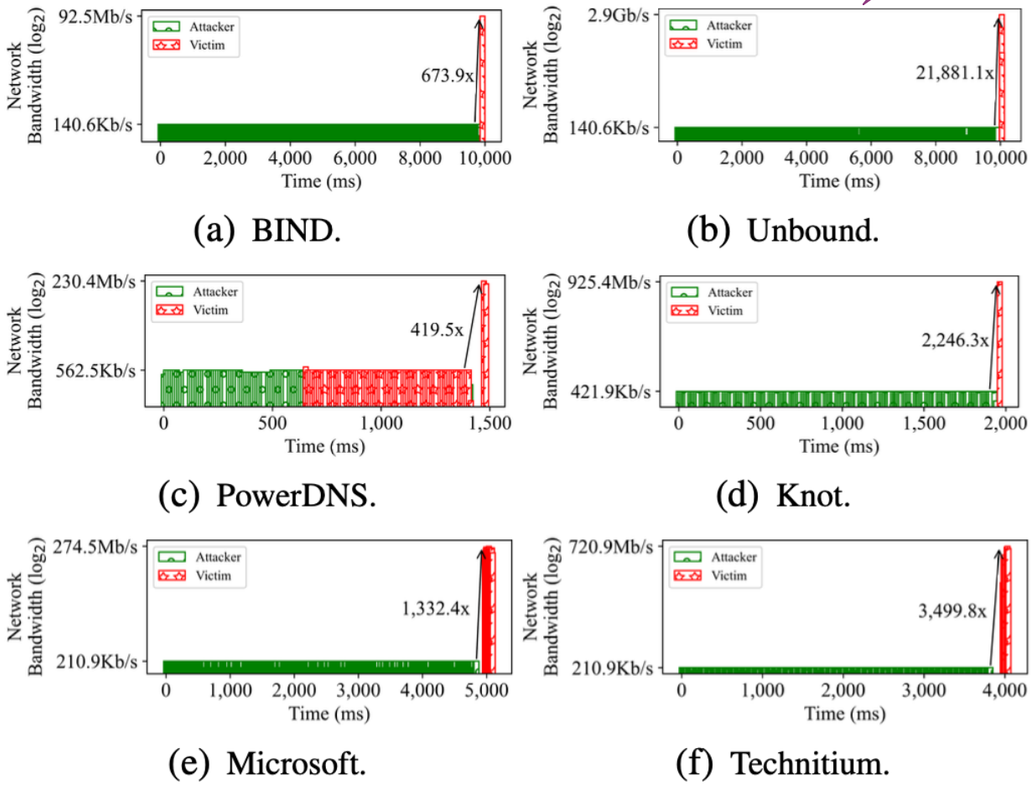
Vulnerable DNS Software

➢ 10 Mainstream DNS Software (All)

❑ Testing attack factors (timeout, pkt. size, returning-time) and local experiments

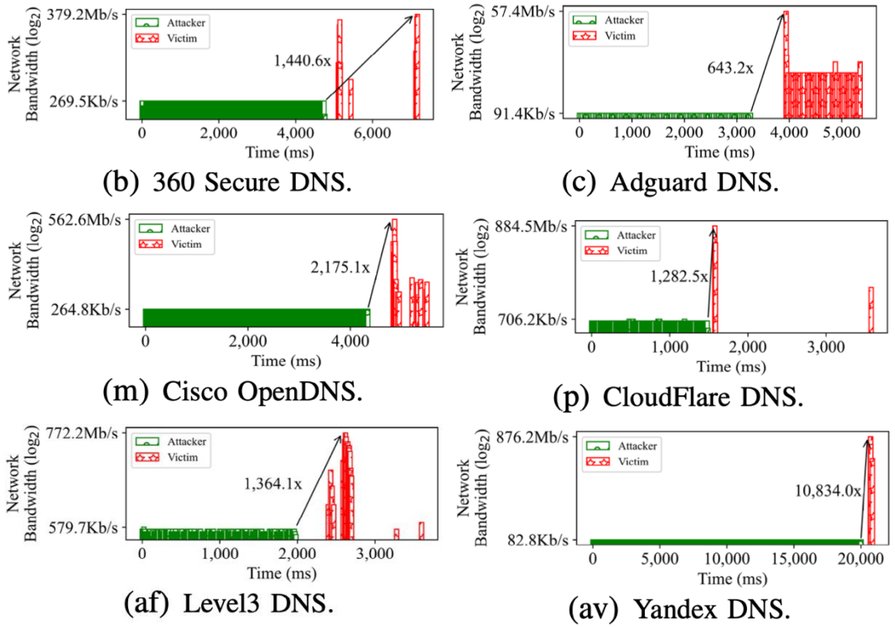
Software	Practical Attack Bandwidth			
	Attacker -side	Victim -side	Nameserver -side	BAF
BIND	140.6Kb/s	92.5Mb/s	155.5Kb/s	**673.9x**
Unbound	**140.6Kb/s**	**2.9Gb/s**	**140.6Kb/s**	**21,881.1x**
PowerDNS	562.5Kb/s	**230.4Mb/s**	70.3Kb/s	**419.5x**
Knot	421.9Kb/s	**925.4Mb/s**	70.3Kb/s	**2,246.3x**
Microsoft	210.9Kb/s	**274.5Mb/s**	70.3Kb/s	**1,332.4x**
Technitium	210.9Kb/s	**720.9Mb/s**	140.6Kb/s	**3,499.8x**
Simple DNS+	562.5Kb/s	36.4Mb/s	1,167.4Kb/s	66.3x
MaraDNS	140.6Kb/s	2.5Mb/s	123.4Kb/s	18.5x
Dnsmasq	140.6Kb/s	**458.9Mb/s**	210.9Kb/s	**3,341.8x**
CoreDNS	140.6Kb/s	**447.5Mb/s**	468.0Kb/s	**3,258.4x**

>8.7Gb/s (More Unbound)



Vulnerable Public DNS Services

- **46 Public DNS Services (All)**
  - Testing their attack factors (timeout, pkt size, returning-time) and small experiments, **14/46:** BAF >1,000x



Part Vendors	Practical Attack Bandwidth			
	Attacker -side	Victim -side	Nameserver -side	BAF
360 Secure DNS	269.5Kb/s	379.2Mb/s	269.5Kb/s	1,440.0x
AdGuard DNS	393.8Kb/s	699.5Mb/s	756.2Kb/s	1,819.0x
CIRA Shield DNS	264.8Kb/s	904.9Mb/s	165.6Kb/s	3,498.8x
Cisco OpenDNS	264.8Kb/s	562.6Mb/s	529.7Kb/s	2,175.1x
CloudFlare DNS	706.2Kb/s	884.5Mb/s	441.4Kb/s	1,282.5x
DNS.WATCH	248.4Kb/s	638.6Mb/s	540.6Kb/s	2,632.1x
DNSPod Public DNS	331.2Kb/s	398.3Mb/s	274.2Kb/s	1,231.1x
Dyn DNS	362.5Kb/s	383.1Mb/s	271.9Kb/s	1,082.2x
Level3 DNS	579.7Kb/s	772.2Mb/s	283.6Kb/s	1,364.1x
Neustar UltraDNS	248.4Kb/s	261.1Mb/s	689.1Kb/s	1,076.1x
Verisign Public DNS	248.4Kb/s	329.4Mb/s	459.4Kb/s	1,357.6x
Yandex DNS	82.8Kb/s	876.2Mb/s	536.7Kb/s	**10,834.0x**

Vulnerable Open Resolvers

➢ Internet Scanning

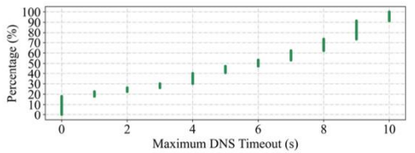
- ❑ Designed probing policies
- ❑ Using XMap + fpdns
  - Software identified: **517,075 (28.7%)**

Type	Resolver number and percentage	
Collected	Alive on 07/05/2023	**1,801,275 (100.0%)**
Software identified	Microsoft DNS	143,928 (8.0%)
	Dnsmasq	96,331 (5.3%)
	BIND	44,016 (2.4%)
	Unbound	15,645 (0.9%)
	PowerDNS	6,367 (0.4%)
	Simple DNS+	166 (0.0%)
	Knot	2 (0.0%)

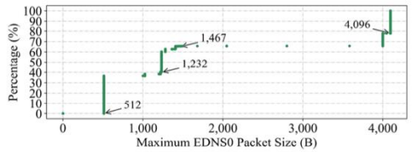
➢ Internet Measurement

- ❑ Measuring attack factors, e.g.,
  - **>50%** resolvers could accumulate >1k queries
  - **>80%** resolvers support timeout of >1s
  - **>60%** resolvers support pkt size of >1,232B

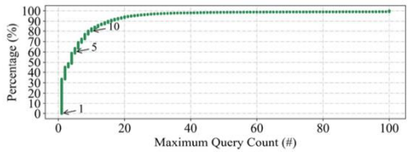
(a) Max. Rate-limit. Rate-limit Values > 1,200 are Shown as 1,200.



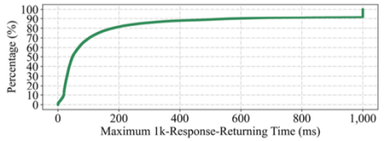
(b) Max. DNS Timeout. Timeout Values > 10s are Shown as 10s.



(c) Max. EDNS0 Packet Size. Size values > 4,096 are Shown as 4,096.



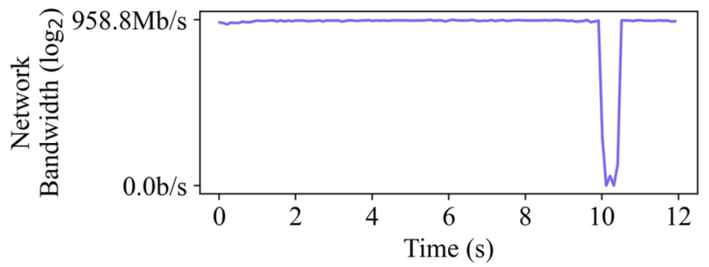
(d) Max. Query Count. Count Values > 100 are Shown as 100.



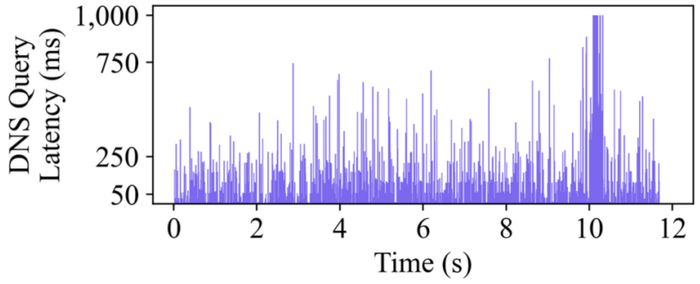
(e) Max. 1k-Responses-Returning Time. Time Values > 1s are Shown as 1s.

Evaluation of DNSBomb

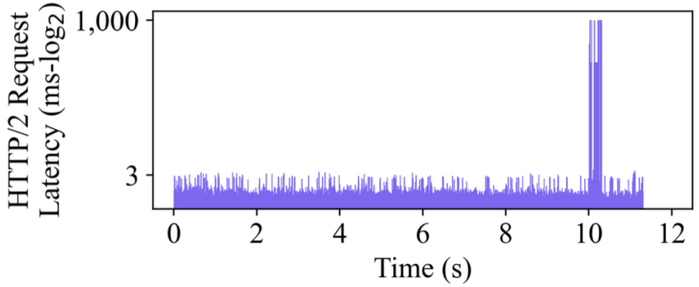
- **Using Unbound**
  - Sending 10k queries within a timeout window of 10s
  - Attacking **a DNS resolver**, **HTTP/2 website**, **and HTTP/3 website**
    - **Network bandwidth is totally occupied**
    - **Resolver never received a query**
    - **HTTP/2 service cannot be fetched**
    - **HTTP/3 is not much affected**



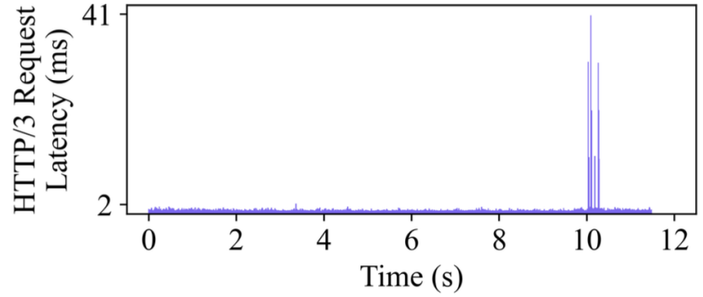
(a) Network Bandwidth.



(b) DNS Resolver.



(c) HTTP/2-based Website.



(d) HTTP/3-based Website.

Mitigation Solutions

➢ Limiting Attack Factors

- ❑ **6 experiments:** base, restricting **timeout** to 1s, **rate-limit** to 100, **pkt. size** to 1,232, **response-returning time** to 1s, all restrictions
- ❑ **Best mitigation:** restricting the timeout and response-returning speed

Software	Base[1]		Timeout[2]		Rate-limit[3]		Pkt. Size[4]		Res. Time[5]		All[6]	
	BAF	*%*	*BAF*	*%*	*BAF*	*%*	*BAF*	*%*	*BAF*	*%*	*BAF*	*%*
BIND	673.9x	100.0%	122.5x	18.2%	1,347.8x	200.0%	673.9x	100.0%	13.5x	2.0%	47.2x	7.0%
Unbound	21,881.1x	100.0%	2,398.5x	11.0%	4,525.6x	20.7%	4,400.5x	20.1%	45.3x	0.2%	20.2x	0.1%
PowerDNS	419.5x	100.0%	178.9x	42.6%	1,132.1x	269.9%	237.6x	56.6%	257.8x	61.4%	20.2x	4.8%
Knot	2,246.3x	100.0%	1,225.3x	54.5%	1,347.8x	60.0%	2,246.3x	100.0%	40.4x	1.8%	13.5x	0.6%
Microsoft	1,332.4x	100.0%	280.7x	21.1%	2,649.8x	198.9%	700.8x	52.6%	44.9x	3.4%	20.2x	1.5%
Technitium	3,499.8x	100.0%	2,867.6x	81.9%	4,525.6x	129.3%	4,492.6x	128.4%	467.6x	13.4%	74.1x	2.1%
Simple DNS+	66.3x	100.0%	61.7x	93.0%	726.3x	1094.8%	97.7x	147.3%	17.5x	26.3%	20.2x	30.5%
MaraDNS	18.5x	100.0%	3.1x	16.7%	37.0x	200.0%	18.5x	100.0%	18.5x	100.0%	18.5x	100.0%
Dnsmasq	3,341.8x	100.0%	624.1x	18.7%	4,546.7x	136.1%	1,033.5x	30.9%	2,728.0x	81.6%	20.5x	0.6%
CoreDNS	3,258.4x	100.0%	524.2x	16.1%	4,389.8x	134.7%	821.8x	25.2%	158.4x	4.9%	20.5x	0.6%

[1]: Base Experiment. [2]: Timeout to 1s. [3]: Rate-limit to 100. [4]: Packet Size to 1,232. [5]: Response-Returning Time to Timeout. [6]: All Restrictions Set.

Vulnerability Disclosure

- **All DNS Implementation are Vulnerable**
  - Reporting to 10 DNS software and 46 vendors
  - 24 Discussed/Confirmed (10 CVEs)
- **Industry-wide CVE-2024-33655**

BIND 9 unbound POWERDNS KNOT RESOLVER Technitium Dnsmasq CoreDNS

114DNS 360 安全DNS Akamai Vantio DNS CZ.NIC ODVR

DNS.SB TOM OneDNS quad9 SAFEDNS

ADGUARD DNS AliDNS 公共解析服务 Baidu DNS ByteDance DNS

CFIEC Public DNS CONTROL D DYN Yandex DNS

Wrap-up

Thanks for listening!

Any question?

Paper

Tool

Xiang Li, Nankai University

lixiang@nankai.edu.cn