Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers

Fenglu Zhang, Baojun Liu, Eihal Alowaisheq, Jianjun Chen, Chaoyi Lu, Linjian Song, Yong Ma, Ying Liu, Haixin Duan and Min Yang

Requirement of load balancing on authoritative DNS servers

To improve security and robustness, DNS specifications require deploying a load balancing mechanism on authoritative DNS servers:

RFC 1034: “By administrative fiat, we REQUIRE every zone to be available on at least two servers, and many zones have more redundancy than that.”

RFC 2182: “Secondary servers (Authoritative servers) MUST be placed at both topologically and geographically dispersed locations on the Internet.”

DNS hosting in cloud services

- Providing infrastructure to resolve the DNS query for hosted domains
- Providing a user-friendly UI to help manage hosted domains

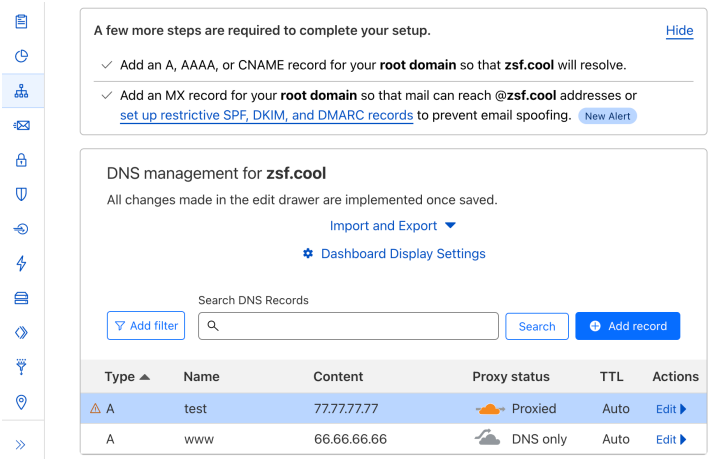
CLOUDFLARE

aws

Alibaba Cloud

DNSPOD

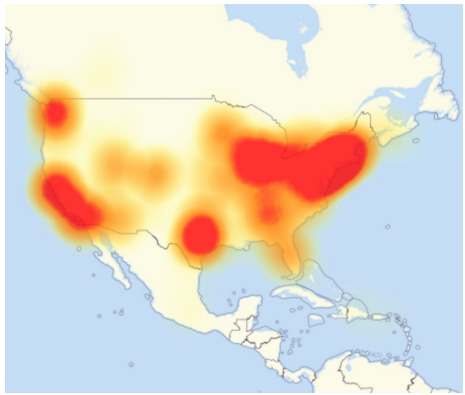
Some vendors of DNS hosting services



The user-friendly UI provided by a DNS hosting service

Numerous domains are sharing a DNS hosting service

- Numerous domains are sharing the same nameservers of a hosting provider.
- Load balancing is critical to the stability and security of DNS hosting services



BBC CNN GitHub PayPal amazon.com

The users and some popular domains affected by DDoS attack on Dyn in Oct 2016

Our study: Disablance (DNS Load Balancing Disabler)

Uncovered a new attack (Disablance) that disrupts the load balancing mechanism of a kind of non-compliant authoritative DNS servers

Our study: Disablance (DNS Load Balancing Disabler)

Uncovered a new attack (Disablance) that disrupts the load balancing mechanism of a kind of non-compliant authoritative DNS servers

- **Exploitable recursive DNS software**
  - BIND9, PowerDNS, and Microsoft DNS

Our study: Disablance (DNS Load Balancing Disabler)

Uncovered a new attack (Disablance) that disrupts the load balancing mechanism of a kind of non-compliant authoritative DNS servers

- **Exploitable recursive DNS software**
  - BIND9, PowerDNS, and Microsoft DNS
- **Exploitable domains**
  - 22.24% of the top 1M SecRank FQDNs
  - 3.94% of the top 1M Tranco SLDs

Our study: Disablance (DNS Load Balancing Disabler)

Uncovered a new attack (Disablance) that disrupts the load balancing mechanism of a kind of non-compliant authoritative DNS servers

- **Exploitable recursive DNS software**
  - BIND9, PowerDNS, and Microsoft DNS
- **Exploitable domains**
  - 22.24% of the top 1M SecRank FQDNs
  - 3.94% of the top 1M Tranco SLDs
- **Exploitable open resolvers**
  - 37.88% of selected open resolvers
  - 10 popular public DNS services, including Cloudflare and Quad9

Security impacts of disrupting DNS Load Balancing

Security impacts of disrupting DNS Load Balancing

Bypassing DoS defense mechanisms and overloading nameservers

- Redirecting legitimate DNS traffic to a specified target and no malicious traffic can be filtered
- Bypassing defense mechanisms against traditional DoS attacks [1-3]

Security impacts of disrupting DNS Load Balancing

Bypassing DoS defense mechanisms and overloading nameservers

- Redirecting legitimate DNS traffic to a specified target and no malicious traffic can be filtered
- Bypassing defense mechanisms against traditional DoS attacks [1-3]

Lowering the bar of traffic hijacking and cache poisoning

- Eliminating the possibility for clients to query diverse nameservers
- DNS manipulation becomes less challenging since a unique path is dedicated to victims [4]

Security impacts of disrupting DNS Load Balancing

Bypassing DoS defense mechanisms and overloading nameservers

- Redirecting legitimate DNS traffic to a specified target and no malicious traffic can be filtered
- Bypassing defense mechanisms against traditional DoS attacks [1-3]

Lowering the bar of traffic hijacking and cache poisoning

- Eliminating the possibility for clients to query diverse nameservers
- DNS manipulation becomes less challenging since a unique path is dedicated to victims [4]

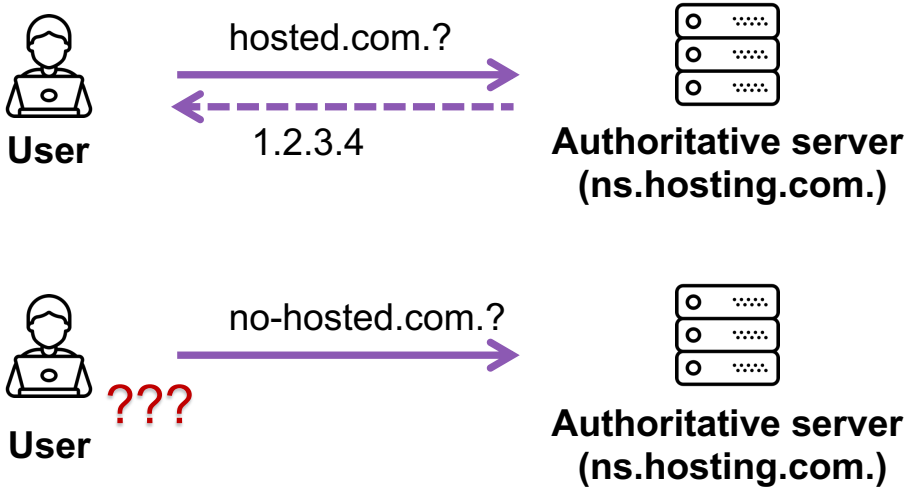
Disrupting the infrastructure of DNS-based load balancing systems

- One may directly configure each authoritative server to respond with different resource record sets.
- The attack against DNS load balancing can also have a subsequent impact on upper infrastructure

The Disablance Attack

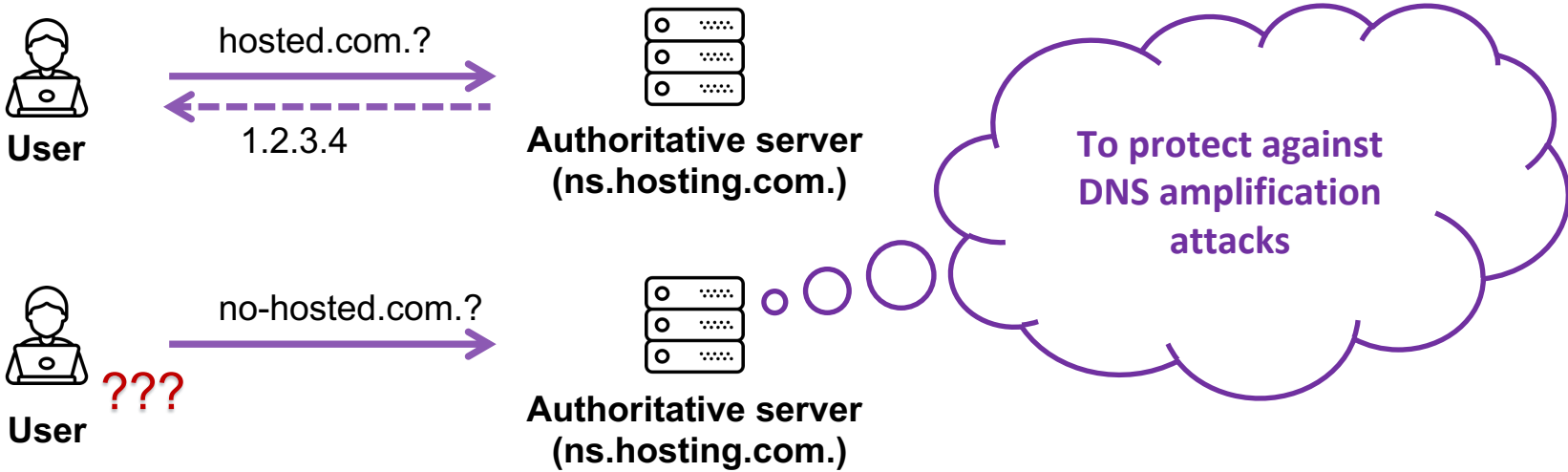
“Silence is golden”: a strategy of authoritative servers

Extensive authoritative servers are configured to **not respond** to DNS requests which are **outside of their authority**



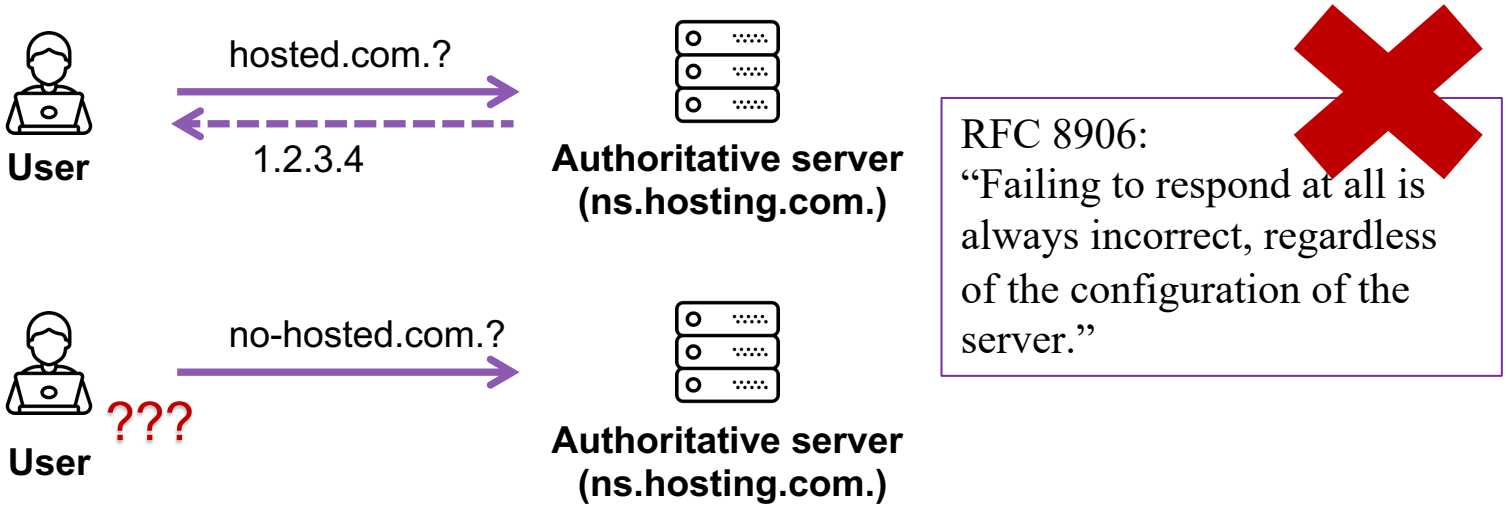
“Silence is golden”: a strategy of authoritative servers

Extensive authoritative servers are configured to **not respond** to DNS requests which are **outside of their authority**



“Silence is golden”: a strategy of authoritative servers

Extensive authoritative servers are configured to **not respond** to DNS requests which are **outside of their authority**

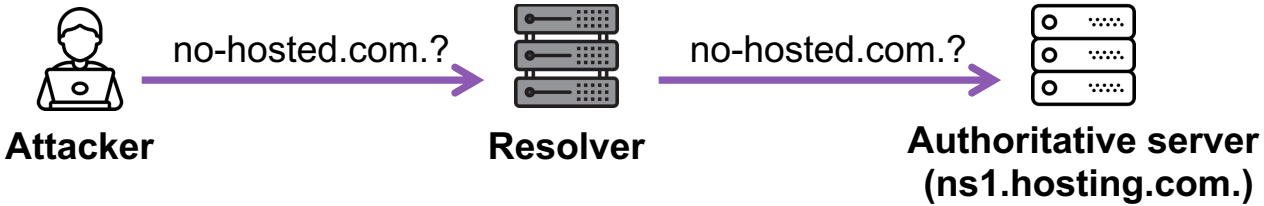


While resolvers meeting a “silence” authoritative server

- Recursive DNS software **prefers** the nameserver with the best performance
- Recursive DNS software **avoids** the nameserver failed to response
- The status of nameserver is globally shared by all domains.

While resolvers meeting a “silence” authoritative server

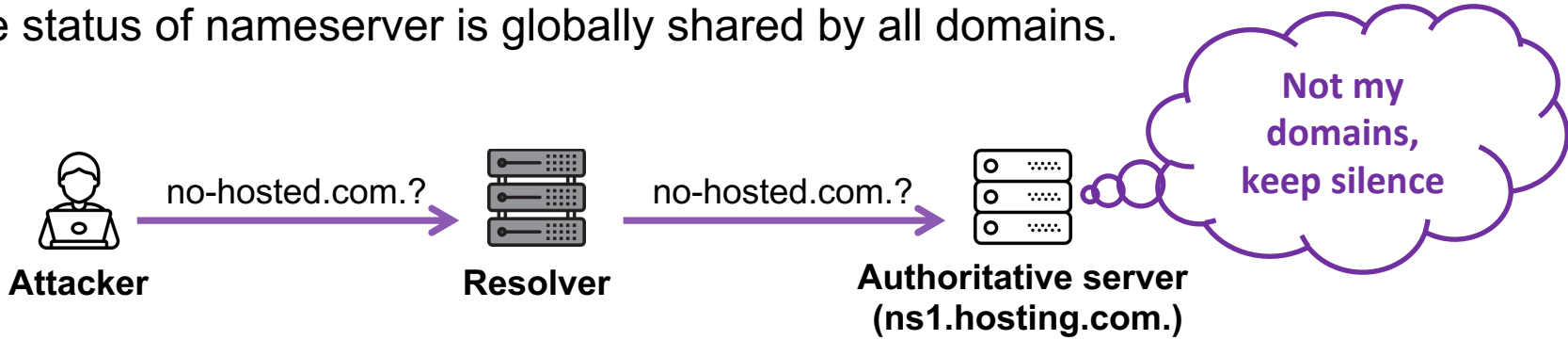
- Recursive DNS software **prefers** the nameserver with the best performance
- Recursive DNS software **avoids** the nameserver failed to response
- The status of nameserver is globally shared by all domains.



candidate	priority
ns1.hosting.com	100
ns2.hosting,com	100

While resolvers meeting a “silence” authoritative server

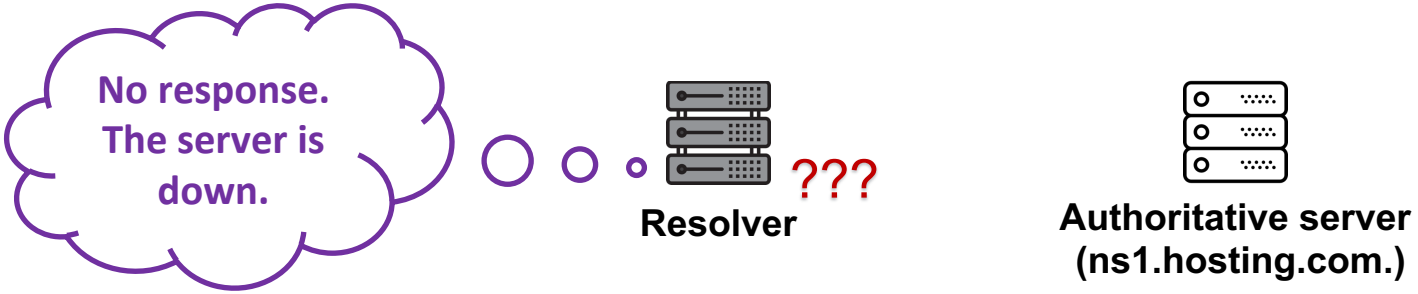
- Recursive DNS software **prefers** the nameserver with the best performance
- Recursive DNS software **avoids** the nameserver failed to response
- The status of nameserver is globally shared by all domains.



candidate	priority
ns1.hosting.com	100
ns2.hosting,com	100

While resolver meeting a “silence” authoritative server

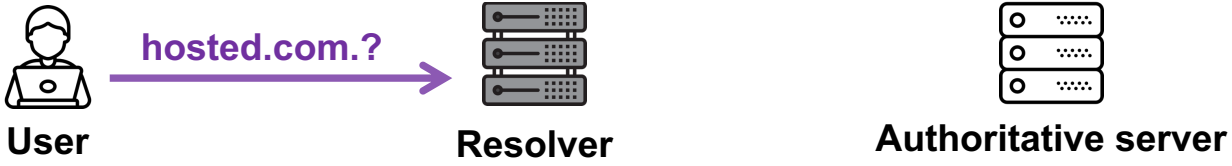
- Recursive DNS software **prefers** the nameserver with the best performance
- Recursive DNS software **avoids** the nameserver failed to response
- The status of nameserver is globally shared by all domains.



candidate	priority
ns1.hosting.com	100 -> 1
ns2.hosting,com	100

While resolver meeting a “silence” authoritative server

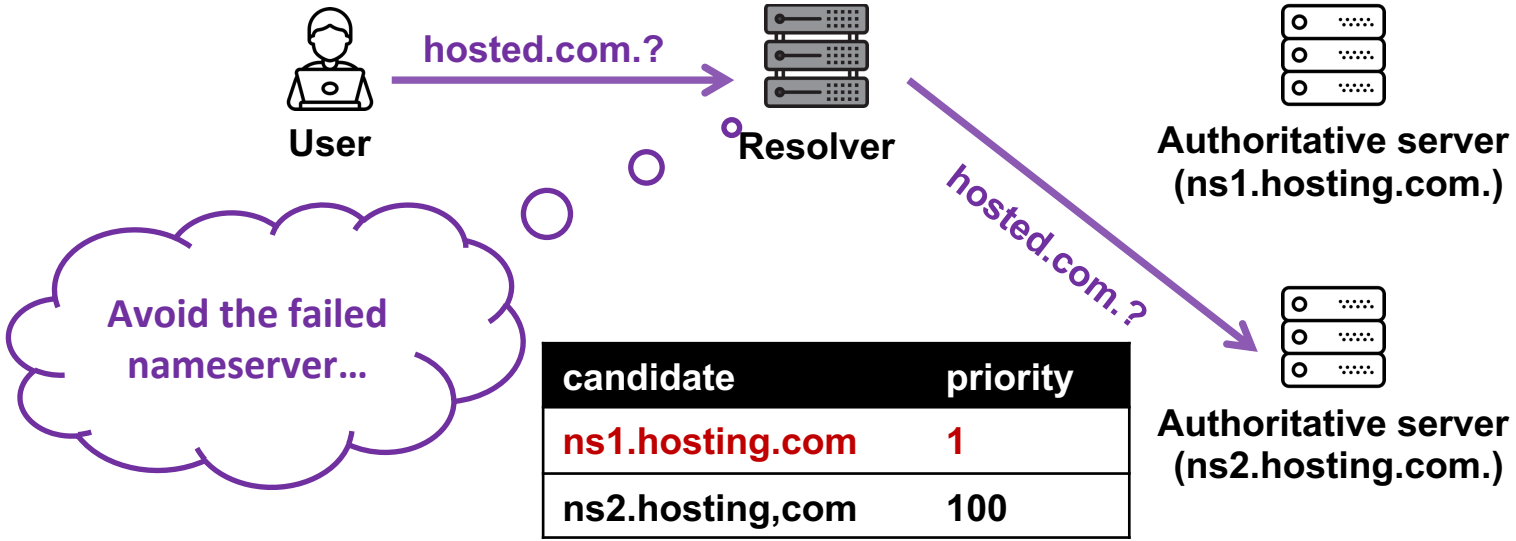
- Recursive DNS software prefers the nameserver with the best performance
- Recursive DNS software avoids the nameserver failed to response
- The status of nameserver is **globally shared by all domains.**



candidate	priority
ns1.hosting.com	1
ns2.hosting,com	100

While resolver meeting a “silence” authoritative server

- Recursive DNS software prefers the nameserver with the best performance
- Recursive DNS software avoids the nameserver failed to response
- The status of nameserver is **globally shared by all domains.**



candidate	priority
ns1.hosting.com	1
ns2.hosting,com	100

The Disablance Attack

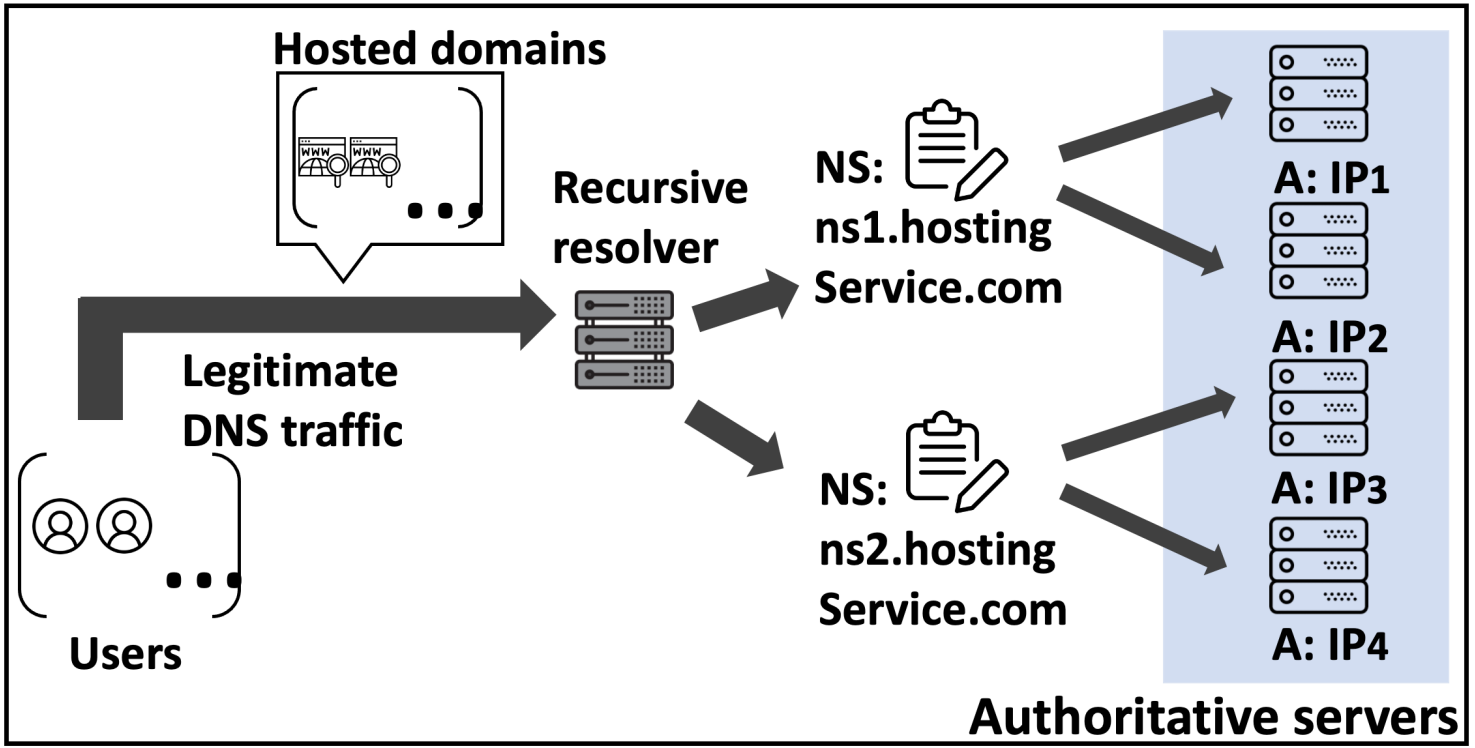
An example: victim's configuration

```
$ dig hostedDomain.com NS
          ...
;; ANSWER SECTION:
hostedDomain.com. 3600   IN NS ns1.hostingService.com.
hostedDomain.com. 3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns1.hostingService.com.        3600   IN A   IP1
ns1.hostingService.com.        3600   IN A   IP2
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```

The Disablance Attack

```
$ dig hostedDomain.com NS
        ...
;; ANSWER SECTION:
hostedDomain.com. 3600   IN NS ns1.hostingService.com.
hostedDomain.com. 3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns1.hostingService.com.        3600   IN A   IP1
ns1.hostingService.com.        3600   IN A   IP2
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```

An example: victim's configuration



Variant 1: Attacking a NS record: ns1.hosting…

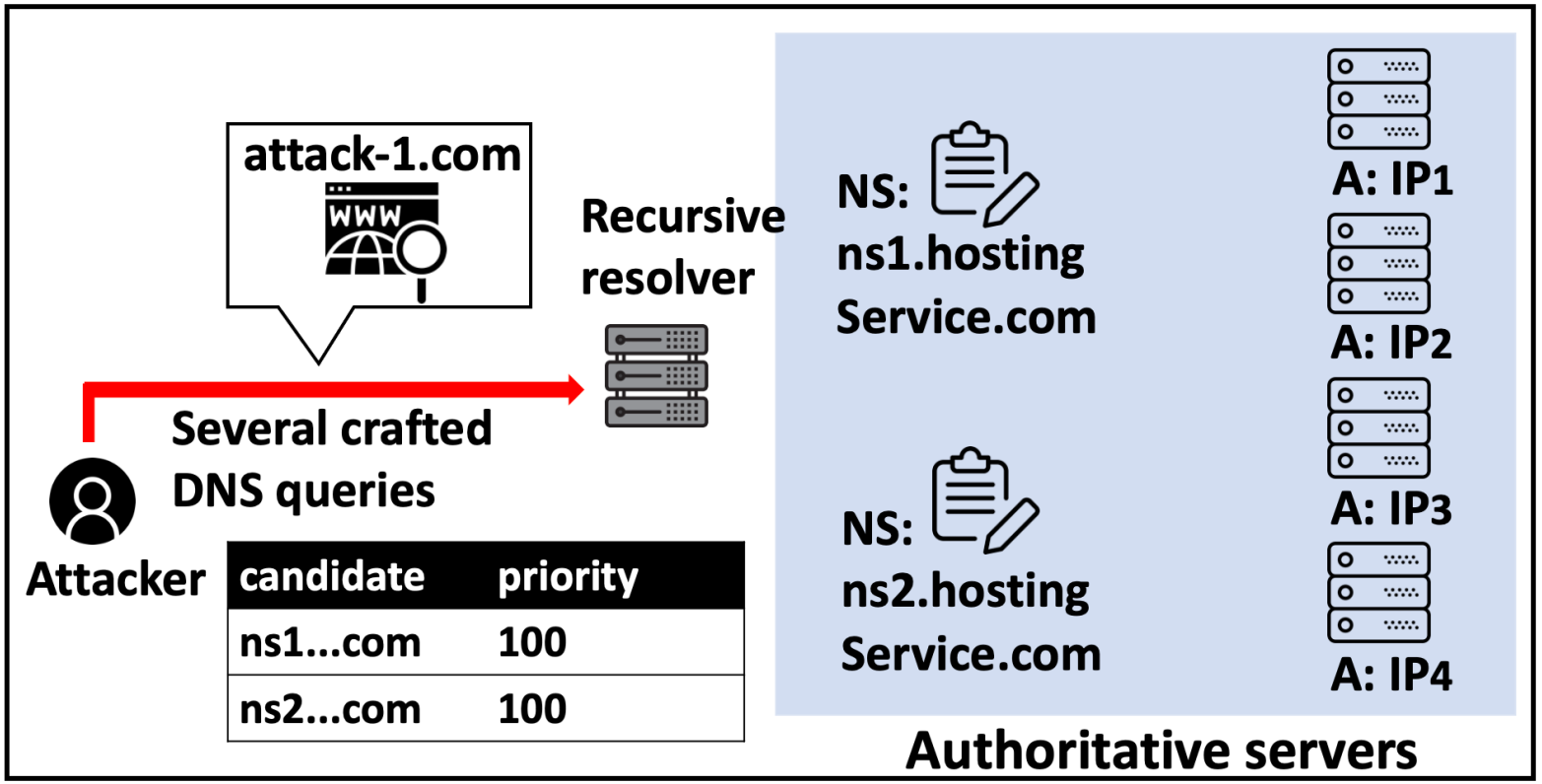
Attacker's configuration

```
$ dig attack-1.com NS
          ...
;; ANSWER SECTION:
attack-1.com.   3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```

Note that the domain is NOT hosted on the targeted authoritative server

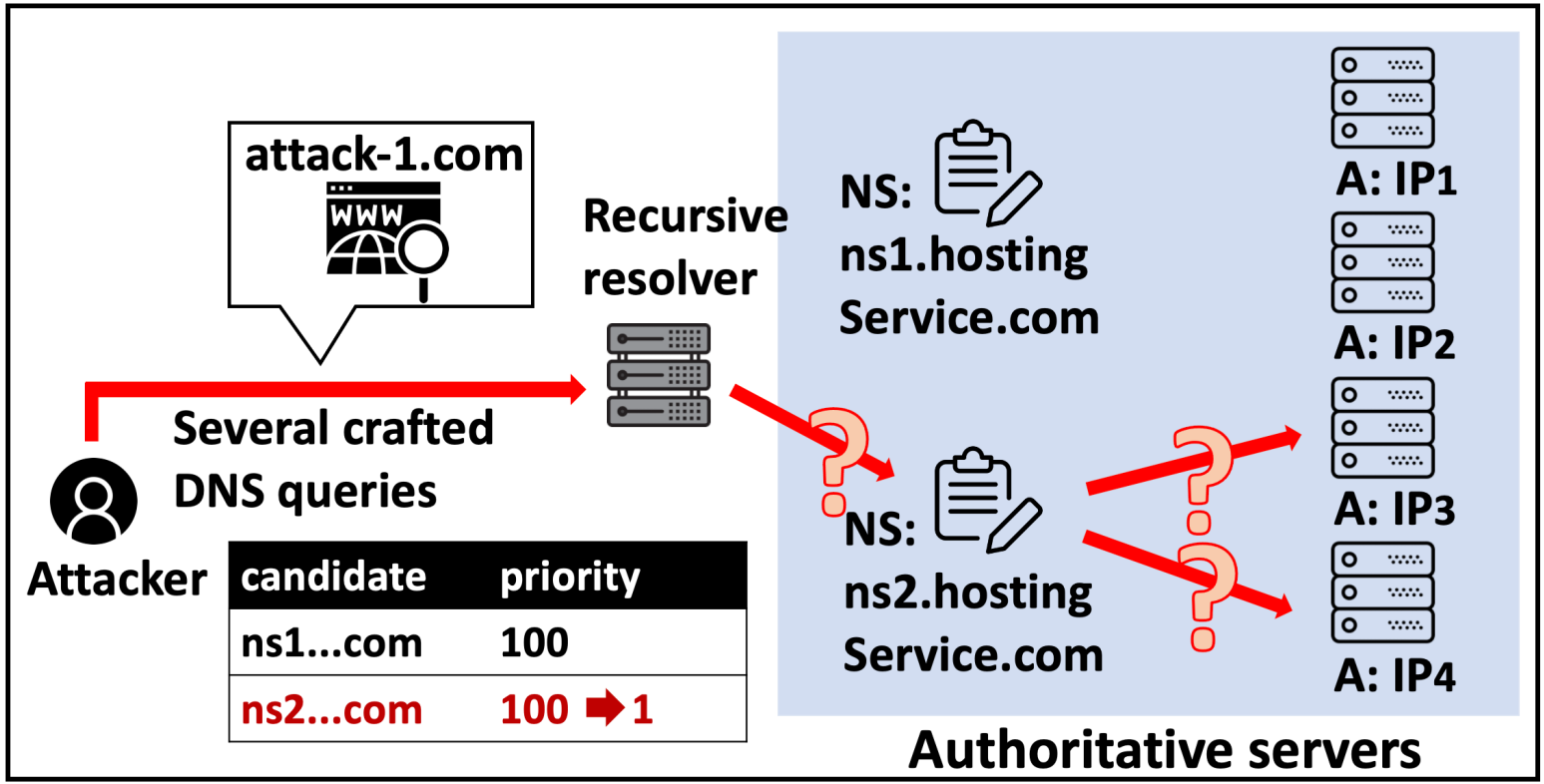
Variant 1: Attacking a NS record

```
$ dig attack-1.com NS
          ...
;; ANSWER SECTION:
attack-1.com.   3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```



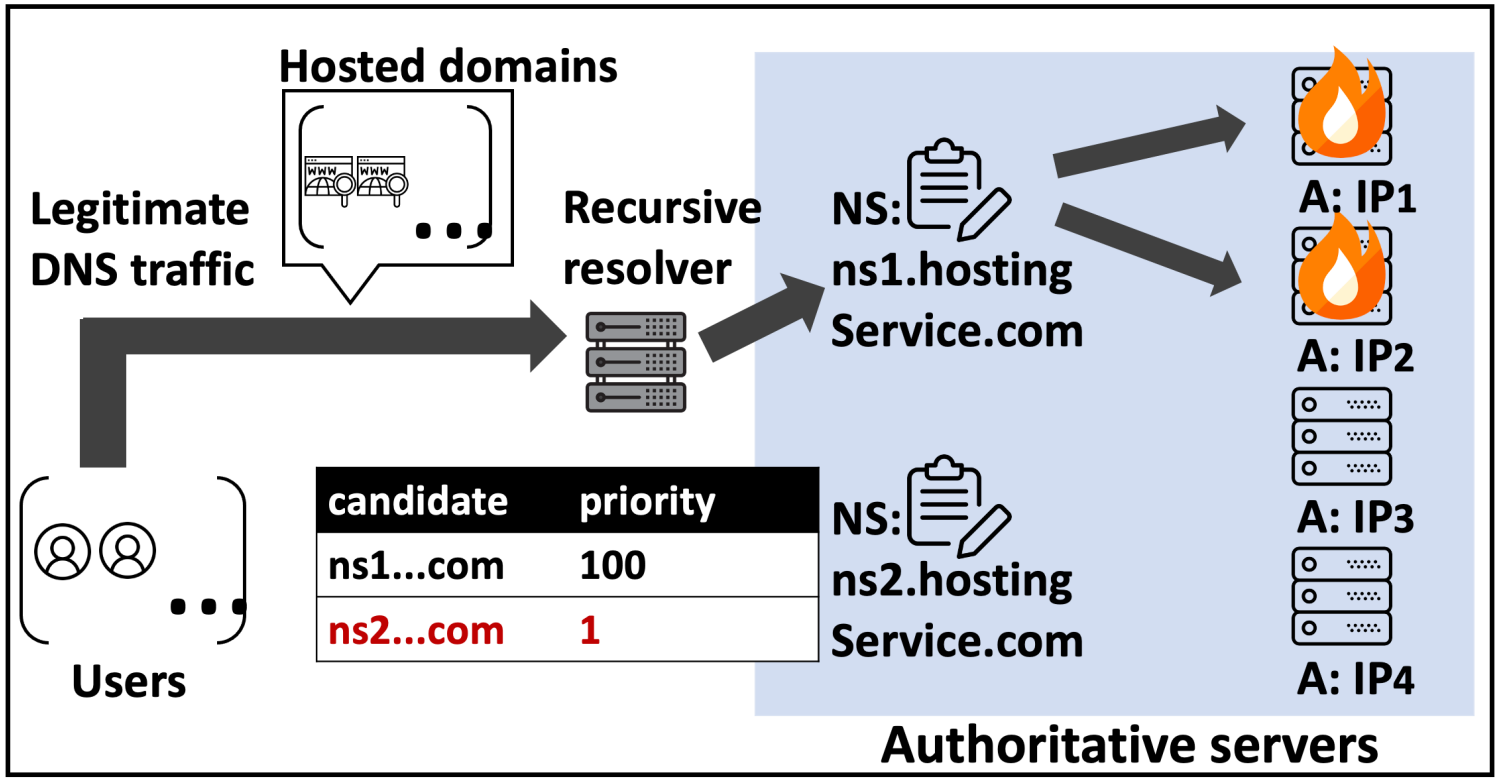
Variant 1: Attacking a NS record

```
$ dig attack-1.com NS
          ...
;; ANSWER SECTION:
attack-1.com.   3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```



Variant 1: Attacking a NS record

```
$ dig attack-1.com NS
          ...
;; ANSWER SECTION:
attack-1.com.   3600   IN NS ns2.hostingService.com.

;; ADDITIONAL SECTION
ns2.hostingService.com.        3600   IN A   IP3
ns2.hostingService.com.        3600   IN A   IP4
```



Variant 2: Attacking an IP address: IP_1

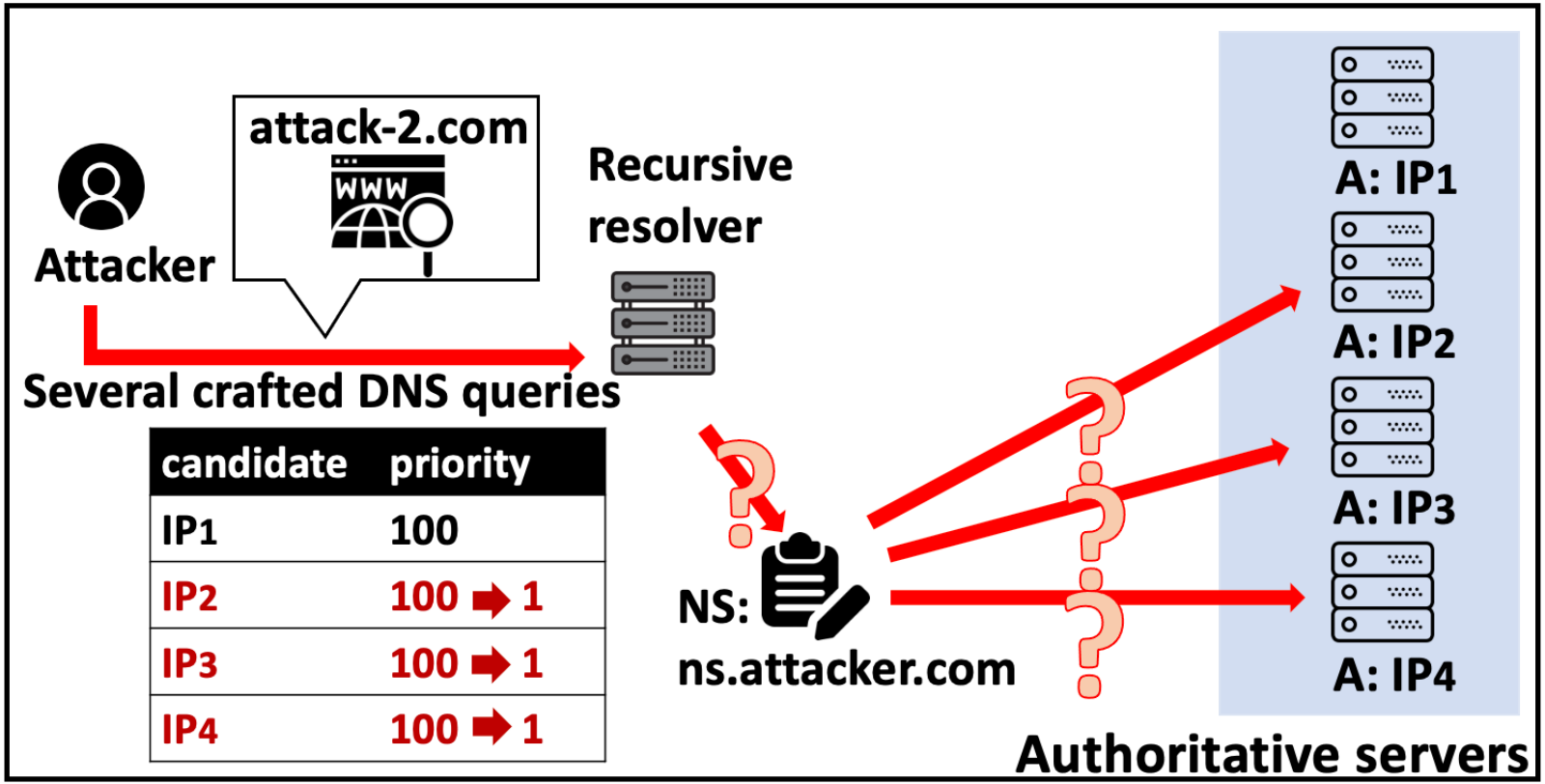
Attacker's configuration

```
$ dig attack-2.com NS
          ...
;; ANSWER SECTION:
attack-2.com.   3600   IN NS ns.attacker.com.

;; ADDITIONAL SECTION
ns.attacker.com.                3600   IN A   IP2
ns.attacker.com.                3600   IN A   IP3
ns.attacker.com.                3600   IN A   IP4
```

Note that the domain is NOT hosted on the targeted authoritative server

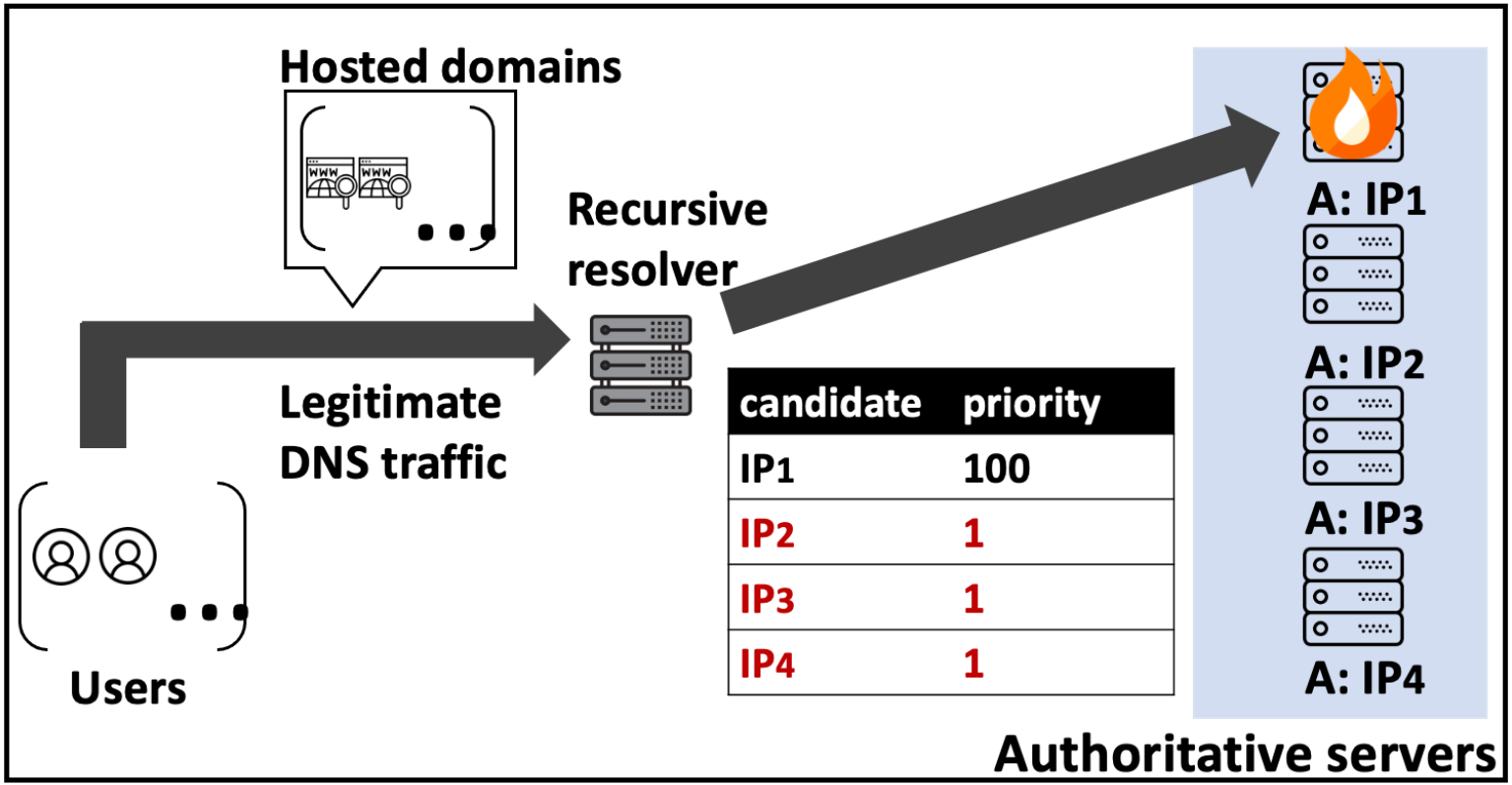
Variant 2: Attacking an IP address

```
$ dig attack-2.com NS
          ...
;; ANSWER SECTION:
attack-2.com.   3600   IN NS ns.attacker.com.

;; ADDITIONAL SECTION
ns.attacker.com.                3600   IN A   IP2
ns.attacker.com.                3600   IN A   IP3
ns.attacker.com.                3600   IN A   IP4
```



Variant 2: Attacking an IP address

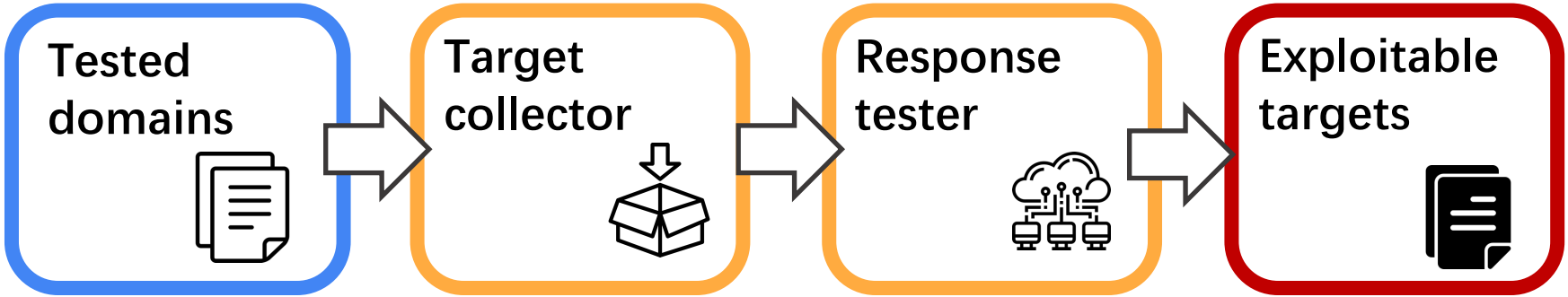
```
$ dig attack-2.com NS
          ...
;; ANSWER SECTION:
attack-2.com.   3600   IN NS ns.attacker.com.

;; ADDITIONAL SECTION
ns.attacker.com.                3600   IN A   IP2
ns.attacker.com.                3600   IN A   IP3
ns.attacker.com.                3600   IN A   IP4
```



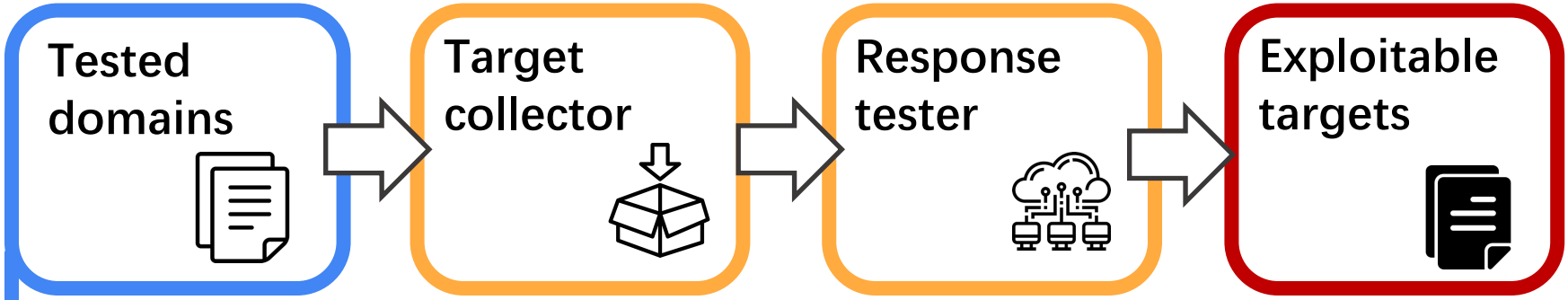
Evaluating Exploitable Targets

Part I: hosted domains, authoritative servers, and service providers

Methodology

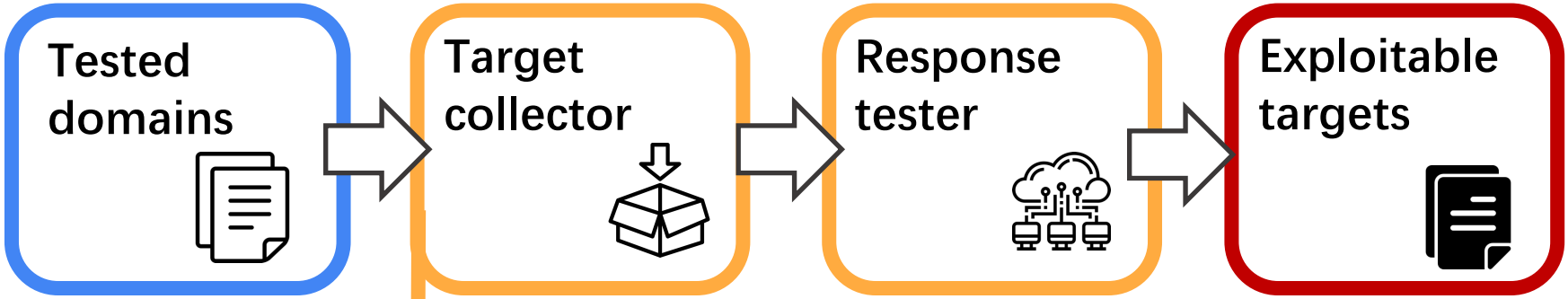


Methodology



- Top 1M SecRank FQDNs
- Top 1M Tranco SLDs

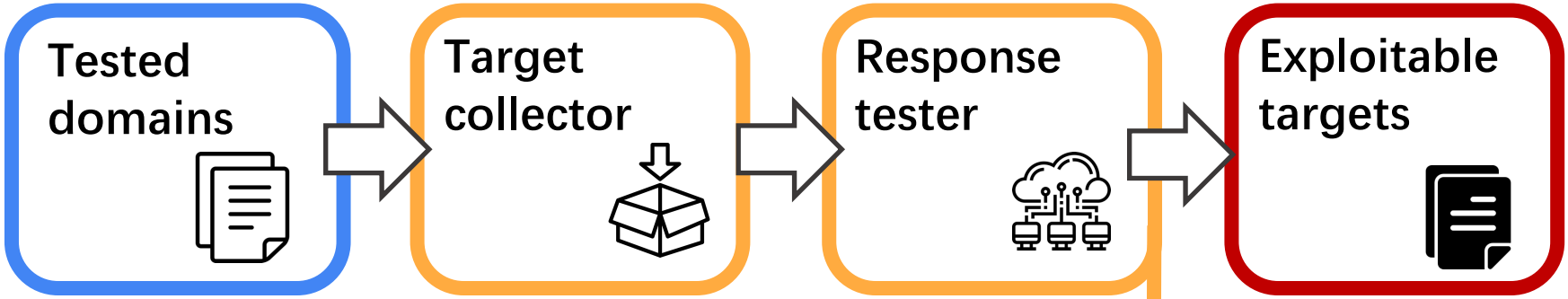
Methodology



For each targeted domain:

- Request the NS records at the parent zone
- Request IP addresses of each NS record

Methodology



Mark a nameserver as vulnerable when it:

- ignores queries for a domain that is not hosted
- provides responses for its hosted domain

Exploitable hosted domains

Our measurement started on May 12, 2022:

22.24% of the top 1M FQDNs and **3.94% of the top 1M SLDs** are exploitable

Distribution of affected domains

Top	10	100	1K	10K	100K	1M
# FQDN	20%	29%	34.7%	26.9%	25.3%	22.2%
# SLD	10%	11%	6.8%	5.5%	4.6%	3.9%

Exploitable hosted domains

Our measurement started on May 12, 2022:
22.24% of the top 1M FQDNs and **3.94% of the top 1M SLDs** are exploitable

Distribution of affected domains

Top	10	100	1K	10K	100K	1M
# FQDN	20%	29%	34.7%	26.9%	25.3%	22.2%
# SLD	10%	11%	6.8%	5.5%	4.6%	3.9%

Example:

API for a mobile operating system	FQDNs are at rank 2 and 9
Short-form video applications	26 domains among the top 100 FQDNs
E-commerce	FQDNs are at rank 50 and 54, 180, 181, 186, and 200

Exploitable authoritative servers

- **11.73%** of nameservers for the top 1M FQDNs and **4.40%** of nameservers for the top 1M SLDs are exploitable

Exploitable authoritative servers

- **11.73%** of nameservers for the top 1M FQDNs and **4.40%** of nameservers for the top 1M SLDs are exploitable

- Tencent Cloud (DNSPod) hosted 6.26% of the top 1M FQDNs and 0.81% of the top 1M SLDs

Top 10 affected providers for the top sites

Top 1M FQDNs			Top 1M SLDs		
Provider	**Service[a]**	**# Hosting**	**Provider**	**Service[a]**	**# Hosting**
Tencent Cloud	Cloud	**62,607**	Tencent Cloud	Cloud	**8,119**
WANGSU	Cloud	**34,838**	DNS.COM	Cloud	**4,071**
DNS.COM	Cloud	9,949	WANGSU	Cloud	2,738
GNAME	Domain	7,647	GNAME	Domain	1,645
360	Cloud	2,212	Freenom	Domain	580
SFN	Domain	1,920	Danesconames	Domain	390
Baidu Cloud	Cloud	965	Baidu Cloud	Cloud	337
22.cn	Cloud	843	XZ.com	Domain	250
Na.wang	Cloud	623	22.cn	Cloud	226
CNDNS	Cloud	345	Heteml	Cloud	218
Total		**222,370**	**Total**		**39,392**

Amplification Factor

- **Definition:** compared to the normal case, the multiplier of the traffic load on nameservers caused by redirecting **legitimate traffic**

Amplification Factor

- **Definition:** compared to the normal case, the multiplier of the traffic load on nameservers caused by redirecting **legitimate traffic**

- While targeting an IP address:
  - Average: 8.51× and 6.84× for the top FQDNs and SLDs
  - Maximum: 32× and 46× for the top FQDNs and SLDs

Amplification Factor

- **The domains requiring high availability are suffering a greater amplification impact**

- This is because they are assigned more nameservers for load balancing

Amplification Factor

- **The domains requiring high availability are suffering a greater amplification impact**

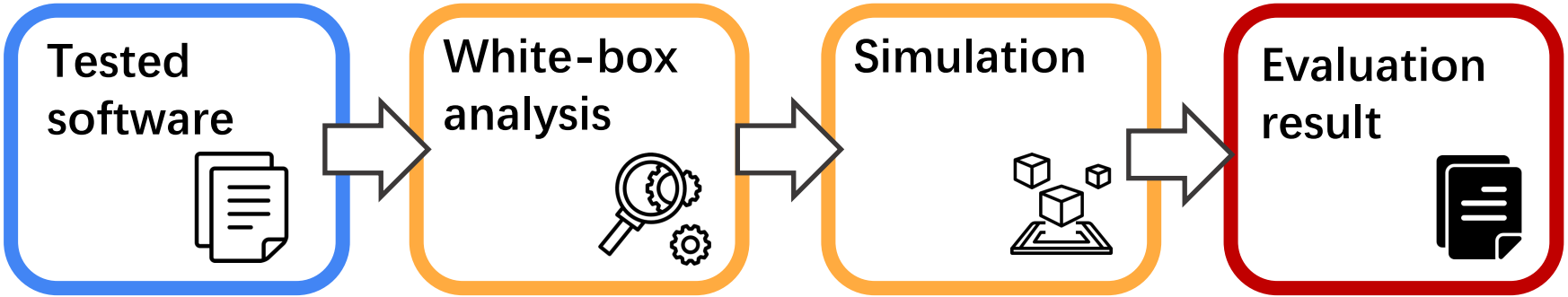
- This is because they are assigned more nameservers for load balancing

- Examples:
  - the AF reaches 46× for a vulnerable SLD owned by a technology company

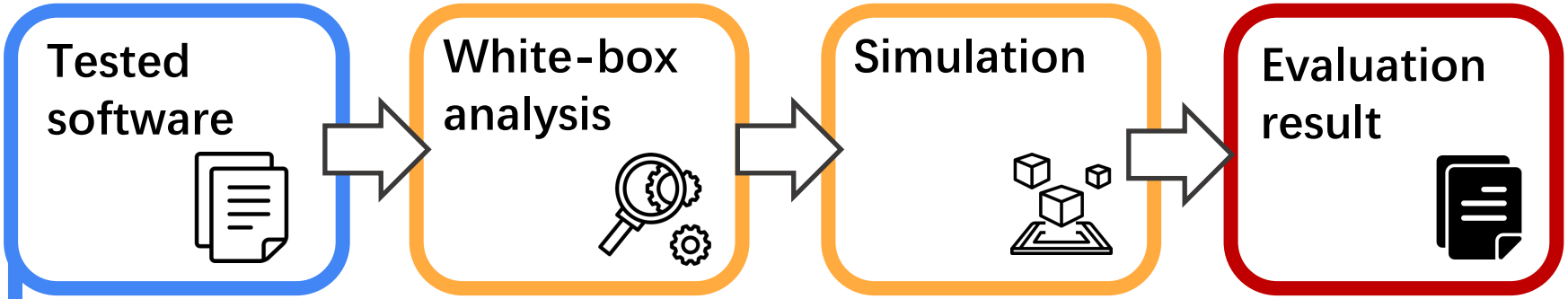
Evaluating Exploitable Targets

Part II: recursive DNS software, open resolvers and public recursive services

Methodology: software analysis

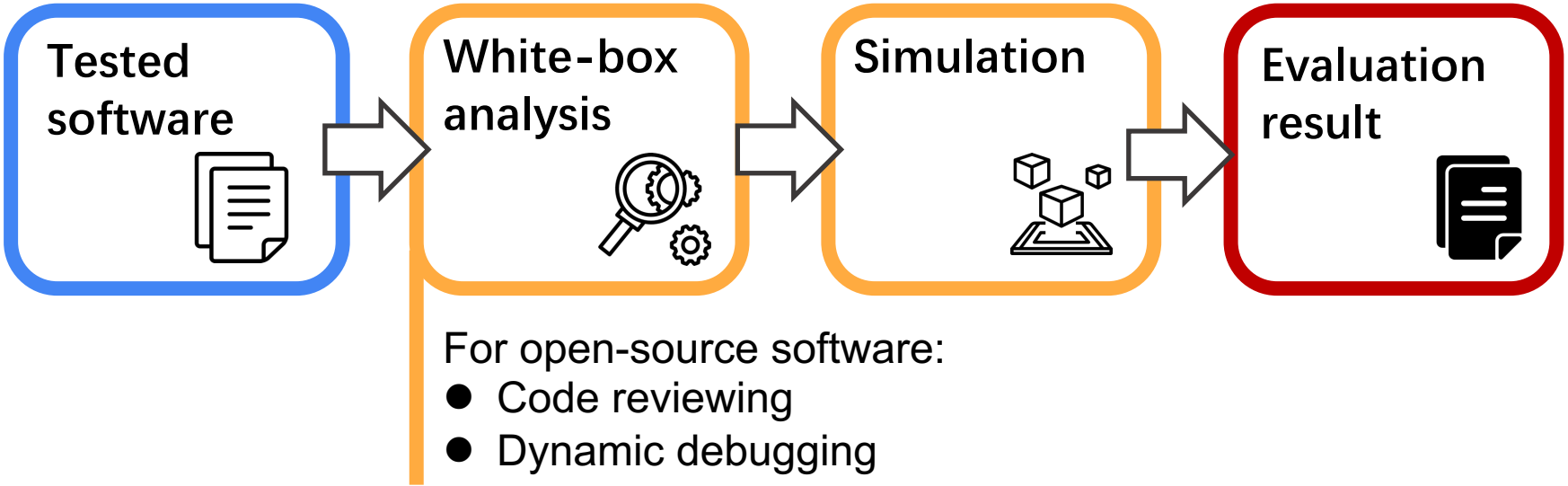


Methodology: software analysis

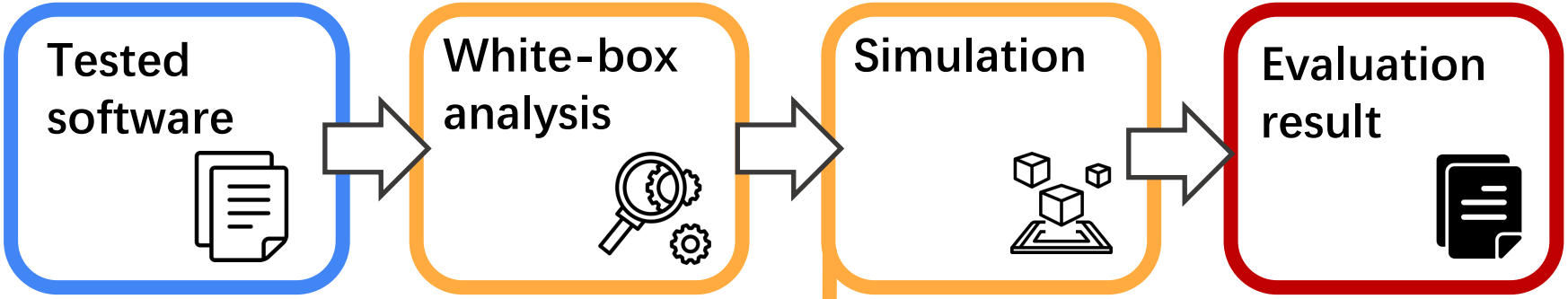


- BIND9 (9.18.4)
- Unbound (1.16.1)
- PowerDNS (4.7.1)
- Knot Resolver (5.5.1)
- Microsoft DNS (10.0.20348.169, 6.1.7600)

Methodology: software analysis



Methodology: software analysis



Open-source software:

- Extracted the essential code
- Executed in a simulated environment

Close-source software:

- Ran the whole operating system in a simulated environment

Result: software analysis

Three of the five analyzed software, which enjoy a **high market share**, are vulnerable

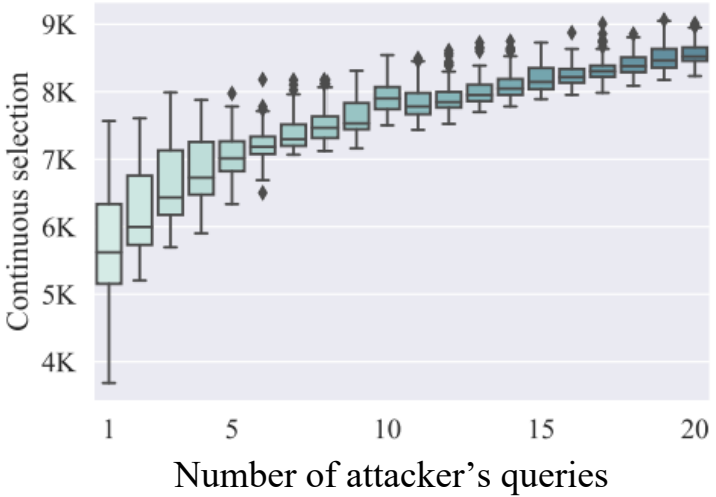
Software	Sensitive Variant	Market Share [46]
BIND9	DisablanceNS/Address	60.2+%
Unbound	-	4.8+%
PowerDNS Recursor	DisablanceNS	3.2+%
Microsoft DNS	DisablanceNS/Address	2.5+%
Knot Resolver	-	(no mention)

Summary of analyzing DNS recursive software

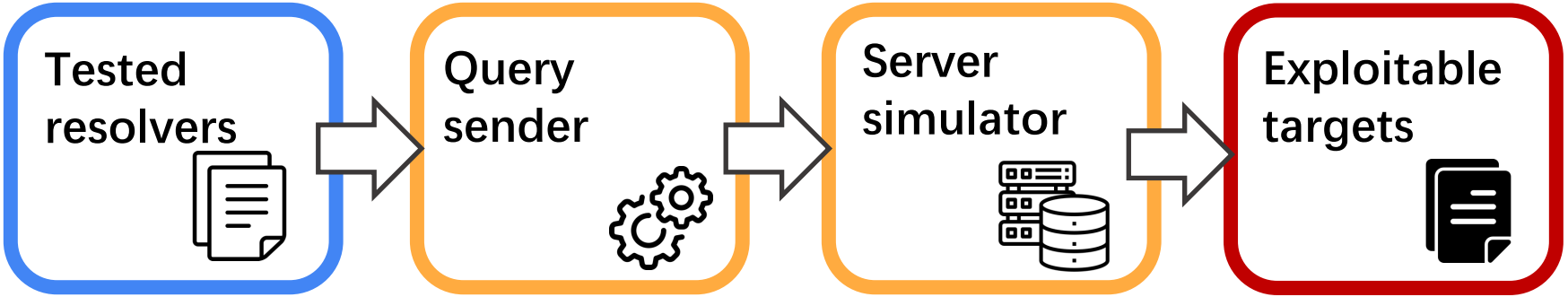
Result: software analysis

The attacking efficiency is high under different conditions

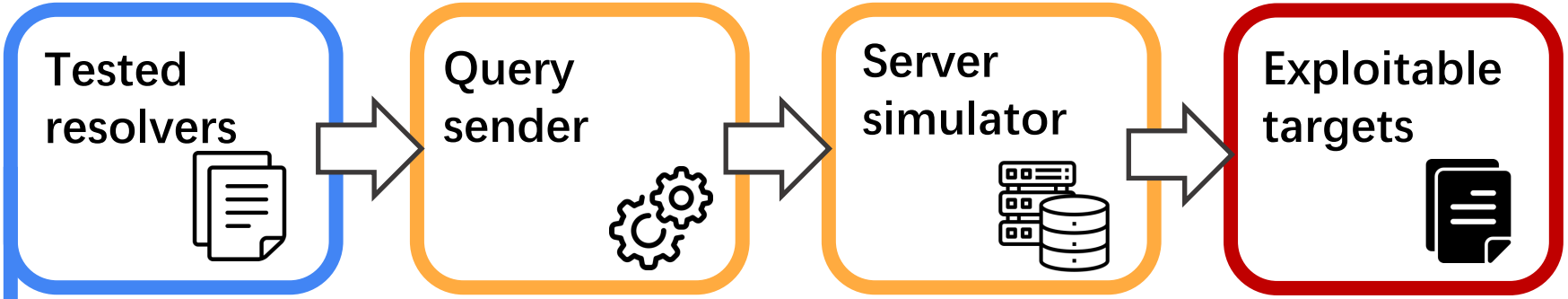
- Example: after receiving **one** attacking query, BIND9 sent **5,730** legitimate queries to the targeted nameserver on average



Methodology: measurement

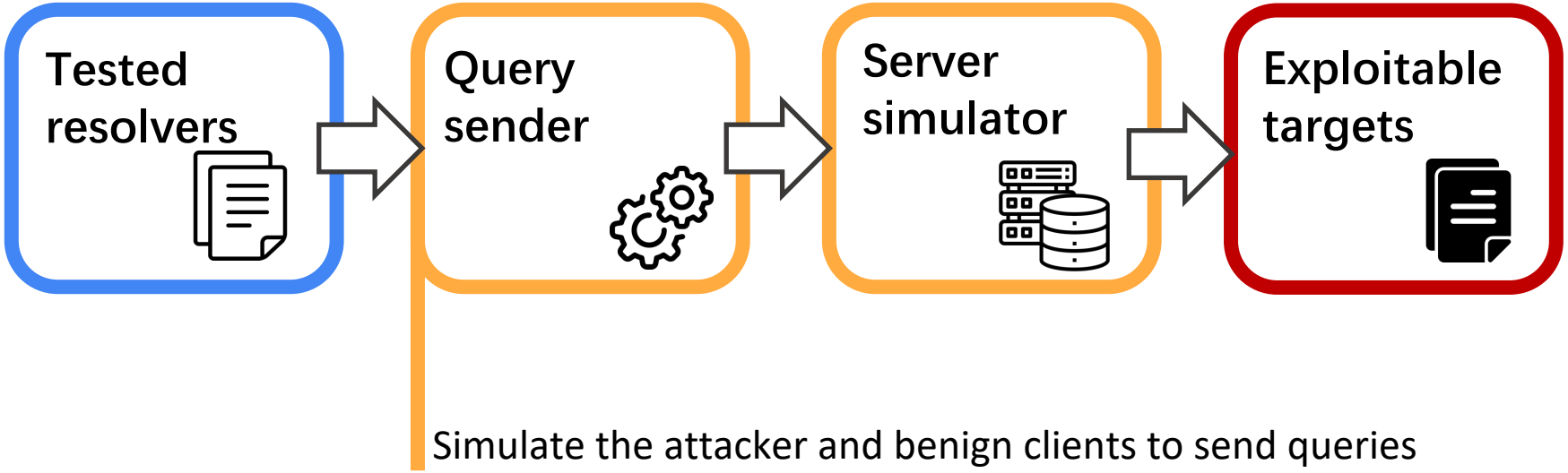


Methodology: measurement

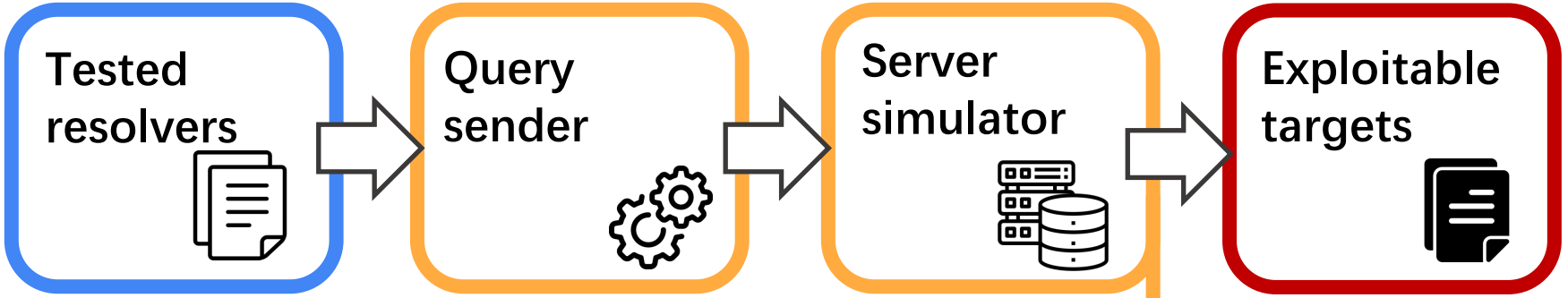


- 37,843 stable open resolvers
- 14 public DNS services

Methodology: measurement



Methodology: measurement

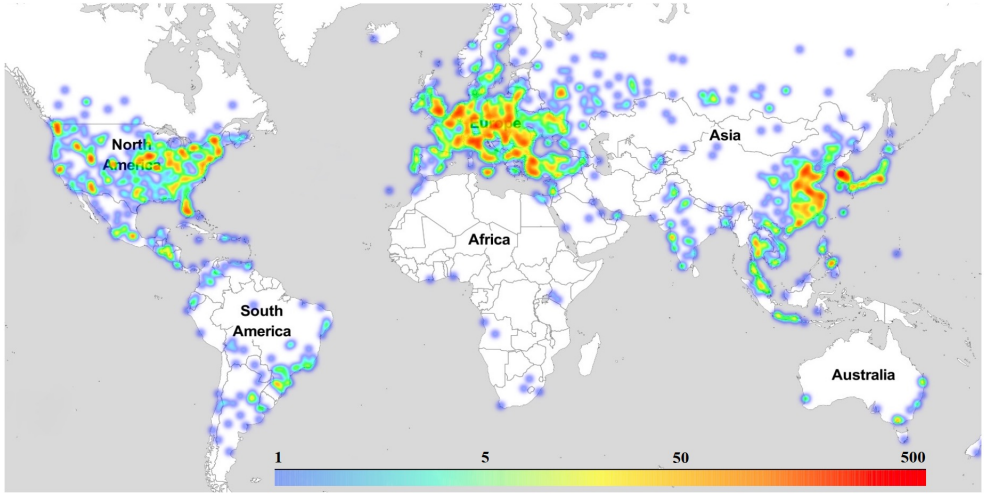


- established a set of vulnerable nameservers
- utilized our own domains

Result: exploitable open resolvers

Our measurement started on Dec 14, 2021:

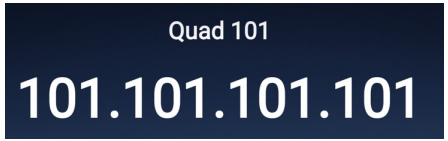
- **14,372 (37.88%)** of the tested open resolvers are vulnerable
- Distributed in **130 countries, 2,821 cities, and 1,778 Ases**
- Serving a considerable number of users whose DNS traffic can be diverted



Result: exploitable public recursive services

Our measurement started on Dec 29, 2021:

- **45 of 100** IP addresses operated by **10 of 14** providers are exploitable
- The vulnerable vendors including Cloudflare, OneDNS, and Quad9



Discussion and Conclusion

Reasons causing Disablance

Authoritative server

To protect against DNS amplification attacks,

- it drops DNS queries for non-authoritative domains.

Reasons causing Disablance

Authoritative server

To protect against DNS amplification attacks,

- it drops DNS queries for non-authoritative domains.

Recursive resolver

To improve efficiency,

- it decreases the priority of a nameserver when the query is timed-out, and
- shares the status of nameservers across all authoritative domains

Mitigation and Disclosure

Authoritative server

Should take responsibility since their strategy violates the DNS specification:

> RFC 8906:
> “Failing to respond at all is always incorrect, regardless of the configuration of the server.”

Mitigation and Disclosure

Authoritative server

Should take responsibility since their strategy violates the DNS specification:

> RFC 8906:
> "Failing to respond at all is always incorrect, regardless of the configuration of the server."

Recommendation

- With EDNS support: Returning REFUSED with an EDNS error code
- Without EDNS support: Returning REFUSED instead of other misleading errors
- Answering with REFUSED does not introduce other DDoS attack vectors

Mitigation and Disclosure

Authoritative server

Should take responsibility since their strategy violates the DNS specification:

> RFC 8906:
> "Failing to respond at all is always incorrect, regardless of the configuration of the server."

Recommendation

- Support EDNS: Returning REFUSED with an EDNS error code
- Not support EDNS: Returning REFUSED instead of misleading errors
- Do not cause DDoS attacks since it does not generate more responses than what the adversary sent

Feedback

Tencent Cloud, Amazon, and TSSNS have taken action to fix this issue

Mitigation and Disclosure

Recursive resolver

- The vulnerable software are installed on most of the affected resolvers
- Adjusting software is more efficient for fixing the issue

Mitigation and Disclosure

Recursive resolver

- The vulnerable software are installed on most of the affected resolvers
- Adjusting software is more efficient for fixing the issue

Recommendation

Adopting the strategy of Knot Resolver:

- Knot shares the status of nameservers, but it tries other candidates with a predetermined probability
- It **restores the status once** the nameserver responds successfully.

Mitigation and Disclosure

Recursive resolver

- The vulnerable software are installed on most of the affected resolvers
- Adjusting software is more efficient for fixing the issue

Recommendation

Adopting the strategy of Knot Resolver:

- Knot shares the status of nameservers, but it tries other candidates with a predetermined probability
- It **restores the status once** the nameserver responds successfully.

Feedback

All vendors of vulnerable software acknowledged our findings, but insisted that authoritative servers should fix the issue

Conclusion

Novel attack. Uncovered a vulnerability to turn protocol non-compliance into disrupting the DNS load balancing functionality

Comprehensive measurement. Systematically evaluated the real-world impact of the attack

Responsible disclosure. Responsibly disclosed issues to vendors with mitigation options

Reference

[1] Brij B Gupta and Omkar P Badve. 2017. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications 28, 12 (2017), 3655–3682.

[2] Jelena Mirkovic and Peter Reiher. 2004. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. SIGCOMM Comput. Commun. Rev. 34, 2 (apr 2004), 39–53.https://doi.org/10.1145/997150.997156

[3] Saman Taghavi Zargar, James Joshi, and David Tipper. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks.IEEE Communications Surveys & Tutorials 15, 4 (2013), 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127

[4] Tianxiang Dai, Haya Shulman, and Michael Waidner. 2021. Let's Downgrade Let's Encrypt. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (Virtual Event, Republic of Korea) (CCS '21). Association for Computing Machinery, New York, NY, USA, 1421–1440. https://doi.org/10.1145/3460120.3484815

[5] Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, and Thorsten Holz. 2015. Going Wild: Large-Scale Classification of Open DNS Resolvers. In Proceedings of the 2015 Internet Measurement Conference (Tokyo, Japan) (IMC '15).Association for Computing Machinery, New York, NY, USA, 355–368. https://doi.org/10.1145/2815675.2815683

Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers

Fenglu Zhang, Baojun Liu, Eihal Alowaisheq, Jianjun Chen, Chaoyi Lu, Linjian Song, Yong Ma, Ying Liu, Haixin Duan and Min Yang

zfl20@mails.tsinghua.edu.cn