Understanding the Implementation and Security Implications of Protective DNS Services

Mingxuan Liu*, **Yiming Zhang***, Xiang Li, Chaoyi Lu,

Baojun Liu, Haixin Duan, Xiaofeng Zheng

中关村实验室 ZGC LAB

清華大學 Tsinghua University

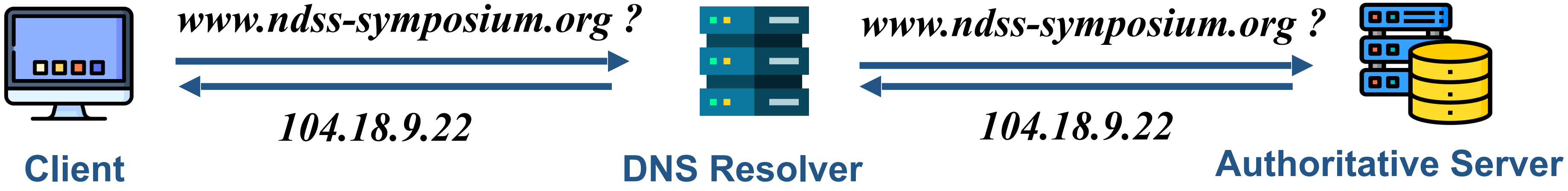
奇安信 QI-ANXIN

NDSS SYMPOSIUM/2024

* *These two authors are both first authors.*

Widespread Abuse of the Domain Name System

- Your journey on the Internet often starts by sending DNS requests



www.ndss-symposium.org ?

104.18.9.22

www.ndss-symposium.org ?

104.18.9.22

Client

DNS Resolver

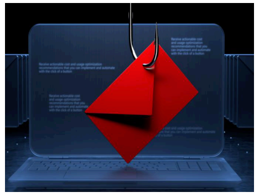
Authoritative Server

- Attackers also widely abuse DNS (use malicious domains) for cyber attacks
  - Over 91% of malware uses DNS to carry out attacks*

Malware

Trojan

Botnet



Phishing

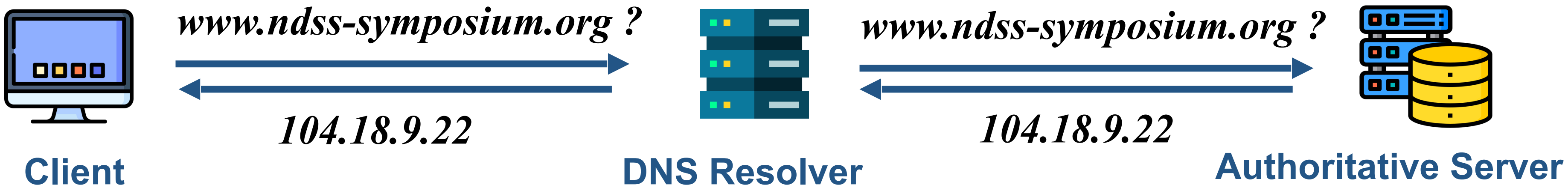
Data Theft

DNS Tunnel

* *https://umbrella.cisco.com/blog/dns-security-your-new-secret-weapon-in-your-fight-against-cybercrime*

Widespread Abuse of the Domain Name System

- Your journey on the Internet often starts by sending DNS requests

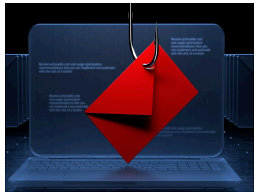


- Attackers also widely abuse DNS (use malicious domains) for cyber attacks
  - Over 91% of malware uses DNS to carry out attacks*

Malware

Trojan

Botnet



Phishing

Data Theft

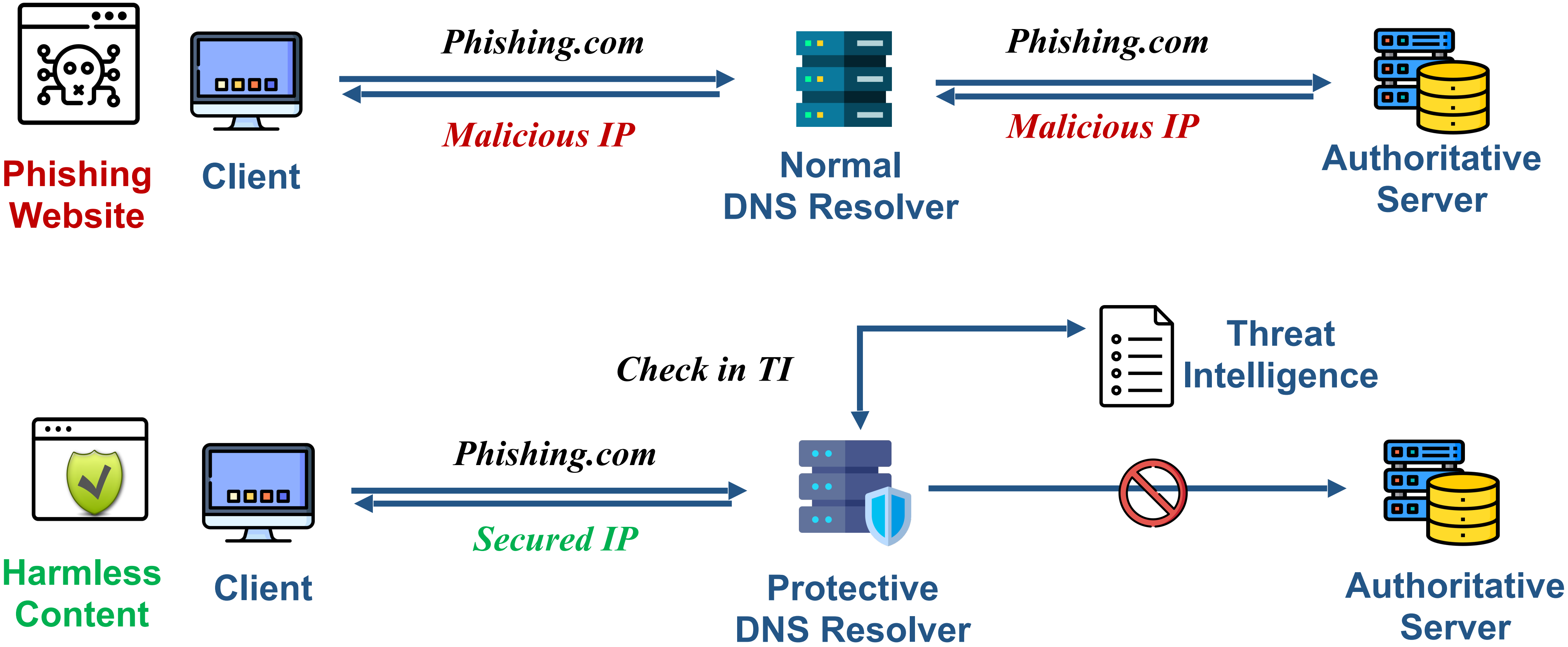
DNS Tunnel

DNS-based blocking mechanisms are effective in curbing cyber attacks!

* *https://umbrella.cisco.com/blog/dns-security-your-new-secret-weapon-in-your-fight-against-cybercrime*

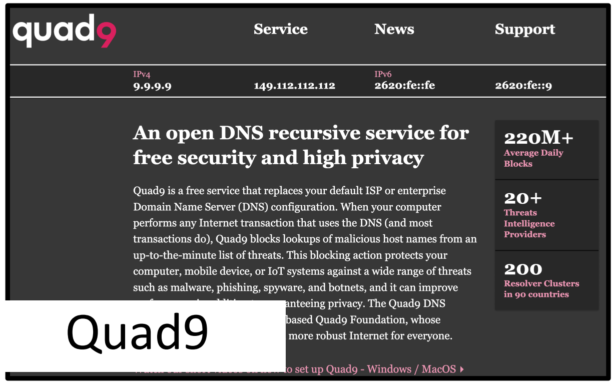
What is Protective DNS (PDNS)

- Protective DNS (PDNS) can proactively intercept and block malicious activities during the domain resolution process



PDNS is a thriving security service

- Gained support from dozens of large DNS services

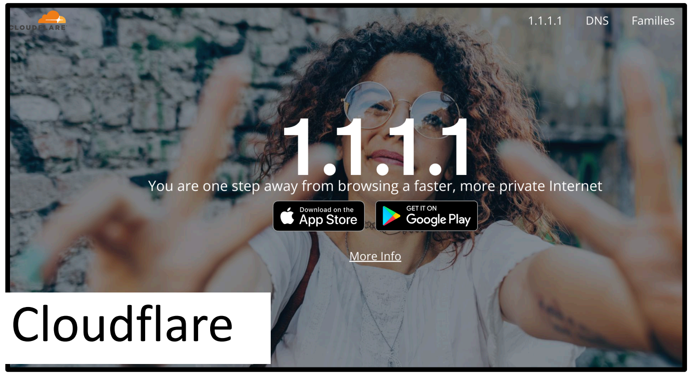


An open DNS recursive service for free security and high privacy

Quad9 is a free service that replaces your default ISP or enterprise Domain Name Server (DNS) configuration. When your computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve
anteeing privacy. The Quad9 DNS
based Quad9 Foundation, whose
more robust Internet for everyone.

o set up Quad9 - Windows / MacOS ▸

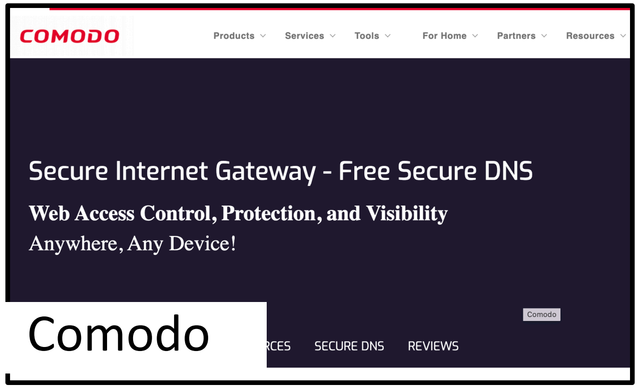
Quad9



1.1.1.1

You are one step away from browsing a faster, more private Internet

Cloudflare



Secure Internet Gateway - Free Secure DNS

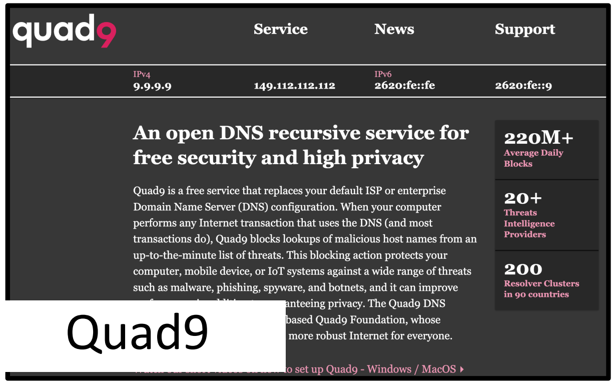
Web Access Control, Protection, and Visibility

Anywhere, Any Device!

Comodo

PDNS is a thriving security service

- Gained support from dozens of large DNS services



quad9 Service News Support

IPv4 9.9.9.9 149.112.112.112 IPv6 2620:fe::fe 2620:fe::9

An open DNS recursive service for free security and high privacy

Quad9 is a free service that replaces your default ISP or enterprise Domain Name Server (DNS) configuration. When your computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve

anteeing privacy. The Quad9 DNS

based Quad9 Foundation, whose

more robust Internet for everyone.

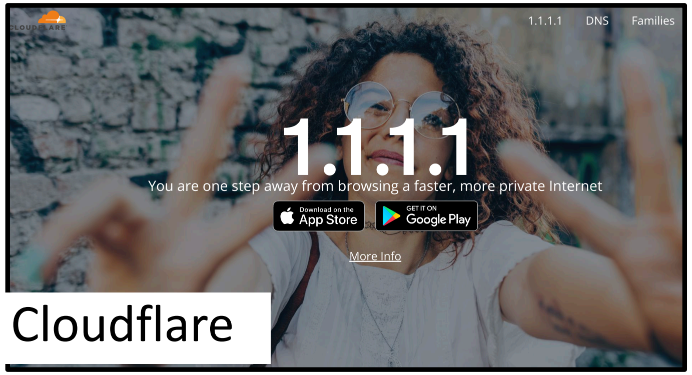
o set up Quad9 - Windows / MacOS ›

220M+ Average Daily Blocks

20+ Threats Intelligence Providers

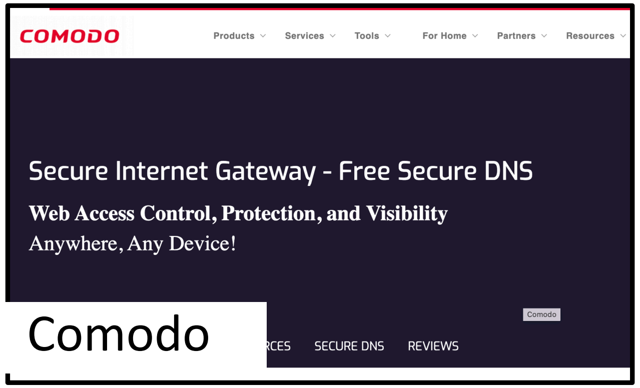
200 Resolver Clusters in 90 countries

Quad9



CLOUDFLARE
1.1.1.1 DNS Families
1.1.1.1
You are one step away from browsing a faster, more private Internet
Download on the App Store
GET IT ON Google Play
More Info

Cloudflare



COMODO Products Services Tools For Home Partners Resources

Secure Internet Gateway - Free Secure DNS

Web Access Control, Protection, and Visibility

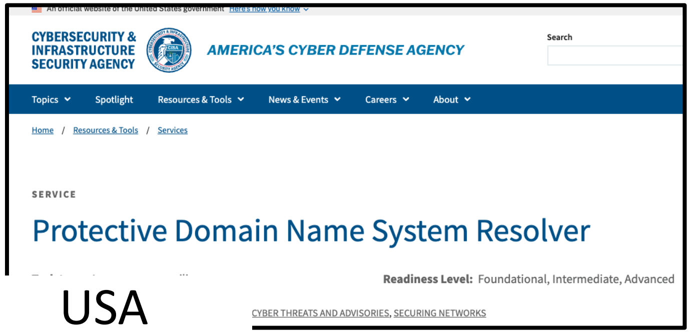
Anywhere, Any Device!

Comodo

RCES SECURE DNS REVIEWS

Comodo

- Promoted to establish National PDNS infrastructure



An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY AMERICA'S CYBER DEFENSE AGENCY

Search

Topics Spotlight Resources & Tools News & Events Careers About

Home / Resources & Tools / Services

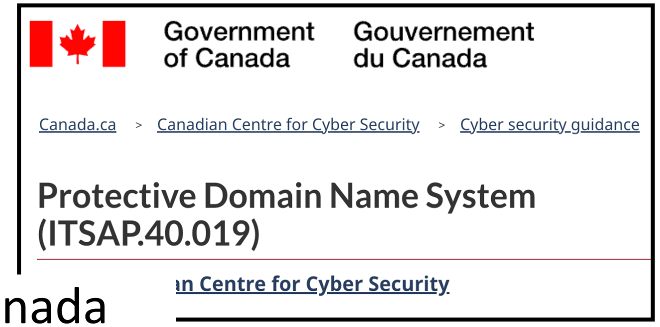
SERVICE

Protective Domain Name System Resolver

Readiness Level: Foundational, Intermediate, Advanced

CYBER THREATS AND ADVISORIES, SECURING NETWORKS

USA



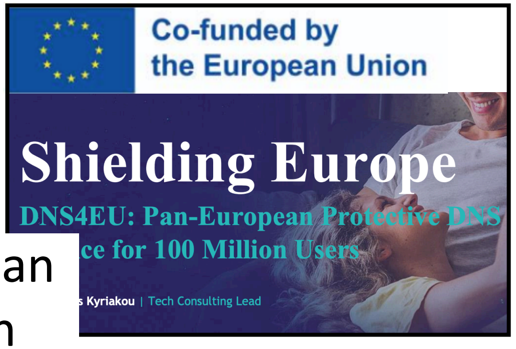
Government of Canada Gouvernement du Canada

Canada.ca > Canadian Centre for Cyber Security > Cyber security guidance

Protective Domain Name System (ITSAP.40.019)

n Centre for Cyber Security

Canada



Co-funded by the European Union

Shielding Europe

DNS4EU: Pan-European Protective DNS ce for 100 Million Users

s Kyriakou | Tech Consulting Lead

European Union

Research Questions of PDNS

- **Research Gap:** High opacity and diversity hinder the understanding of PDNS

Research Questions of PDNS

- **Research Gap:** High opacity and diversity hinder the understanding of PDNS

How many DNS servers in the wild are offering PDNS services?

Research Questions of PDNS

- **Research Gap:** High opacity and diversity hinder the understanding of PDNS

How many DNS servers in the wild are offering PDNS services?

What are the **blocking policies** of PDNS?

Research Questions of PDNS

- **Research Gap:** High opacity and diversity hinder the understanding of PDNS

How many DNS servers in the wild are offering PDNS services?

What are the **blocking policies** of PDNS?

Are there any **security risks** within the PDNS infrastructure?

Our Work

Identifying PDNS Methodology

- Distinguishing modification of PDNS
- Identified 17,601 open PDNS servers in the wild

Understanding of PDNS Ecosystem

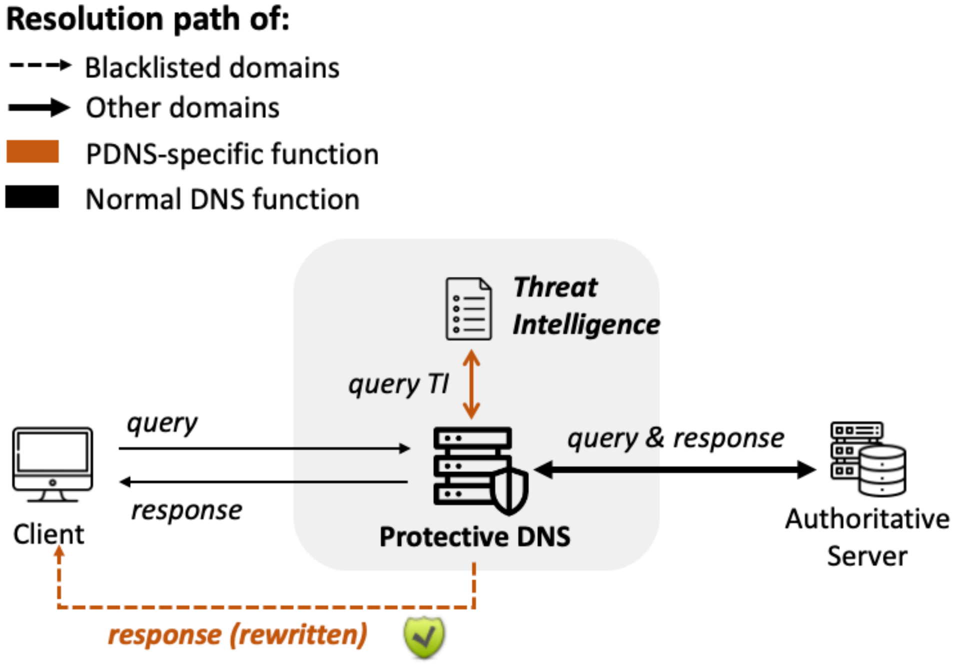
- First active measurement study for PDNS
- Blocklist and rewriting policy

Security analysis of PDNS infrastructure

- First discover 3 types of security flaws
- Denial of Response (DoR)
- Dangling PDNS Infrastructure
- Subversion of Protective Features

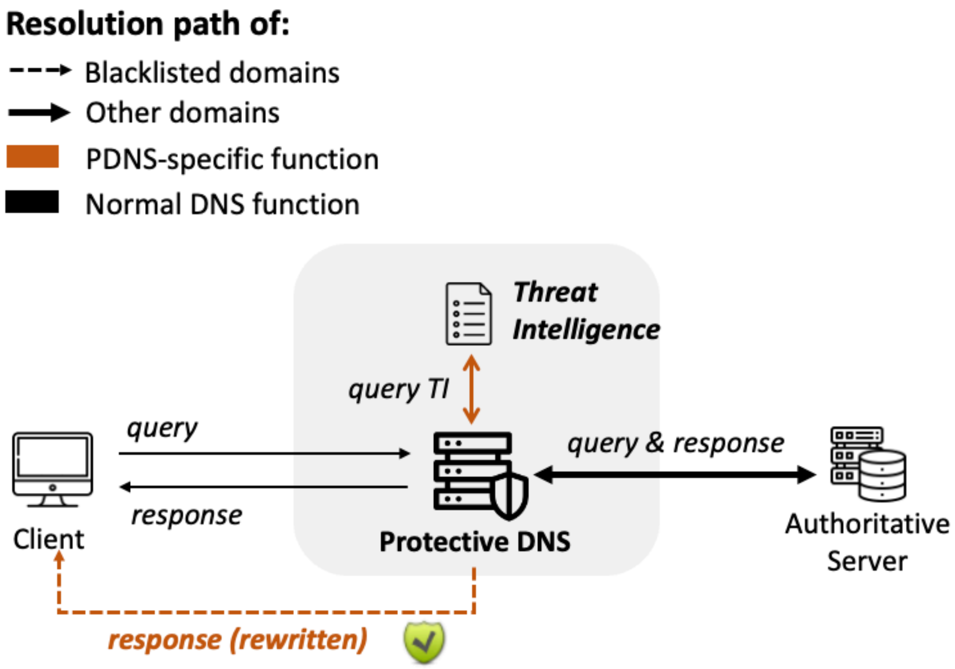
Empirical Study of 28 Public PDNS

- Empirical Study of the domain blocklist and DNS rewriting policies of 28 public-claimed PDNSes



Empirical Study of 28 Public PDNS

- Empirical Study of the domain blocklist and DNS rewriting policies of 28 public-claimed PDNSes

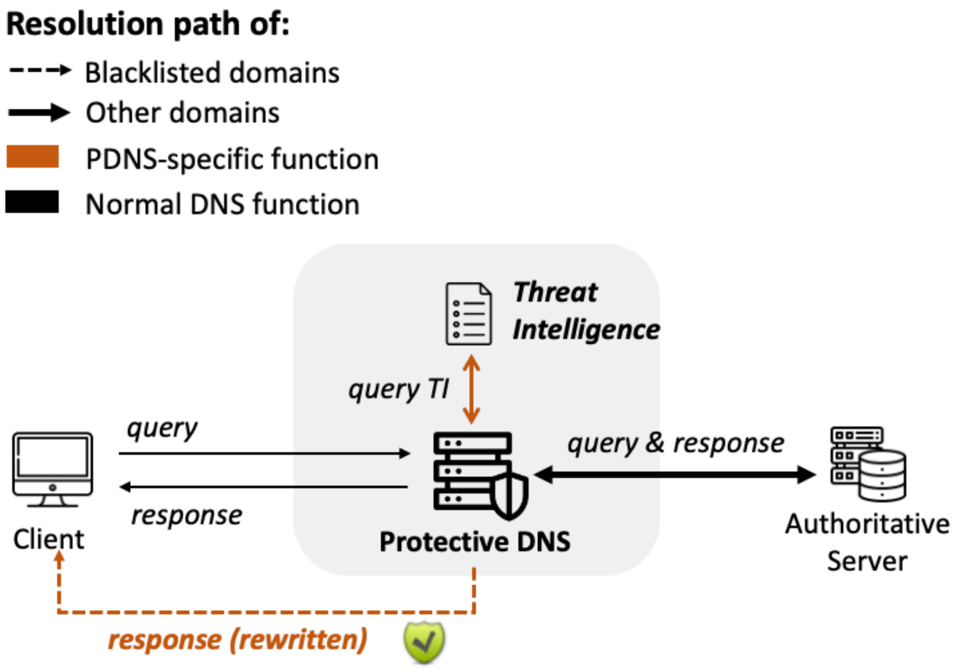


Domain Blocklist

- ➢ **Open-source domain blocklist**: 7 PDNS providers
- ➢ **Private domain blocklist**: 11 PDNS providers
- ➢ **Unknown source**: 16 PDNS providers
- ➢ **User complaints and corrections**: 2 PDNS providers

Empirical Study of 28 Public PDNS

- Empirical Study of the domain blocklist and DNS rewriting policies of 28 public-claimed PDNSes



Domain Blocklist

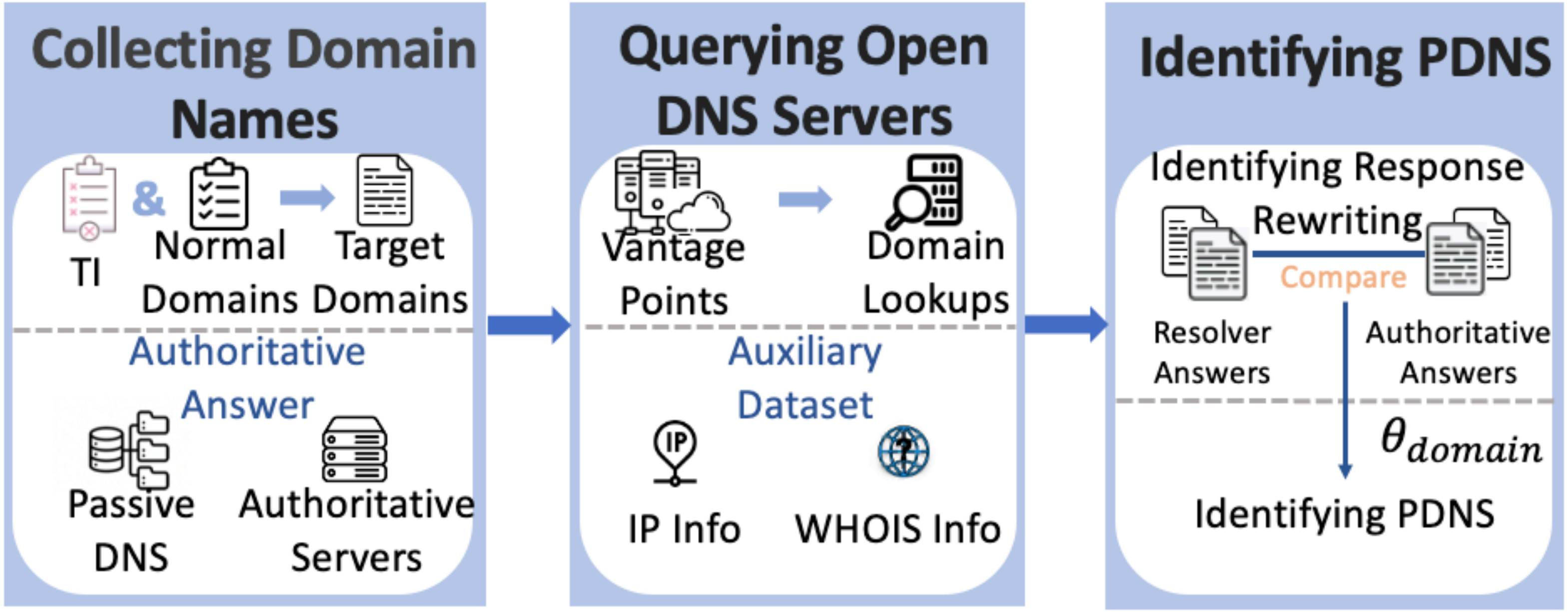
- **Open-source domain blocklist**: 7 PDNS providers
- **Private domain blocklist**: 11 PDNS providers
- **Unknown source**: 16 PDNS providers
- **User complaints and corrections**: 2 PDNS providers

Rewriting Policy

- **Special-use IP addresses**: 4 PDNS providers, e.g., 0.0.0.0
- **Secure IP addresses**: 14 PDNS providers
- **Secure CNAMEs**: 4 PDNS providers
- **Response code**: 2 PDNS providers
- **No data**: 6 PDNS providers

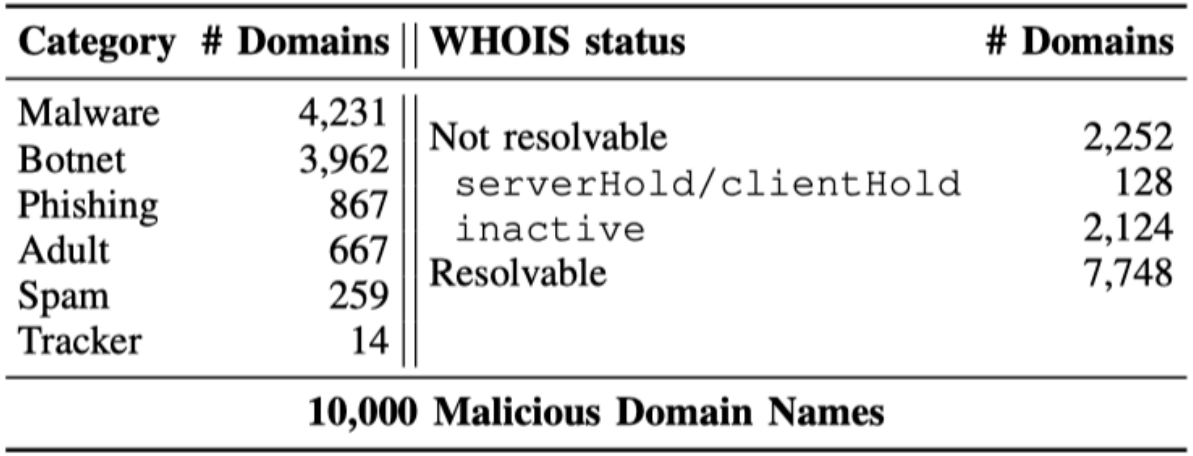
Identification Methodology for PDNS in the wild

- 3-step identification methodology for PDNS
  - Step I: Collecting Domain Names
  - Step II: Querying Open DNS Servers
  - Step III: Identifying PDNS



Identification Methodology for PDNS in the wild

- **Step I - Collecting domain names**: compile a list of **10,000** "generally-malicious" domain names from 7 public blocklists, and 100 popular domains



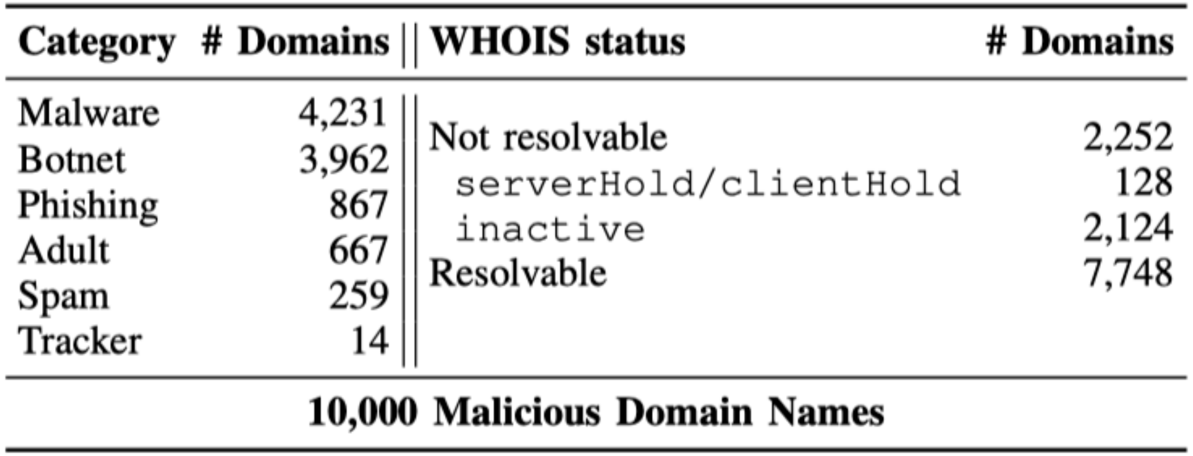
Category	# Domains	WHOIS status	# Domains
Malware	4,231	Not resolvable	2,252
Botnet	3,962	`serverHold/clientHold`	128
Phishing	867	`inactive`	2,124
Adult	667	Resolvable	7,748
Spam	259		
Tracker	14		
10,000 Malicious Domain Names			

Tranco

100 Popular Domains

Identification Methodology for PDNS in the wild

- **Step I - Collecting domain names**: compile a list of **10,000** "generally-malicious" domain names from 7 public blocklists, and 100 popular domains



Category	# Domains	WHOIS status	# Domains
Malware	4,231	Not resolvable	2,252
Botnet	3,962	`serverHold/clientHold`	128
Phishing	867	`inactive`	2,124
Adult	667	Resolvable	7,748
Spam	259		
Tracker	14		
10,000 Malicious Domain Names			

Tranco

100 Popular Domains

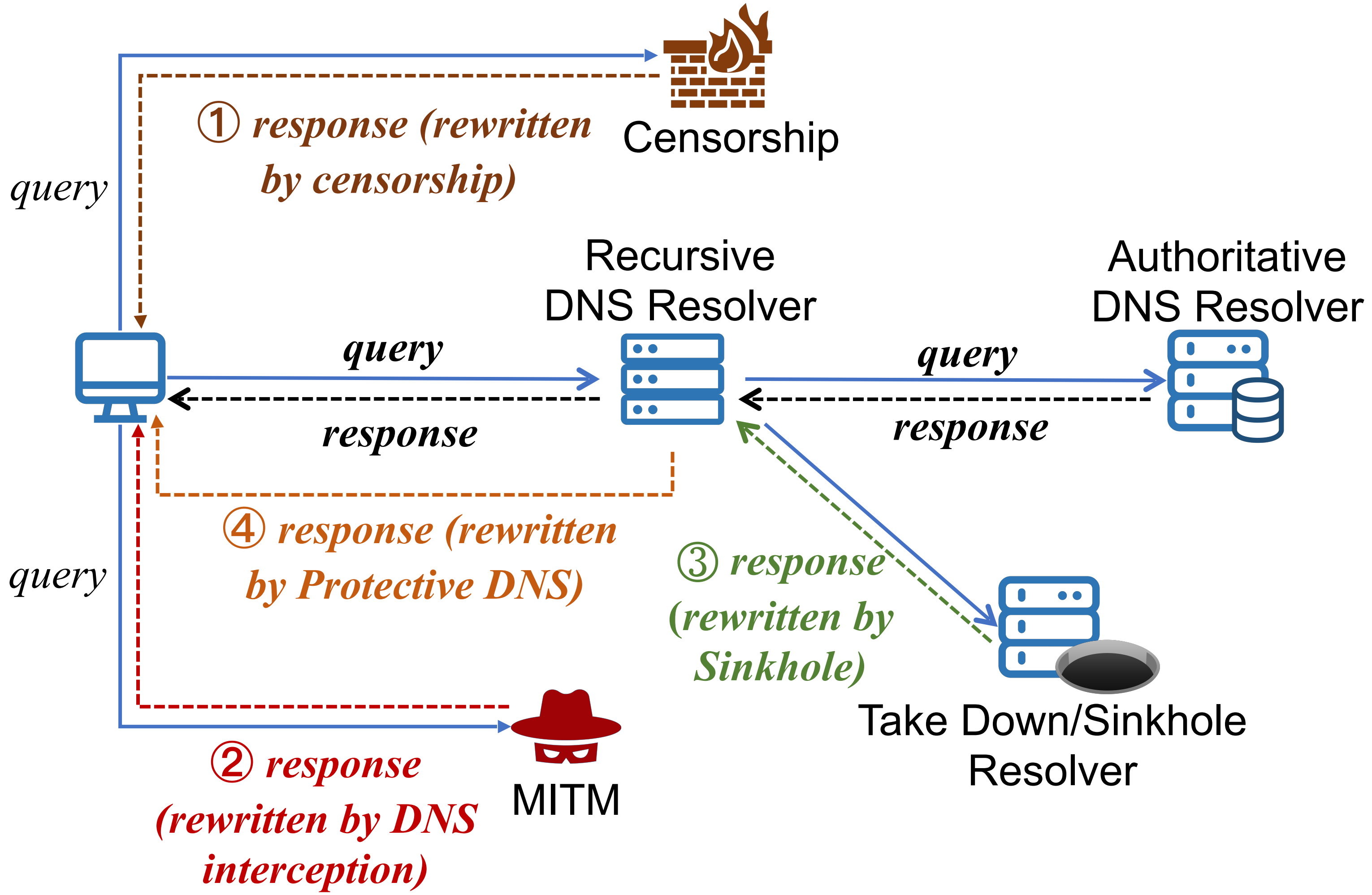
- **Step II - Querying open DNS servers:** combine active query resolution results with Passive DNS records

Actively Querying

Passive DNS

Identify modification of PDNS is challenging

- **Step III – Identifying PDNS:** Distinguish the modified responses from PDNS and from other DNS manipulations



Censorship
query
① response (rewritten by censorship)
Recursive DNS Resolver
Authoritative DNS Resolver
query
response
query
response
④ response (rewritten by Protective DNS)
③ response (rewritten by Sinkhole)
query
Take Down/Sinkhole Resolver
② response (rewritten by DNS interception)
MITM

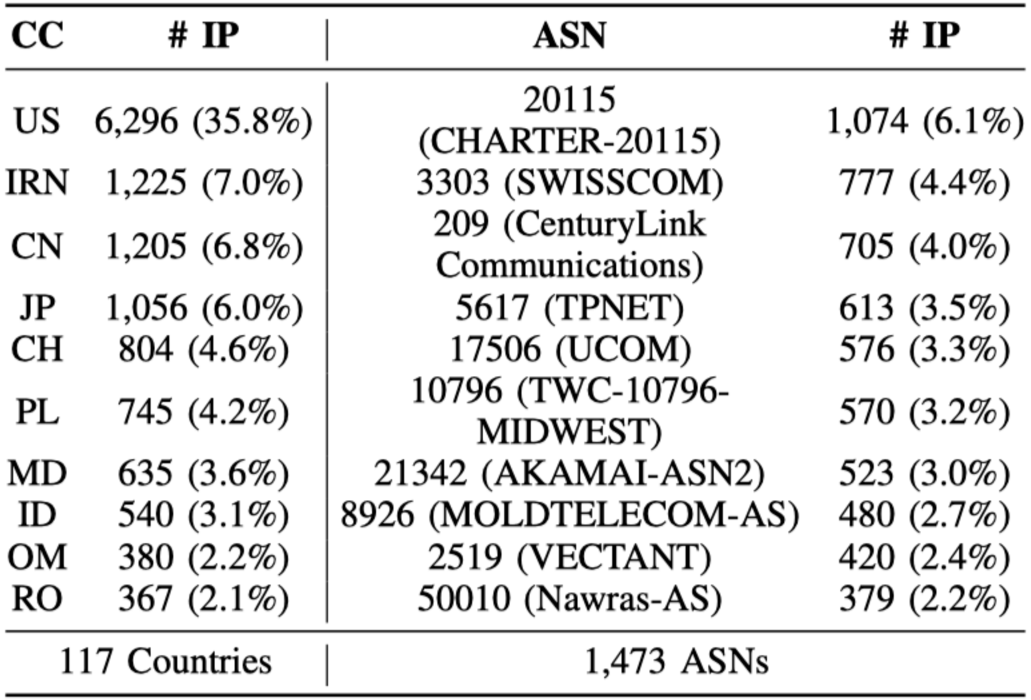
Finding 1: Deployment status of PDNS Services in the wild

- **17,601 (9.08%)** PDNS resolvers in the wild within 193,888 “stable” recursive resolvers from 6 scanning experiments

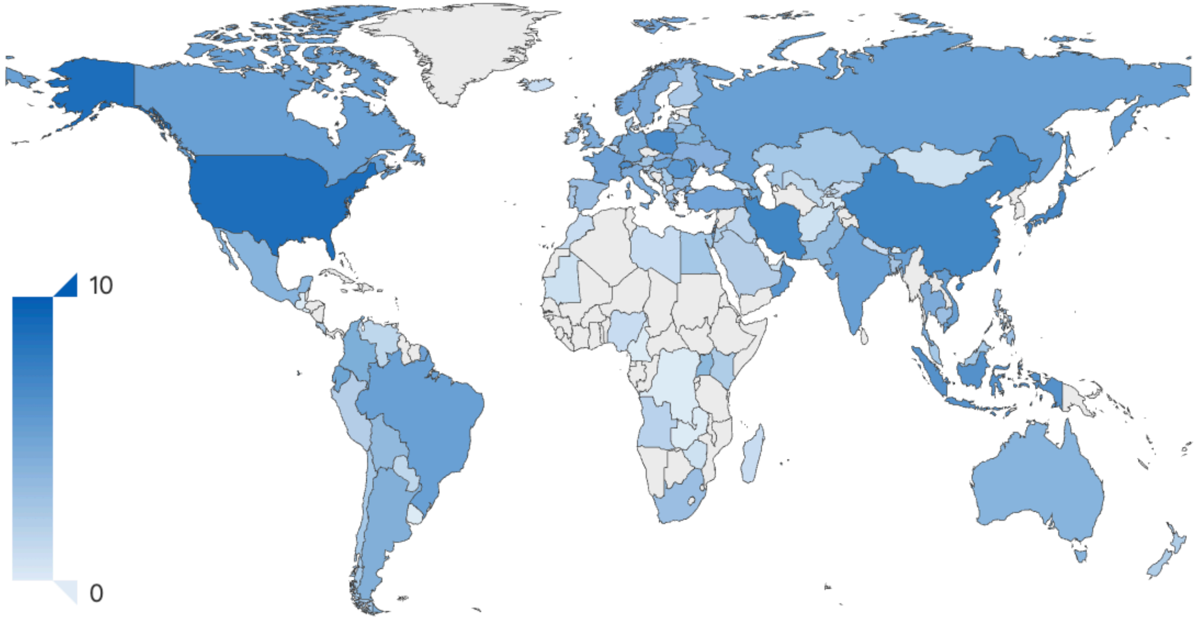
Finding 1: Deployment status of PDNS Services in the wild

- **17,601 (9.08%)** PDNS resolvers in the wild within 193,888 “stable” recursive resolvers from 6 scanning experiments

- **PDNS resolvers are widely deployed around the world**, encompassing **117 countries and regions**, covering a total of **1473 AS**



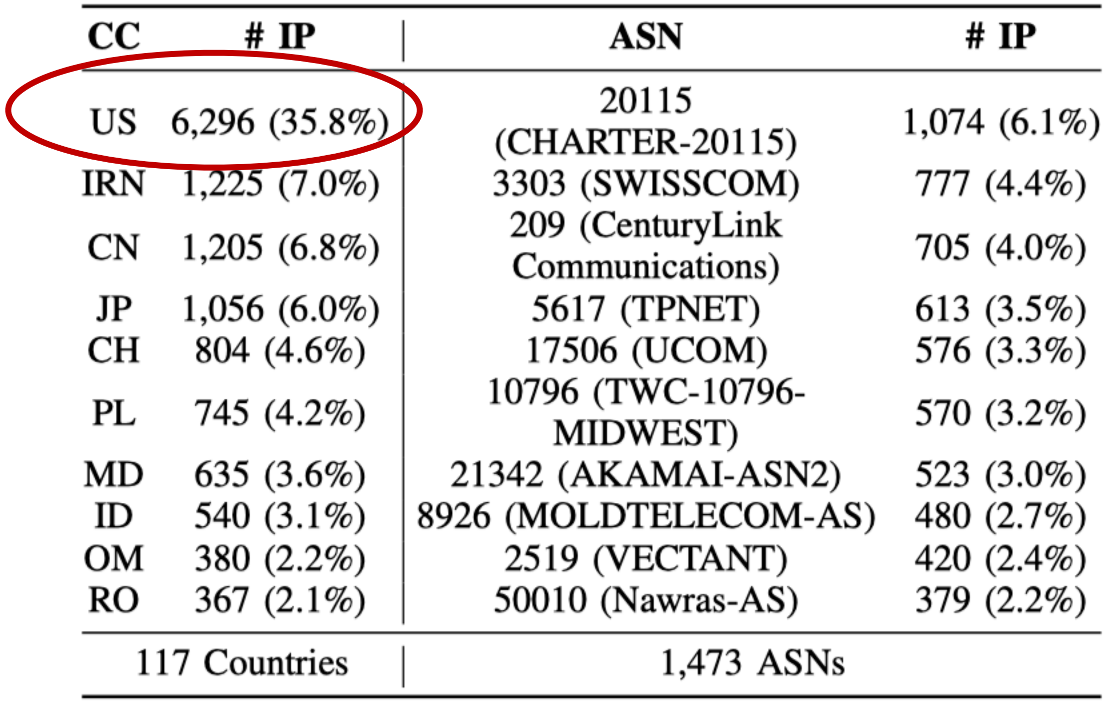
CC	# IP	ASN	# IP
US	6,296 (35.8%)	20115 (CHARTER-20115)	1,074 (6.1%)
IRN	1,225 (7.0%)	3303 (SWISSCOM)	777 (4.4%)
CN	1,205 (6.8%)	209 (CenturyLink Communications)	705 (4.0%)
JP	1,056 (6.0%)	5617 (TPNET)	613 (3.5%)
CH	804 (4.6%)	17506 (UCOM)	576 (3.3%)
PL	745 (4.2%)	10796 (TWC-10796-MIDWEST)	570 (3.2%)
MD	635 (3.6%)	21342 (AKAMAI-ASN2)	523 (3.0%)
ID	540 (3.1%)	8926 (MOLDTELECOM-AS)	480 (2.7%)
OM	380 (2.2%)	2519 (VECTANT)	420 (2.4%)
RO	367 (2.1%)	50010 (Nawras-AS)	379 (2.2%)
117 Countries		1,473 ASNs	



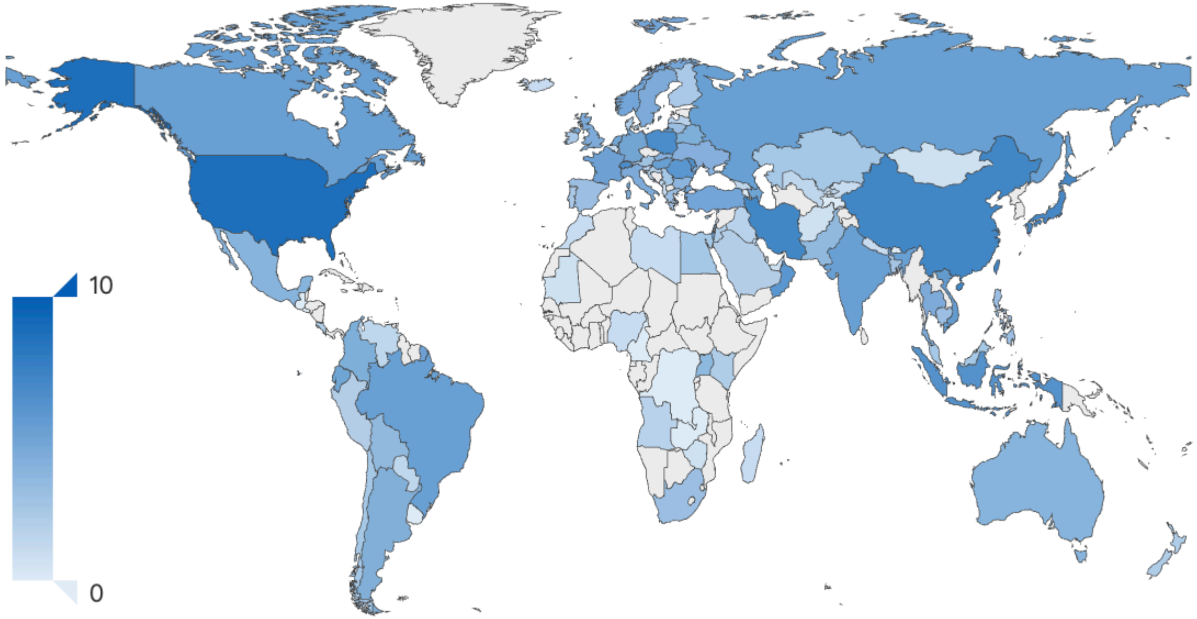
Finding 1: Deployment status of PDNS Services in the wild

- **17,601 (9.08%)** PDNS resolvers in the wild within 193,888 “stable” recursive resolvers from 6 scanning experiments

- **PDNS resolvers are widely deployed around the world**, encompassing **117 countries and regions**, covering a total of **1473 AS**

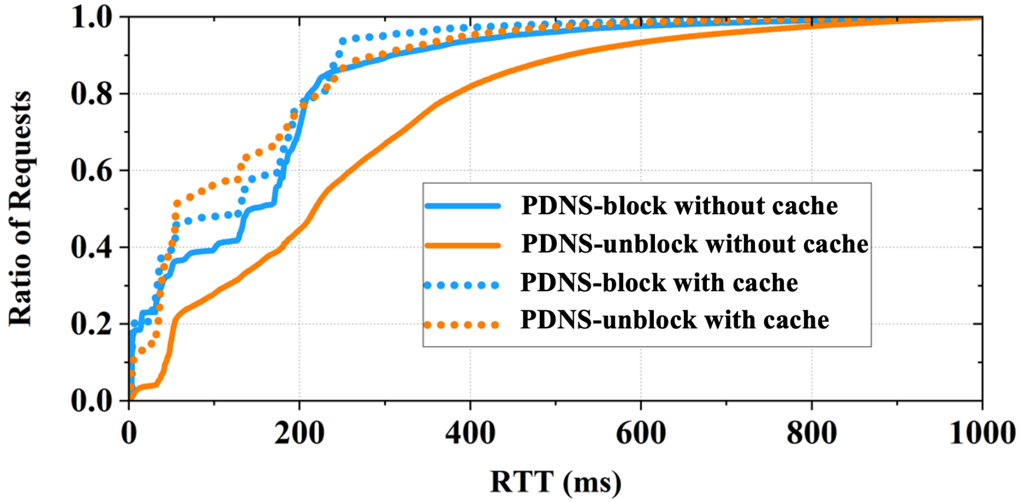


CC	# IP	ASN	# IP
US	6,296 (35.8%)	20115 (CHARTER-20115)	1,074 (6.1%)
IRN	1,225 (7.0%)	3303 (SWISSCOM)	777 (4.4%)
CN	1,205 (6.8%)	209 (CenturyLink Communications)	705 (4.0%)
JP	1,056 (6.0%)	5617 (TPNET)	613 (3.5%)
CH	804 (4.6%)	17506 (UCOM)	576 (3.3%)
PL	745 (4.2%)	10796 (TWC-10796-MIDWEST)	570 (3.2%)
MD	635 (3.6%)	21342 (AKAMAI-ASN2)	523 (3.0%)
ID	540 (3.1%)	8926 (MOLDTELECOM-AS)	480 (2.7%)
OM	380 (2.2%)	2519 (VECTANT)	420 (2.4%)
RO	367 (2.1%)	50010 (Nawras-AS)	379 (2.2%)
117 Countries		1,473 ASNs	



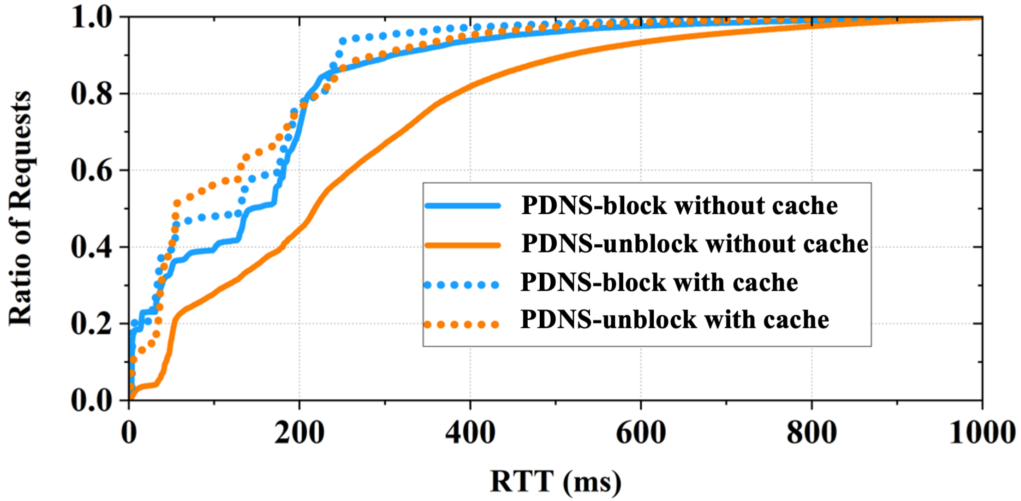
Finding 2: Querying Performance of PDNS

- **Round-Trip Time (RTT)** for evaluating the query performance of 155 prominent PDNSes



Finding 2: Querying Performance of PDNS

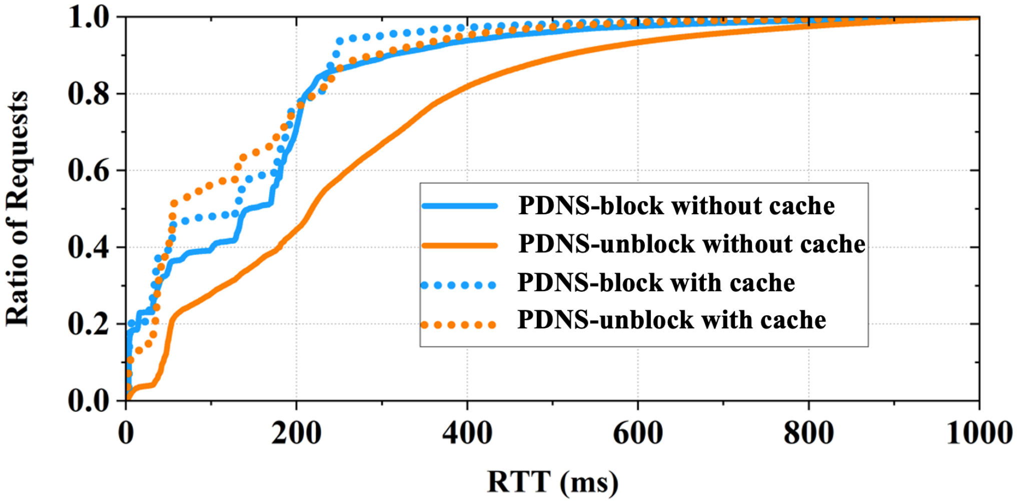
- **Round-Trip Time (RTT)** for evaluating the query performance of 155 prominent PDNSes



- **Without cache**, PDNS responds quicker to blocked domains than other domains

Finding 2: Querying Performance of PDNS

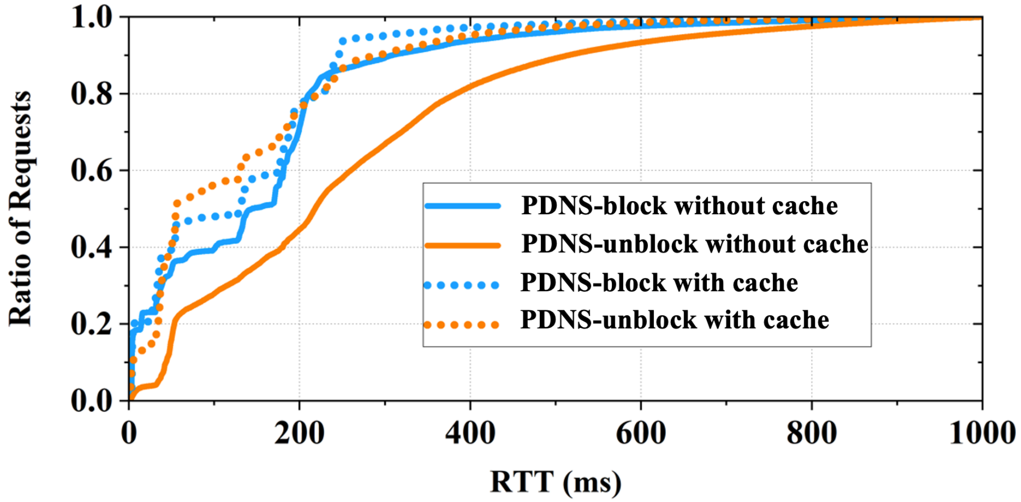
- **Round-Trip Time (RTT)** for evaluating the query performance of 155 prominent PDNSes



- **Without cache**, PDNS responds quicker to blocked domains than other domains
- **With cache,** the difference becomes less pronounced when caching is enabled

Finding 2: Querying Performance of PDNS

- **Round-Trip Time (RTT)** for evaluating the query performance of 155 prominent PDNSes



- **Without cache**, PDNS responds quicker to blocked domains than other domains
- **With cache,** the difference becomes less pronounced when caching is enabled
- **Reason of different performance:** PDNS prefers to block domains before recursive resolution

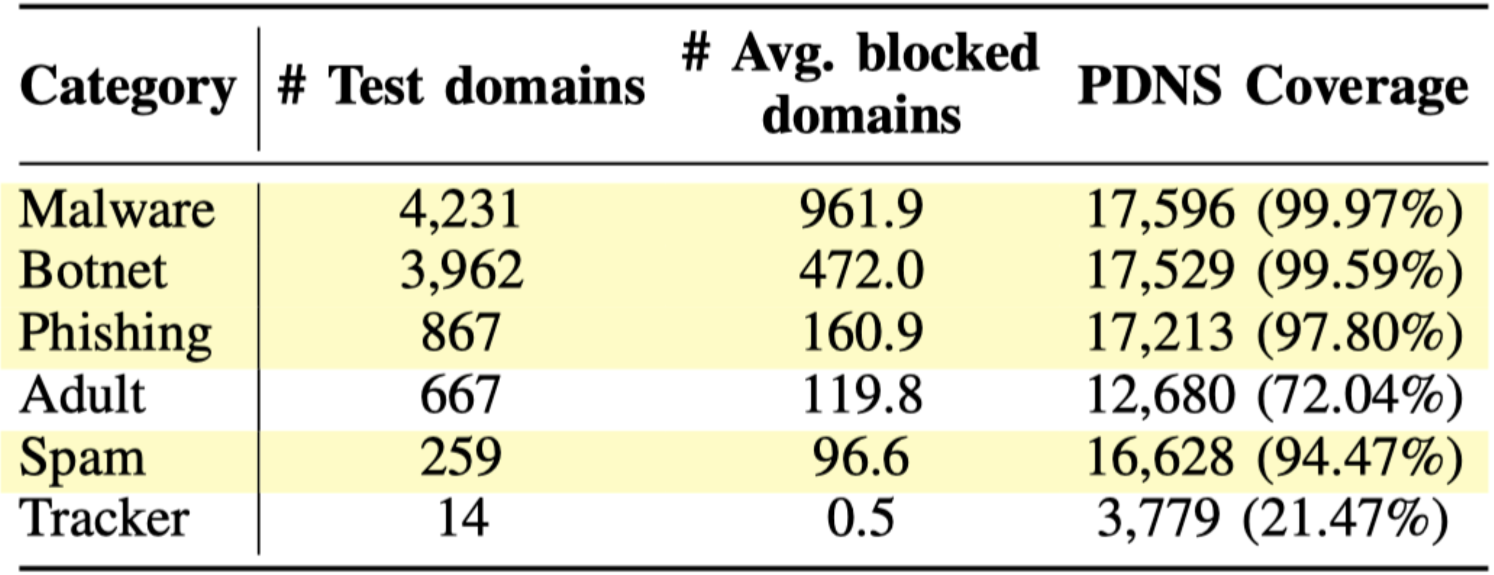
Finding 3: Blocklist of PDNS

- 57% PDNSes block over 500 malicious domains, while 43% prominent PDNSes block fewer than 100 domains

Finding 3: Blocklist of PDNS

- 57% PDNSes block over 500 malicious domains, while 43% prominent PDNSes block fewer than 100 domains

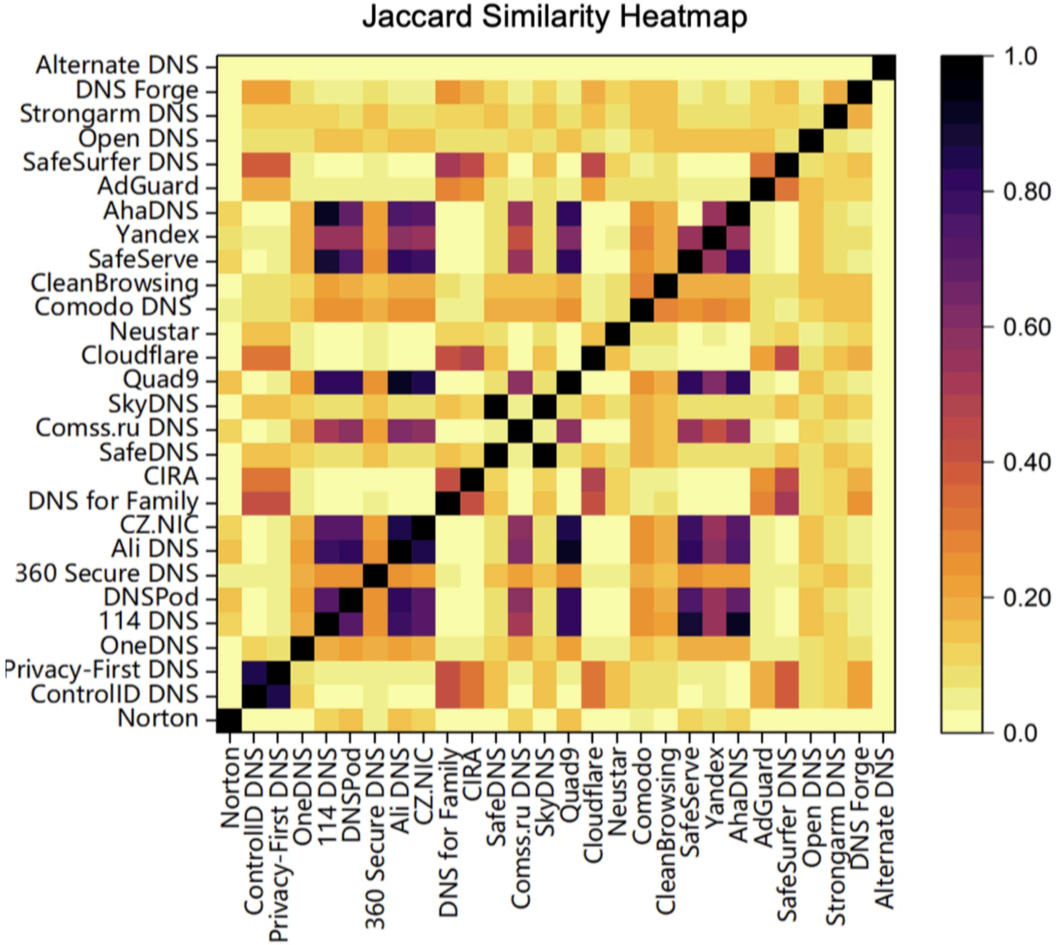
- **Conservative choice of blocklist**: Preference of using a narrow set of "high-risk" domains for prominent DNS providers



Category	# Test domains	# Avg. blocked domains	PDNS Coverage
Malware	4,231	961.9	17,596 (99.97%)
Botnet	3,962	472.0	17,529 (99.59%)
Phishing	867	160.9	17,213 (97.80%)
Adult	667	119.8	12,680 (72.04%)
Spam	259	96.6	16,628 (94.47%)
Tracker	14	0.5	3,779 (21.47%)

Similarity of Blocklist between different PDNS providers

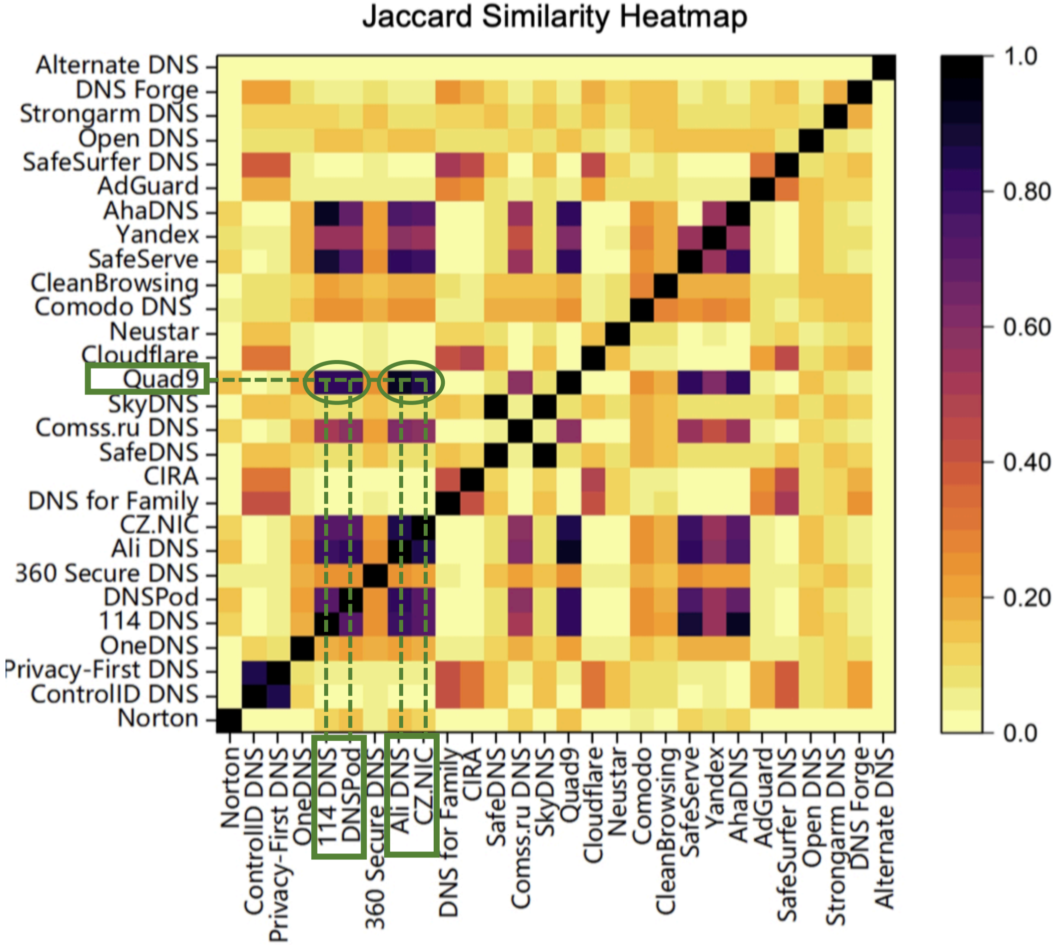
- **Blocklist Similarity**: several blocklists for 28 popular PDNS providers exhibit significant correlations



Similarity of Blocklist between different PDNS providers

- **Blocklist Similarity**: several blocklists for 28 popular PDNS providers exhibit significant correlations

Similarities between Quad9 and 3 PDNS providers are over 0.80

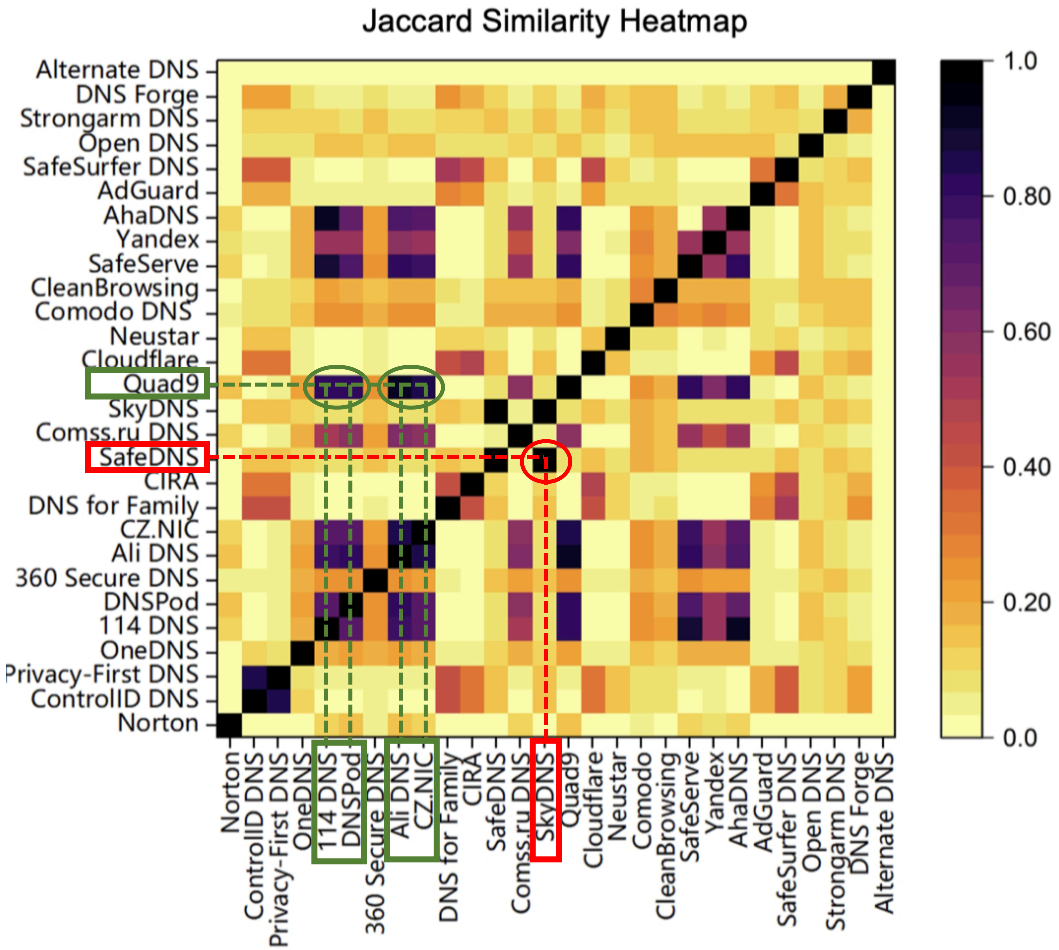


Similarity of Blocklist between different PDNS providers

- **Blocklist Similarity**: several blocklists for 28 popular PDNS providers exhibit significant correlations

Similarities between Quad9 and 3 PDNS providers are over 0.80

Similarity between SkyDNS and SafeDNS is 0.99



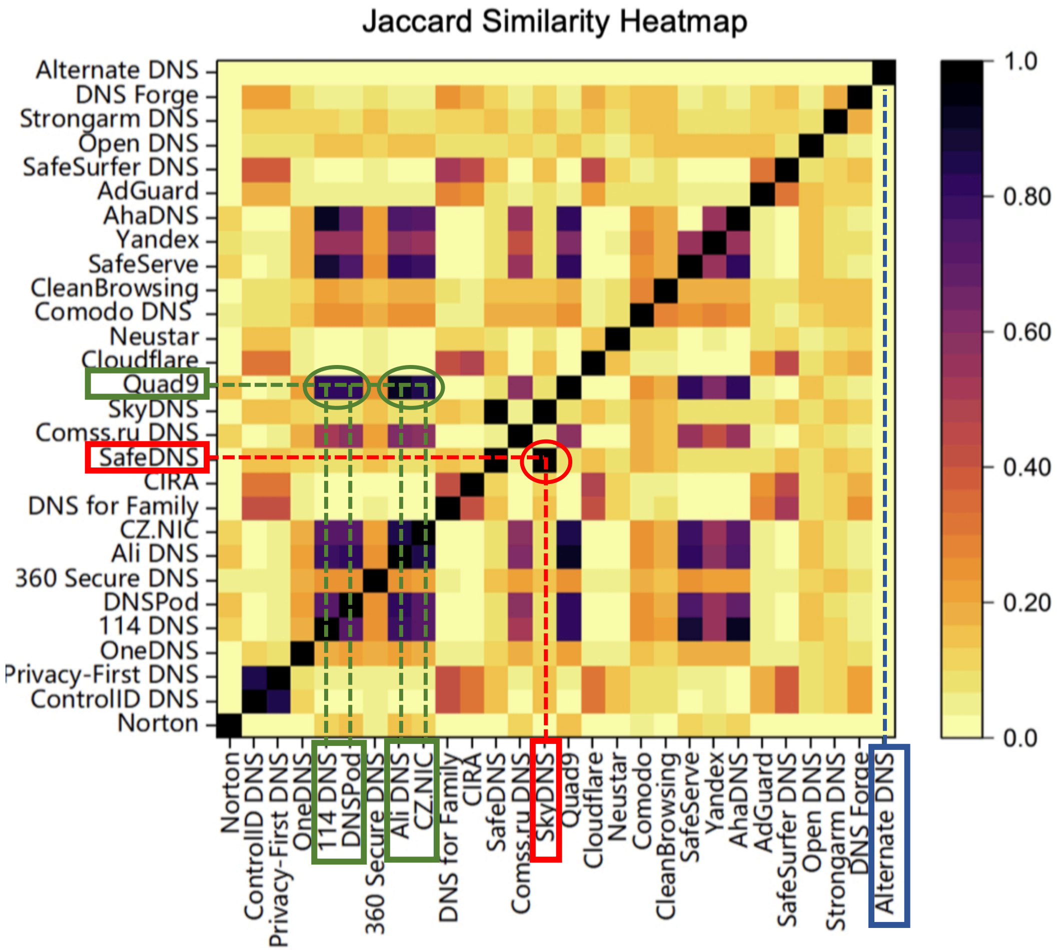
Similarity of Blocklist between different PDNS providers

- **Blocklist Similarity**: several blocklists for 28 popular PDNS providers exhibit significant correlations

Similarities between Quad9 and 3 PDNS providers are over 0.80

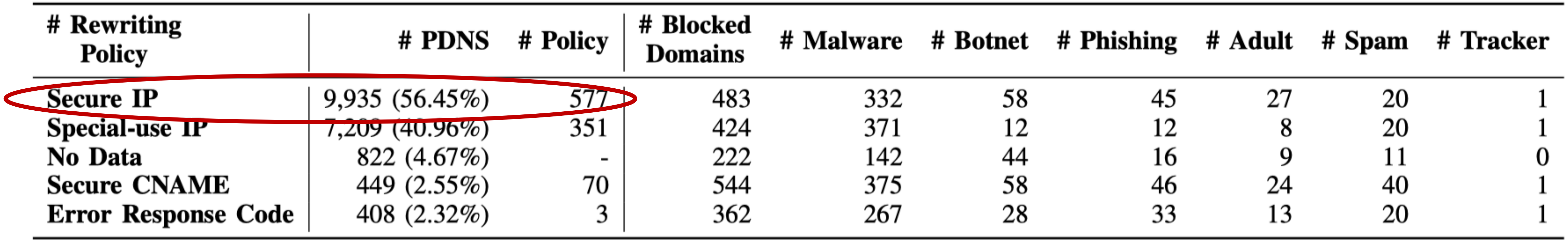
Similarity between SkyDNS and SafeDNS is 0.99

Similarities between Alternate DNS and other PDNSes is 0.21 in average



Finding 4: Rewriting Policies of PDNS

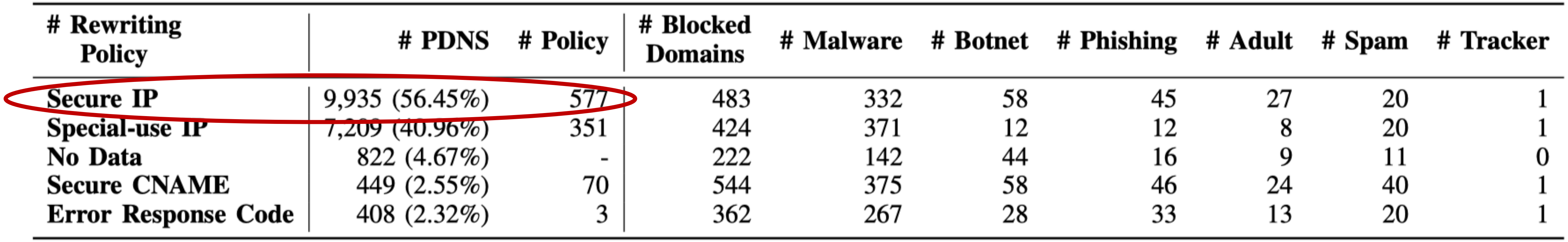
- **Secure IP** is the most prevalent policy, adopted by 56.45% of PDNSes



# Rewriting Policy	# PDNS	# Policy	# Blocked Domains	# Malware	# Botnet	# Phishing	# Adult	# Spam	# Tracker
Secure IP	9,935 (56.45%)	577	483	332	58	45	27	20	1
Special-use IP	7,209 (40.96%)	351	424	371	12	12	8	20	1
No Data	822 (4.67%)	-	222	142	44	16	9	11	0
Secure CNAME	449 (2.55%)	70	544	375	58	46	24	40	1
Error Response Code	408 (2.32%)	3	362	267	28	33	13	20	1

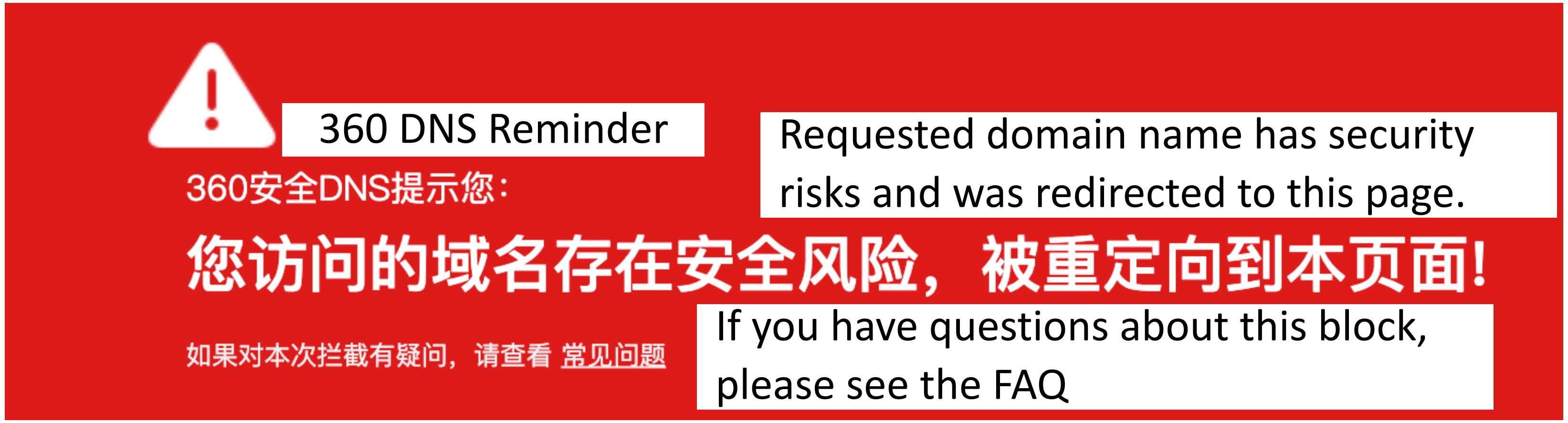
Finding 4: Rewriting Policies of PDNS

- **Secure IP** is the most prevalent policy, adopted by 56.45% of PDNSes



# Rewriting Policy	# PDNS	# Policy	# Blocked Domains	# Malware	# Botnet	# Phishing	# Adult	# Spam	# Tracker
Secure IP	9,935 (56.45%)	577	483	332	58	45	27	20	1
Special-use IP	7,209 (40.96%)	351	424	371	12	12	8	20	1
No Data	822 (4.67%)	-	222	142	44	16	9	11	0
Secure CNAME	449 (2.55%)	70	544	375	58	46	24	40	1
Error Response Code	408 (2.32%)	3	362	267	28	33	13	20	1

- **162 secure IPs (28%)** return block notification webpage, and 14 IPs provide avenues for user complaints



360 DNS Reminder

360安全DNS提示您：

Requested domain name has security risks and was redirected to this page.

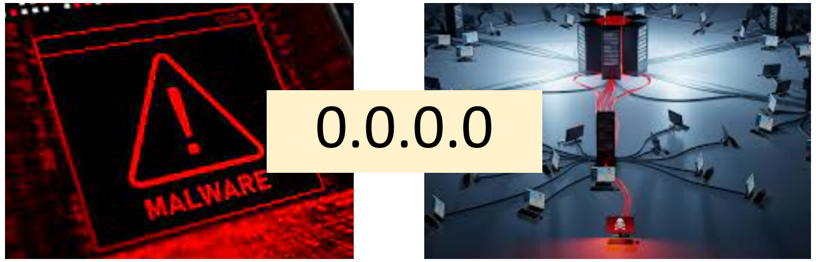
您访问的域名存在安全风险，被重定向到本页面!

如果对本次拦截有疑问，请查看 常见问题

If you have questions about this block, please see the FAQ

Finding 4: Rewriting Policies of PDNS

- **1,222 PDNSes** apply diverse rewriting policies per domain category



0.0.0.0

Malware

Botnet

Phishing

Spam

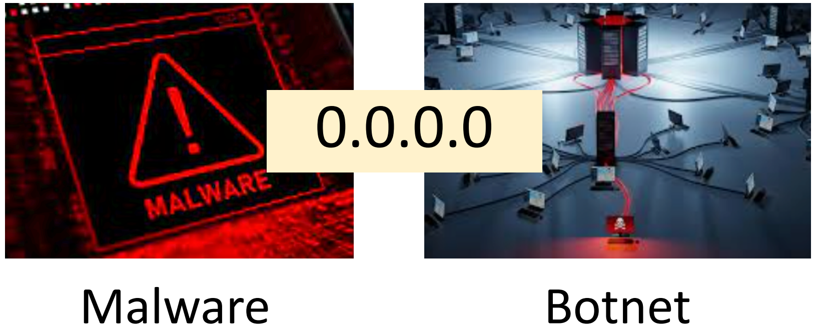
1.2.3.4

Tracker

Adult

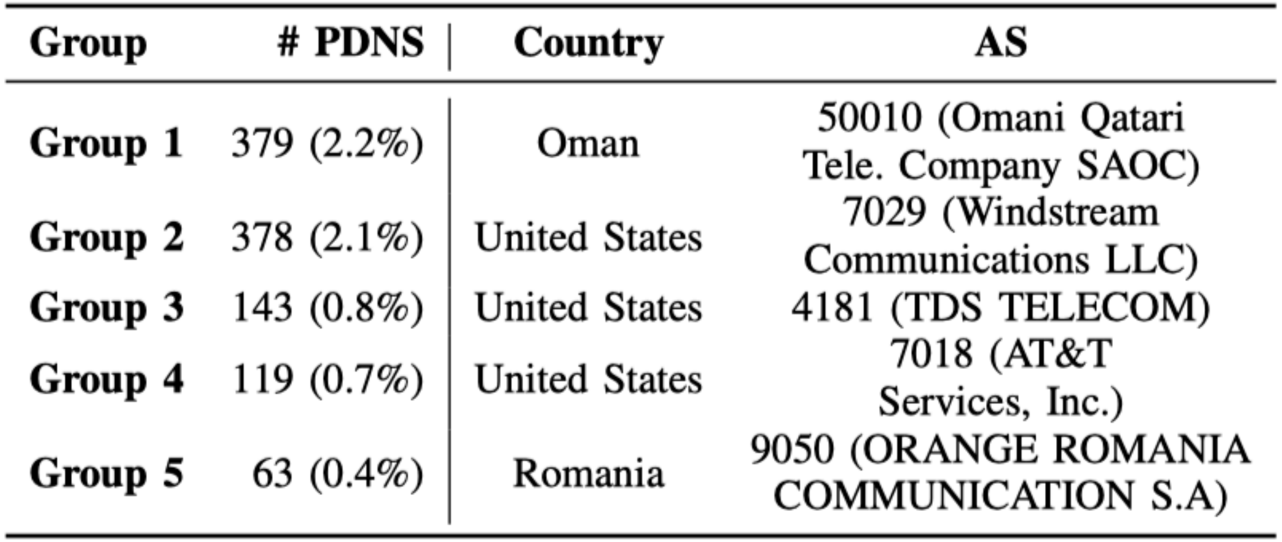
Finding 4: Rewriting Policies of PDNS

- **1,222 PDNSes** apply diverse rewriting policies per domain category



Phishing
Spam
1.2.3.4
Tracker
Adult
new leaks

- **PDNS groups** based on the same rewriting policies, with 12 groups having over 50 PDNS servers



Group	# PDNS	Country	AS
Group 1	379 (2.2%)	Oman	50010 (Omani Qatari Tele. Company SAOC)
Group 2	378 (2.1%)	United States	7029 (Windstream Communications LLC)
Group 3	143 (0.8%)	United States	4181 (TDS TELECOM)
Group 4	119 (0.7%)	United States	7018 (AT&T Services, Inc.)
Group 5	63 (0.4%)	Romania	9050 (ORANGE ROMANIA COMMUNICATION S.A)

Security Issues of PDNS

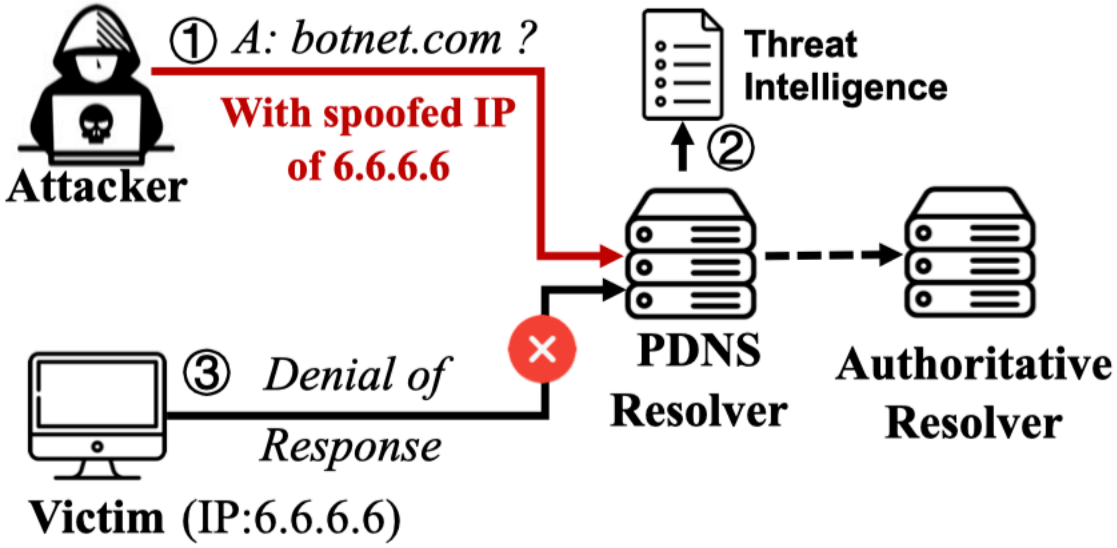
- **3 security risks** arising from flawed blocking strategy implementations
  - **Denial of Response (DoR)** due to aggressive non-responsive policies
  - **Dangling cloud IPs** susceptible to takeover and misuse by attackers
  - **Subversion of protective features** by multiple flawed blocking strategies implementations

Security Issue 1: Denial of Response (DoR)

- **822 PDNSes** employ No Data to block malicious domains
- **28 PDNSes** have DoR risk due to aggressive no-data response policies

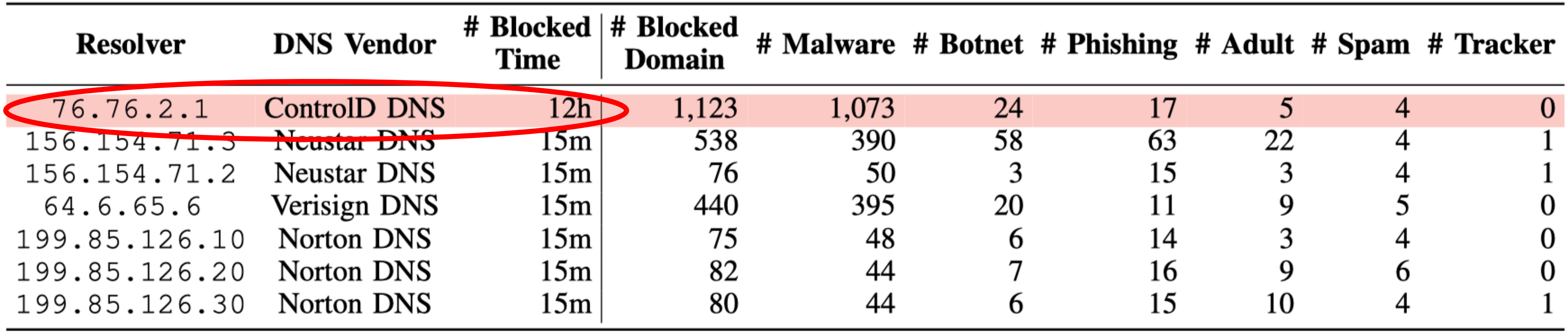
Security Issue 1: Denial of Response (DoR)

- **822 PDNSes** employ No Data to block malicious domains
- **28 PDNSes** have DoR risk due to aggressive no-data response policies
- Threat Model of DoR
  - Attackers can exploit this security issue of PDNS to deny DNS resolution services for arbitrary victims by spoofing the source IP address



Security Issue 1: Denial of Response (DoR)

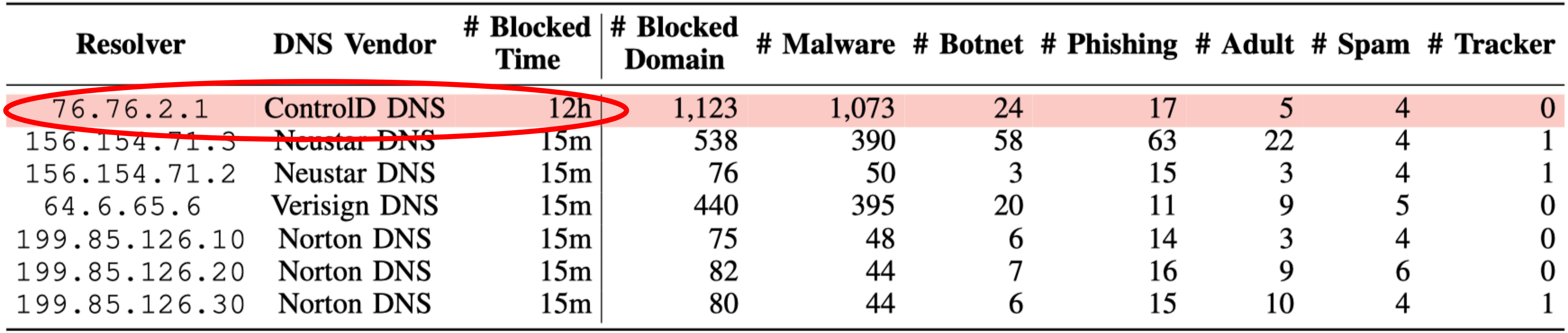
- **7 popular PDNS providers exhibit denial of response**, even blocking the resolution of popular domain names



Resolver	DNS Vendor	# Blocked Time	# Blocked Domain	# Malware	# Botnet	# Phishing	# Adult	# Spam	# Tracker
76.76.2.1	ControlD DNS	12h	1,123	1,073	24	17	5	4	0
156.154.71.3	Neustar DNS	15m	538	390	58	63	22	4	1
156.154.71.2	Neustar DNS	15m	76	50	3	15	3	4	1
64.6.65.6	Verisign DNS	15m	440	395	20	11	9	5	0
199.85.126.10	Norton DNS	15m	75	48	6	14	3	4	0
199.85.126.20	Norton DNS	15m	82	44	7	16	9	6	0
199.85.126.30	Norton DNS	15m	80	44	6	15	10	4	1

Security Issue 1: Denial of Response (DoR)

- **7 popular PDNS providers exhibit denial of response**, even blocking the resolution of popular domain names



Resolver	DNS Vendor	# Blocked Time	# Blocked Domain	# Malware	# Botnet	# Phishing	# Adult	# Spam	# Tracker
76.76.2.1	ControlD DNS	12h	1,123	1,073	24	17	5	4	0
156.154.71.3	Neustar DNS	15m	538	390	58	63	22	4	1
156.154.71.2	Neustar DNS	15m	76	50	3	15	3	4	1
64.6.65.6	Verisign DNS	15m	440	395	20	11	9	5	0
199.85.126.10	Norton DNS	15m	75	48	6	14	3	4	0
199.85.126.20	Norton DNS	15m	82	44	7	16	9	6	0
199.85.126.30	Norton DNS	15m	80	44	6	15	10	4	1

DoR attack leads to a response denial lasting up to 12 hours

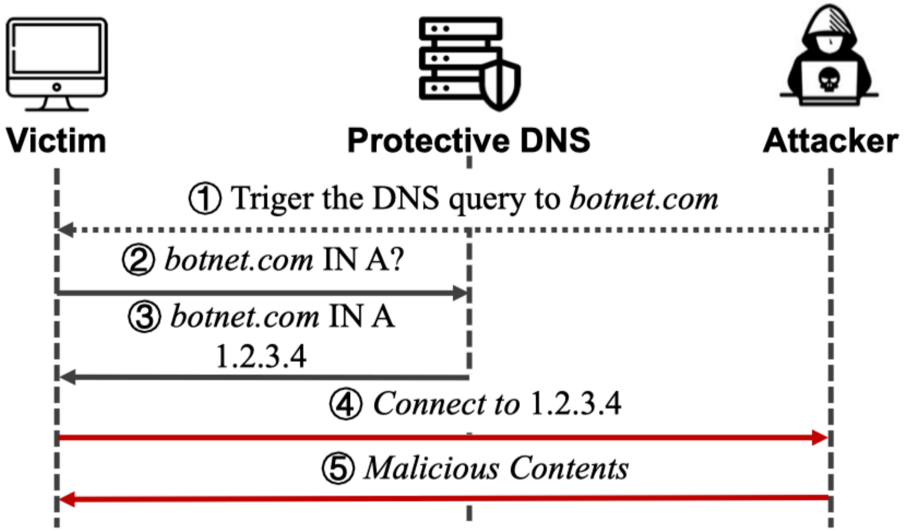
Security Issue 2: Dangling PDNS Infrastructure

- **Dangling PDNS Infrastructure** susceptible to takeover and misuse by attackers, caused by not-in-use IPs (Dare resources)

[CCS'16] All your dns records point to us: Understanding the security threats of dangling dns records

Security Issue 2: Dangling PDNS Infrastructure

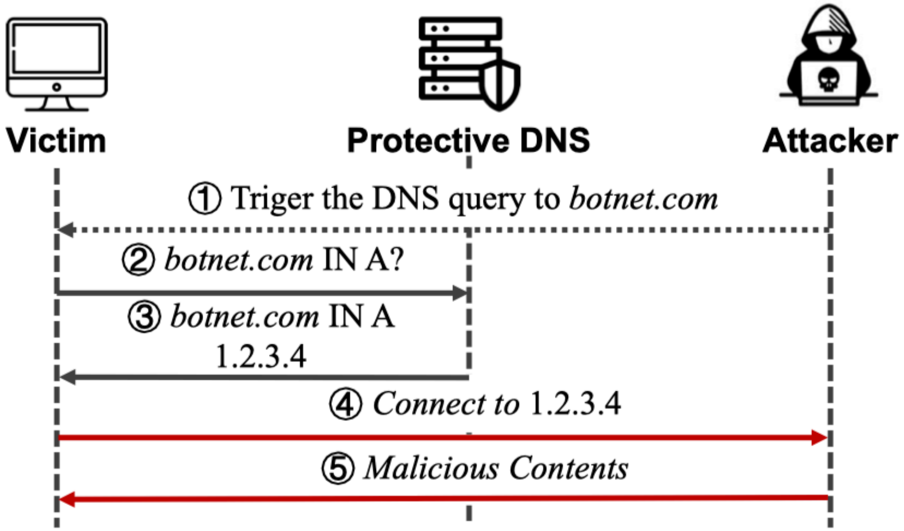
- **Dangling PDNS Infrastructure** susceptible to takeover and misuse by attackers, caused by not-in-use IPs (Dare resources)
- Threat Model of Dangling: Takeover threats
  - The potential takeover and abuse of a PDNS's security-orientated policy by a third-party adversary could pose serious security implications.



[CCS'16] All your dns records point to us: Understanding the security threats of dangling dns records

Security Issue 2: Dangling PDNS Infrastructure

- **Dangling PDNS Infrastructure** susceptible to takeover and misuse by attackers, caused by not-in-use IPs (Dare resources)
- Threat Model of Dangling: Takeover threats
  - The potential takeover and abuse of a PDNS's security-orientated policy by a third-party adversary could pose serious security implications.



7 obsolete cloud IPs employed by 21 PDNSes

[CCS'16] All your dns records point to us: Understanding the security threats of dangling dns records

Security Issue 3: Subversion of Protective Features

- **Subversion of protective features** by multiple flawed blocking strategies implementations

Security Issue 3: Subversion of Protective Features

- **Subversion of protective features** by multiple flawed blocking strategies implementations

- Flawed Implementations of PDNS
  - **105 PDNSes** return both forged (e.g., 127.42.0.148) and authoritative answers for malicious domain queries

Security Issue 3: Subversion of Protective Features

- **Subversion of protective features** by multiple flawed blocking strategies implementations

- Flawed Implementations of PDNS
  - **105 PDNSes** return both forged (e.g., 127.42.0.148) and authoritative answers for malicious domain queries

- Non-configured Query Types of PNDS
  - **13 PDNSes** return original resolution results for types that are not configured with blocking measures, e.g., TXT records

Recommendation for PDNS Implementation

Recommendation for PDNS Implementation

Transparent Blocking Activity: setting up a webpage to inform users of block reasons (e.g., Malware domain) and providing complaint channels (e.g., email)

Recommendation for PDNS Implementation

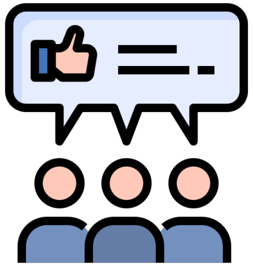
Transparent Blocking Activity: setting up a webpage to inform users of block reasons (e.g., Malware domain) and providing complaint channels (e.g., email)

Utilizing safe rewriting infrastructures: exercising increased caution when utilizing third-party resources like cloud IPs and sinkhole domains

Recommendation for PDNS Implementation

Transparent Blocking Activity: setting up a webpage to inform users of block reasons (e.g., Malware domain) and providing complaint channels (e.g., email)

Utilizing safe rewriting infrastructures: exercising increased caution when utilizing third-party resources like cloud IPs and sinkhole domains



Defense of denial of response: forcing the client to use DNS over TCP, in response to clients issuing numerous DNS queries for malicious domains

Summary

Identifying DNS Methodology

- We design and implement the **first identification methodology for PDNS**, which can distinguish PDNS from other DNS manipulations
- Open-source scripts: https://github.com/MingxuanLiu/ProtectiveDNS

Understanding of PDNS Ecosystem

- We present the first active measurement study on the emerging PDNS ecosystem and find **17,601 open PDNS servers**, and comprehensively understand their operational status

Security analysis of PDNS infrastructure

- We first discover **three types of security flaws within PDNS operation**, which enable evasion of security protection and denial of service, and report them to affected vendors and get their positive responses

Providing recommendations for PDNS implementation

Understanding the Implementation and Security Implications of Protective DNS Services

Mingxuan Liu, **Yiming Zhang**, Xiang Li, Chaoyi Lu,

Baojun Liu, Haixin Duan, Xiaofeng Zheng

Email: liumx@mail.zgclab.edu.cn

https://github.com/MingxuanLiu/ProtectiveDNS

NDSS SYMPOSIUM/2024