



One Char to Rule Them All: Systematically Exploring and Exploiting DNS Silent Vulnerabilities in Domain Name Resolution

Fasheng Miao, Xiang Li, Changqing An, Jilong Wang

Presenter: **Fasheng Miao**, Tsinghua University

mfs24@mails.tsinghua.edu.cn



Fasheng Miao

Master Student, Tsinghua University

Fasheng Miao, a second-year master's student at Tsinghua University, specializes in AI Security and vulnerability exploitation and discovery in real-world internet environments. He has published papers at top cybersecurity conferences, including IEEE S&P, ACM CCS, and ACM IMC, and has been assigned 24 CVE identifiers. He also won the championship in the DAF track at GeekCon·New Geekpwn 2025.

Homepage: <https://www.miaofs18.top/>

Silent Vulnerability

For specific DNS queries, the resolver remains silent and provides no response to downstream resolvers

Shar Attack

Attack Impact

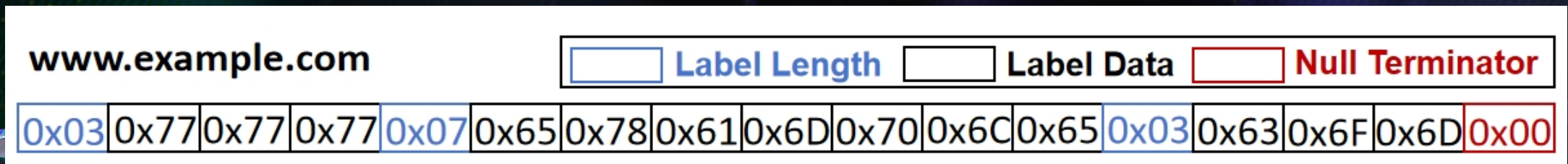
- The SHAR attack exposes the silent vulnerabilities, leaving all 31 tested mainstream DNS software implementations vulnerable to cache poisoning and load balancing disruption.
- SHAR attack compromises all tested Wi-Fi routers, router OSes, public DNS services, 531.1K open resolvers, 522 TLDs, and 12.5M domain names, enabling domain takeover, full TLD hijacking, and persistent DoS.
- SHAR attack enhances 10 out of 13 classic off-path DNS cache poisoning attacks.

One vulnerability, multiple attack impacts

Shar Attack

Domain Name

- Domain names are human-friendly Internet identifiers for easy memorization, such as Web and Email.
- Domain names consist of labels, and characters are the basic building blocks of labels.



Shar Attack

Domain Name Character Set

- RFC 1035 specifies that domain names may only contain letters, digits, and hyphens.
- RFC 2181 states that implementations *"must not place any restrictions on label content"*

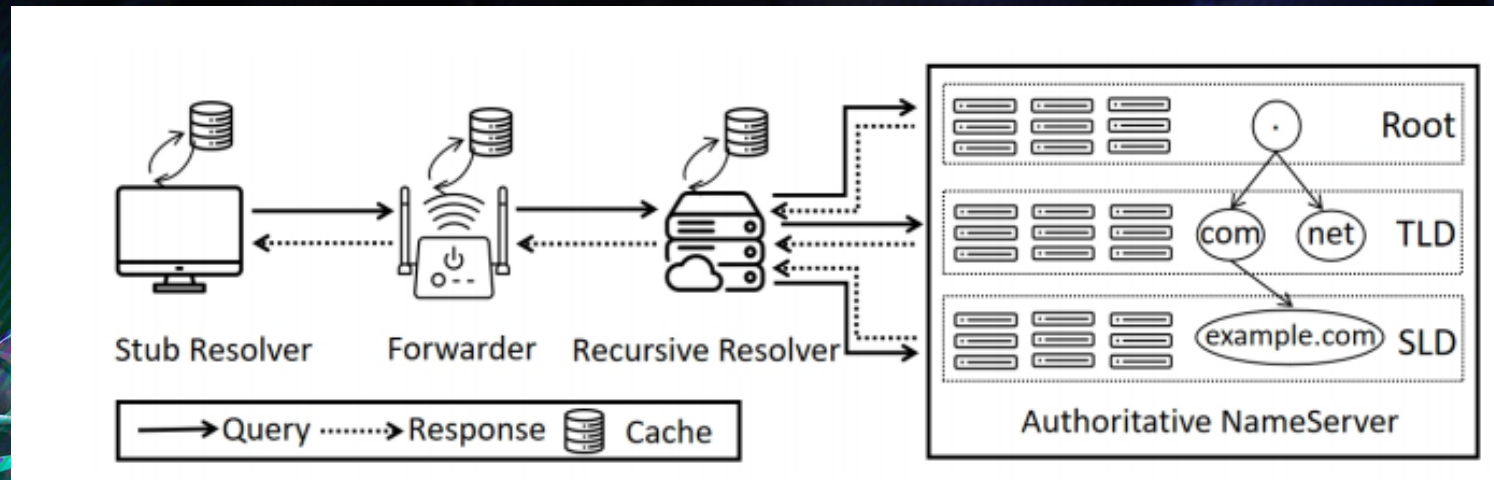
Inconsistencies exist in the specifications for characters allowed in domain names.

Shar Attack

Domain Name System (DNS)

- **DNS Overview**

- Translates human-readable domain names to machine-readable IP addresses.
- DNS consists of multiple components, including stub resolvers, forwarders, recursive resolvers, and authoritative servers.



Different components may exhibit inconsistent support for characters

Shar Attack

Takeaway

- The character specifications for domain names in RFC documents are inconsistent.
- DNS comprises multiple components, which may show inconsistent support for characters in domain names.

Shar Attack

Question

What is the state of character support across real-world software and services, and what handling logic is employed for unsupported characters?

Characters are fundamental to DNS. Yet, since its introduction 40 years ago, no systematic measurement has been conducted to evaluate real-world support for characters in domain names.

Shar Attack

Test Methodology

- We analyzed DNS character handling via source code review, GDB debugging for open-source software, and empirical testing for closed-source systems.
- We performed measurements using queries in the format {char}.{nonce}.attacker.com on our controlled nameserver and captured all DNS packets.
- In this work, we comprehensively examine the entire ASCII character set (0x00–0x7F), and treat all non-alphanumeric characters (beyond a–z, A–Z, 0–9) as special characters.

Shar Attack

Test Result

- Character support varies significantly across different software implementations.

Resolver		Characters		Response Result		
Actor	Software	Unsupported	Support	Unsupported	Support	Status
Recursive Resolver	BIND	0	65(All)	-	x	-
	Unbound	0	65(All)	-	x	-
	PowerDNS	0	65(All)	-	√	Servfail
	Knot Resolver	0	65(All)	-	√	Servfail
	Microsoft DNS	0	65(All)	-	x	-
	Technitium DNS	62	3	√	√	Servfail
	Simple DNS Plus	0	65(All)	-	x	-
	MaraDNS	33	32	x	x	-
	HickoryDNS	0	65(All)	-	x	-

Shar Attack

Test Result

Resolver		Characters		Response Result		
Actor	Software	Unsupported	Support	Unsupported	Support	Status
Forwarder	Dnsmasq	0	65(All)	-	x	-
	CoreDNS	0	65(All)	-	√	Servfail
	DNSSDist	0	65(All)	-	x	-
	SmartDNS	2	63	√	√	Servfail
	Pi-hole	0	65(All)	-	x	-
	Pdnsd	0	65(All)	-	√	Servfail
	Acrylic DNS	0	65(All)	-	x	-
	AdGuard	0	65(All)	-	x	-
	AdGuard Home	0	65(All)	-	x	-
	DNS Safety	0	65(All)	-	√	Servfail
	Dual DHCP DNS	0	65(All)	-	x	-
	Nxfilter	0	65(All)	-	x	-
	YogaDNS	0	65(All)	-	x	-

Shar Attack

Test Result

Resolver		Characters		Response Result		
Actor	Software	Unsupported	Support	Unsupported	Support	Status
Stub Resolver	Linux	0	65(All)	-	✓	NXDomain
	Windows	0	65(All)	-	x	-
	MacOS	0	65(All)	-	x	-
	iOS	0	65(All)	-	x	-
	Android	0	65(All)	-	x	-
	ChromeOS	64	1	x	x	-
DNS Library	Python	0	65(All)	-	x	-
	Golang	0	65(All)	-	x	-
	JavaScript	60	5	✓	x	-
	Java	0	65(All)	-	✓	Network Error

Shar Attack

Question

What potential exploits may arise from these inconsistencies and silent vulnerabilities?

Shar Attack

- **What is the Shar Attack**

- By exploiting special characters to trigger silent vulnerabilities, named Shar (Special Characters) Attack.
- A new set of powerful DNS-related attacks.
 - Attack-1(V_{EN}) : Enhance classic off-path DNS cache poisoning attacks
 - Attack-2(V_{BF}) : DNS cache poisoning
 - Attack-3(V_{LB}) : DNS load balancing disruption
 - Attack-4(V_{SF}) : Persistent DoS
- One vulnerability, multiple attack impacts

- **List of Vulnerable Entities**

- 31 mainstream DNS software
- 21 Wi-Fi routers, 6 router operating systems
- 43 public DNS services
- 531,100 (60.1%) open DNS resolvers
- 522 (36.1%) TLDs and 12.5 million domains (5.6%)

Shar Attack

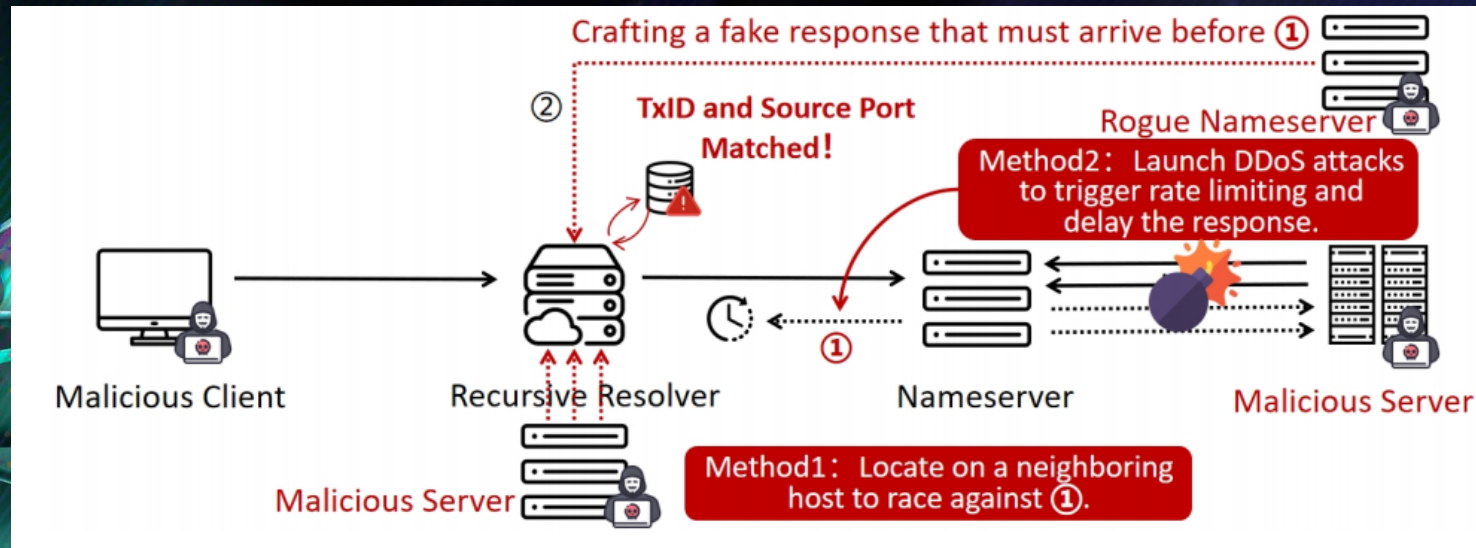
Attack-1 (V_{EN})

- **Core Insight**

- DNS cache poisoning relies on racing against legitimate nameservers
- Shar Attack forces nameservers to be silent.
- It assists and strengthens traditional DNS attacks.

- **Target**

- Stub resolver, forwarder, recursive resolver



Shar Attack

Attack-1 (V_{EN})

- Enhance 10/13 Well-known DNS cache poisoning attacks

Resolver		Response Result			Can Be Enhanced
Work	Year	Stub	Forwarder	Recursive	
[79]	2002	x	x	✓	✓
[41]	2008	x	x	✓	✓
[82]	2010	x	x	✓	✓
[31]	2012	x	x	✓	✓
[32]	2013	x	✓	✓	x
[33]	2013	✓	x	✓	✓
[81]	2014	✓	x	✓	x
[89]	2020	x	✓	x	x
[60]	2020	✓	✓	✓	✓
[61]	2021	✓	✓	✓	✓
[30]	2023	✓	✓	✓	✓
[54]	2023	x	x	✓	✓
[56]	2024	✓	✓	✓	✓

Shar Attack

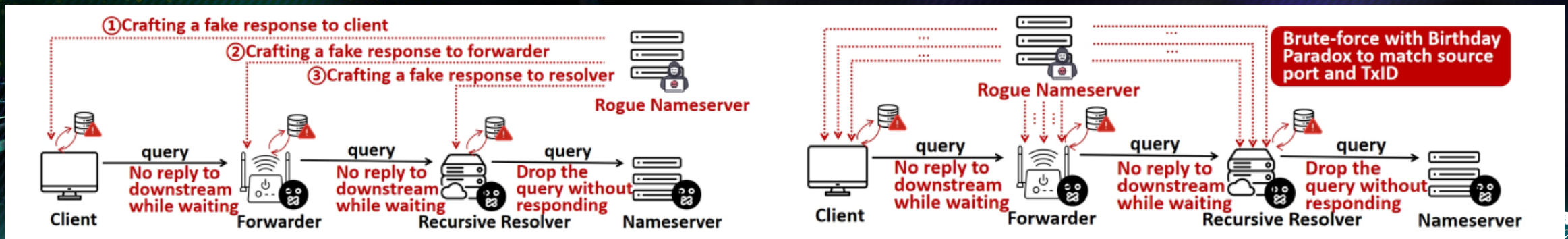
Attack-2 (V_{BF})

Core Insight

- DNS relies on 16-bit TxID + 16-bit port, giving a 32-bit guessing space
- Brute-force is thought impractical due to a narrow 80–100ms window
- V_{BF} silences upstream resolvers/nameservers, extending the waiting timeout (e.g., 5s) and significantly widening the brute-force spoofing window
- V_{BF} revives feasible TxID/port brute-force, long considered infeasible since 2008

Target

- Stub resolver, forwarder, recursive resolver



Shar Attack

Attack-2 (V_{BF})

- **All 20 trials achieved success within a controllable timeframe, which had been considered impossible since 2008.**

Resolver		Avg. Round Taken	Avg. Time Taken (s)	Success Rate
Work	Year			
[79]	2002	7,532	8,687	20/20
[41]	2008	7,947	9,469	20/20
[82]	2010	7,282	9,717	20/20

- **List of Vulnerable Entities**
 - 31 mainstream DNS software
 - 21 Wi-Fi routers, 6 router operating systems
 - 43 public DNS services

Shar Attack

Attack-3 (V_{LB}) & Attack-4 (V_{SF})

- **Core Insight**

- Recursive resolvers favor responsive nameservers and avoid unresponsive ones
- SHAR uses a single special character to silence authoritative nameservers and reduce their priority, thereby performing load balancing disruption attacks with two variants: V_{LB} and V_{SF}
- V_{LB} concentrates traffic on a single nameserver, causing overload and reduced resilience.
- V_{SF} marks all nameservers as faulty, making resolvers return Servfail directly to clients.
- Both attacks bypass DoS defenses, lower the barrier for hijacking and cache poisoning, and fully break domain resolution.

Shar Attack

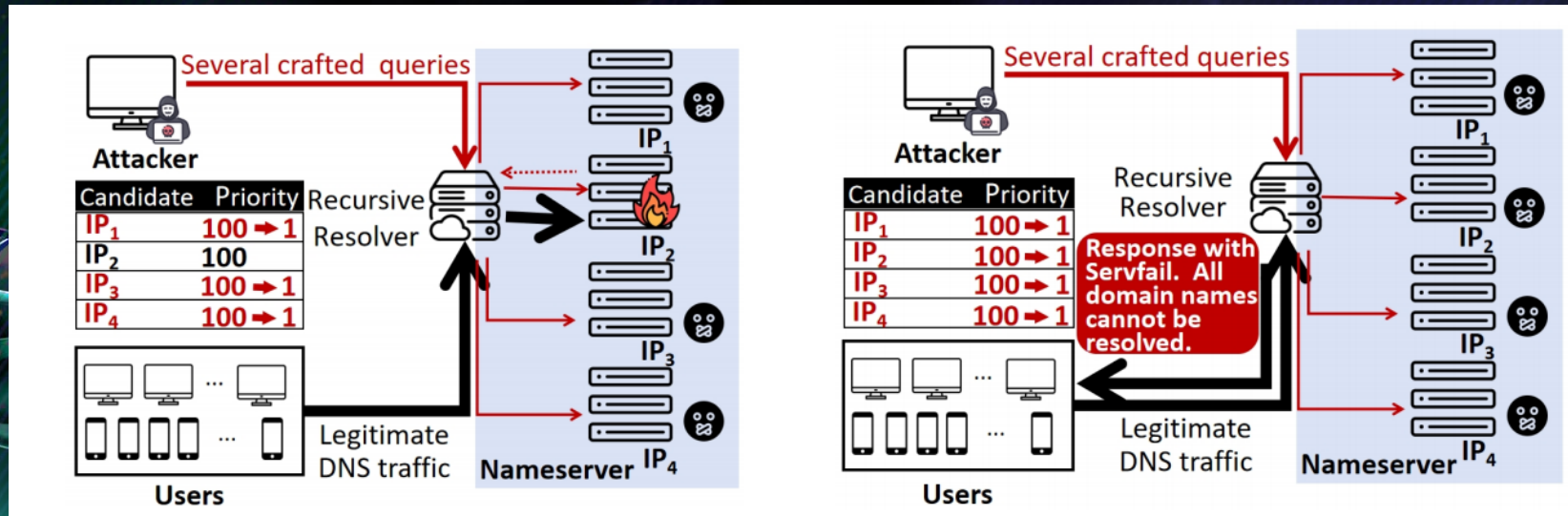
Attack-3 (V_{LB}) & Attack-4 (V_{SF})

- **Attack Model**

- Attack-3 (V_{LB}): Resolvers prefer well-performing nameservers and downgrade the priority of unresponsive ones
- Attack-4 (V_{SF}): Resolvers only query operational nameservers to obtain resources

- **Target**

- Recursive resolver and nameserver



Shar Attack

Attack-3 (V_{LB}) & Attack-4 (V_{SF})

- 4 mainstream DNS software Vulnerable

Recursive Resolver	V_{LB} Impact			V_{SF} Impact		
	SLD	TLD	ALL	SLD	TLD	ALL
BIND	✓	✓	✓	✗	✗	✗
Unbound	✓	✗	✗	✓	✗	✗
Knot	✓	✓	✓	✗	✗	✗
PowerDNS	✓	✓	✓	✓	✓	✓
Microsoft	✗	✗	✗	✗	✗	✗
Simple DNS Plus	✗	✗	✗	✗	✗	✗
Technitium	✓	✓	✓	✗	✗	✗
MaraDNS	✗	✗	✗	✗	✗	✗

- List of Vulnerable Entities

- 25 Public DNS Services vulnerable to V_{LB}
- 16 Public DNS Services vulnerable to V_{SF}

Shar Attack

Takeaway

One vulnerability can lead to 4 attack impacts. Even the most basic characters may carry potential security risks, yet they have not received systematic and sufficient attention.

One vulnerability, multiple attack impacts

Shar Attack

Question

What is the real-world impact of the Shar Attack?

**WIFI Router, Route OS, Public DNS Services,
and Domain Names**

Shar Attack

Vulnerable Wi-Fi Routers and OSes

- 21/21 WI-FI Router and 6/6 Router OSes

Resolver		Characters		Response Result			Vulnerability
Actor	Software	Unsupported	Support	Unsupported	Support	Status	
WI-FI Router	360 WI-FI6 T7	0	65(All)	-	x	-	✓
	ASUS RT-AC66U	0	65(All)	-	x	-	✓
	CISCO Router	0	65(All)	-	x	-	✓
	D-Link 7001	1	64	x	x	-	✓
	Fast FAC1200R	0	65(All)	-	x	-	✓
	Fiberhome SR4201SA	0	65(All)	-	x	-	✓
	H3C Magie NX15	0	65(All)	-	x	-	✓
	Honor X4 Pro	0	65(All)	-	x	-	✓
	Huawei AX3	33	32	x	x	-	✓
	iKuai IK-Q3600	0	65(All)	-	x	-	✓
	Linksys	1	64	-	x	-	✓
	Mereury D191G	0	65(All)	-	x	-	✓
	Netgenr AX5	0	65(All)	-	x	-	✓

Shar Attack

Vulnerable Wi-Fi Routers and OSes

- 21/21 WI-FI Router and 6/6 Router OSer

Resolver		Characters		Response Result			Vulnerability
Actor	Software	Unsupported	Support	Unsupported	Support	Status	
WI-FI Router	PGY X4C-5131G	0	65(All)	-	x	-	✓
	Redmi AX3000	0	65(All)	-	x	-	✓
	Skyworth WR9651X	1	64	-	x	-	✓
	Tenda V1	0	65(All)	✓	x	-	✓
	TP-Link XDR3230	0	65(All)	-	x	-	✓
	TP-Link XDR5430	0	65(All)	-	x	-	✓
	Xiaomi 4C	0	65(All)	-	x	-	✓
	ZTE E2633	0	65(All)	-	x	-	✓
Router OS	DD-WRT	0	65(All)	-	x	-	✓
	Gargoyle	0	65(All)	-	x	-	✓
	iKuai OS	0	65(All)	-	x	-	✓
	libreCMC	0	65(All)	-	x	-	✓
	Openwrt	0	65(All)	-	x	-	✓
	RouterOS	0	65(All)	-	✓	Servfail	✓

Shar Attack

Vulnerable Public DNS Services

All (43/43) public DNS services are affected by at least one attack variant.

Shar Attack

Vulnerable Domain Names

- **522 (36.1%) TLDs**

Variety	Num	>10%	>25%	>50%	>75%	>100%
ccTLD	236	95	58	17	5	4
IDN TLD	151	75	52	23	3	2
gTLD	1,058	727	598	482	1	1
Total (Num)	1,445	897	708	522	9	7
Total (%)	100.0%	62.1%	49.0%	36.1%	0.6%	0.5%

Fraction of vulnerable nameservers per TLD

- **12.5M(5.6%) Domain Names**

Total Num	TLDScope	SLD-NScope	Total Vulnerable
223.6M	11.4M(5.1%)	1.2M(0.5%)	12.5M(5.6%)

TLDScope: Identified by TLD with over 50% NS vulnerable.

SLD-NScope: Identified by SLD with over 50% NS vulnerable

Shar Attack

Core Contributions

- We provided an in-depth analysis of special characters handling logic across all DNS roles.
- We discovered two novel logic vulnerabilities caused by the inconsistent and silent handling logic of special characters.
- Based on these vulnerabilities, we propose two classes of attacks (four variants), named SHAR attack, which can attack all DNS roles and enhance previous DNS cache poisoning attacks.
- We conducted comprehensive experiments to evaluate the real-world impact of the SHAR attack.

Shar Attack

Discussion & Mitigation

- **Lessons Learned**
 - Special character handling is critical to DNS security.
 - SHAR exploits silent query dropping, creating an exploitable time window for attacks.
 - Many real-world DNS servers (TLDs, SLDs, major clouds) silently drop unsupported characters.
- **Root Cause**
 - Inconsistency between RFC 1034 and RFC 2181 on allowed characters
- **Mitigation Solution**
 - Follow latest RFCs and support all valid characters
 - Deploy 0x20 encoding and DNSSEC to prevent cache poisoning.
 - Use anomaly detection and rate limiting to block spoofed responses.
 - Resolvers should periodically probe low-priority nameservers to mitigate load balancing disruption.

Shar Attack

Wrap-up

Thanks for listening!
Any question?

Fasheng Miao

Tsinghua University

mfs24@mails.tsinghua.edu.cn

<https://www.miaofs18.top>