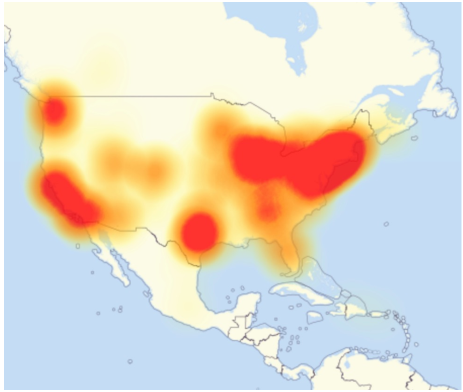
Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers

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

The security of DNS is critical to Internet operation

- Domain Name System (DNS) is a **cornerstone** of Internet infrastructure.
- The outage of DNS can cause **severe** influence.



Several popular domains were unavailable in most regions
in the US during the DDoS attack on Dyn in Oct 2016

Question

How about deploying **more machines** to defend against the DoS attack?

Requirement of load balancing from DNS specifications

To ensure security and robustness, DNS specifications **require load balancing mechanisms** on authoritative DNS servers:

RFC 1034

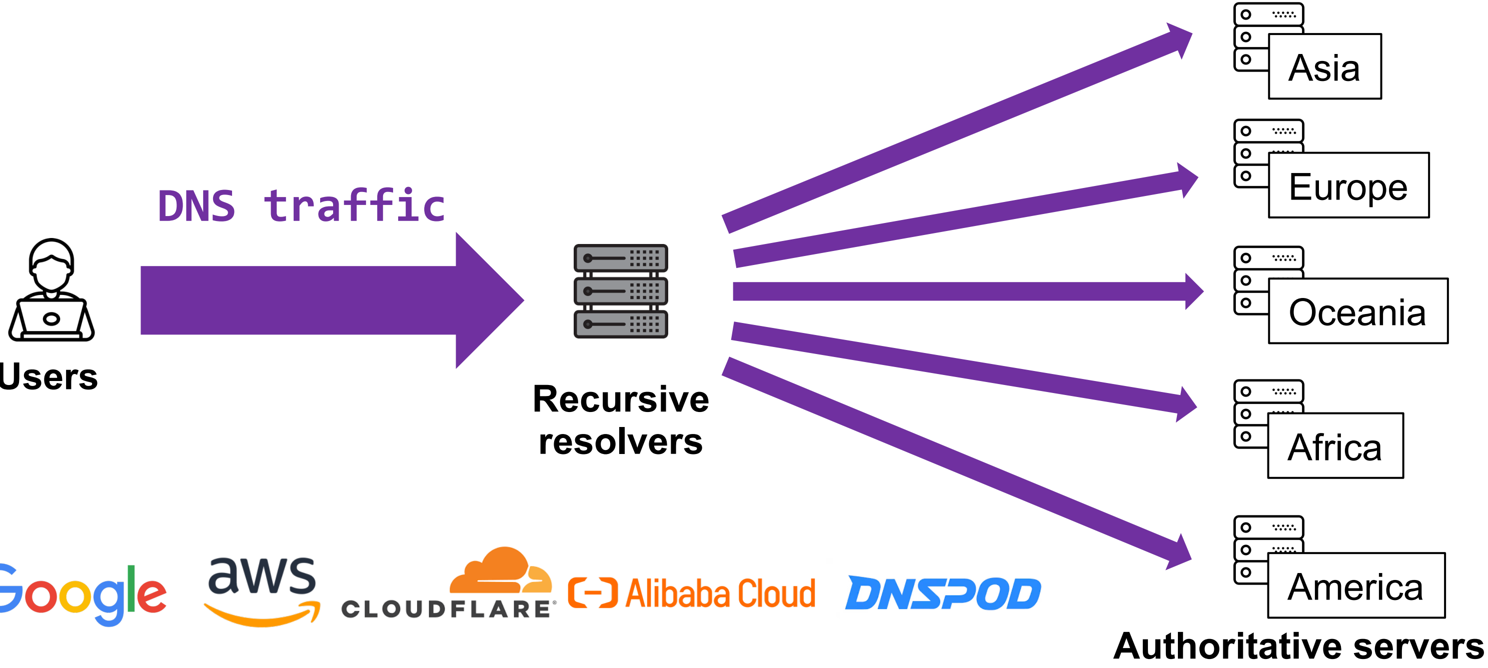
We REQUIRE every zone to **be available on at least two servers**, and many zones have **more redundancy than that.**

RFC 2182

Authoritative servers MUST **be placed at both topologically and geographically dispersed locations.**

DNS load balancing of mainstream vendors

Mainstream vendors of DNS services **support** load balancing mechanisms **complying with DNS specifications.**

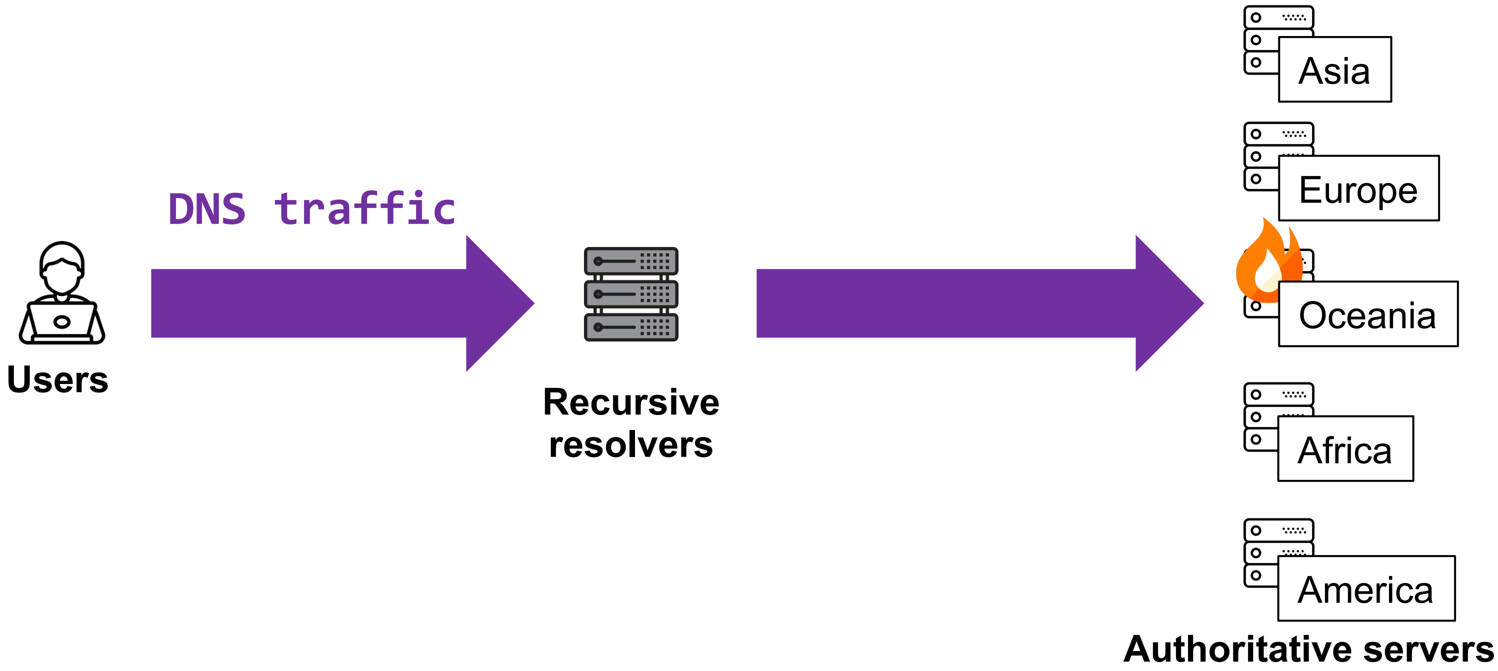


Question

What will happen if attackers **disrupt load balancing of authoritative DNS servers**?

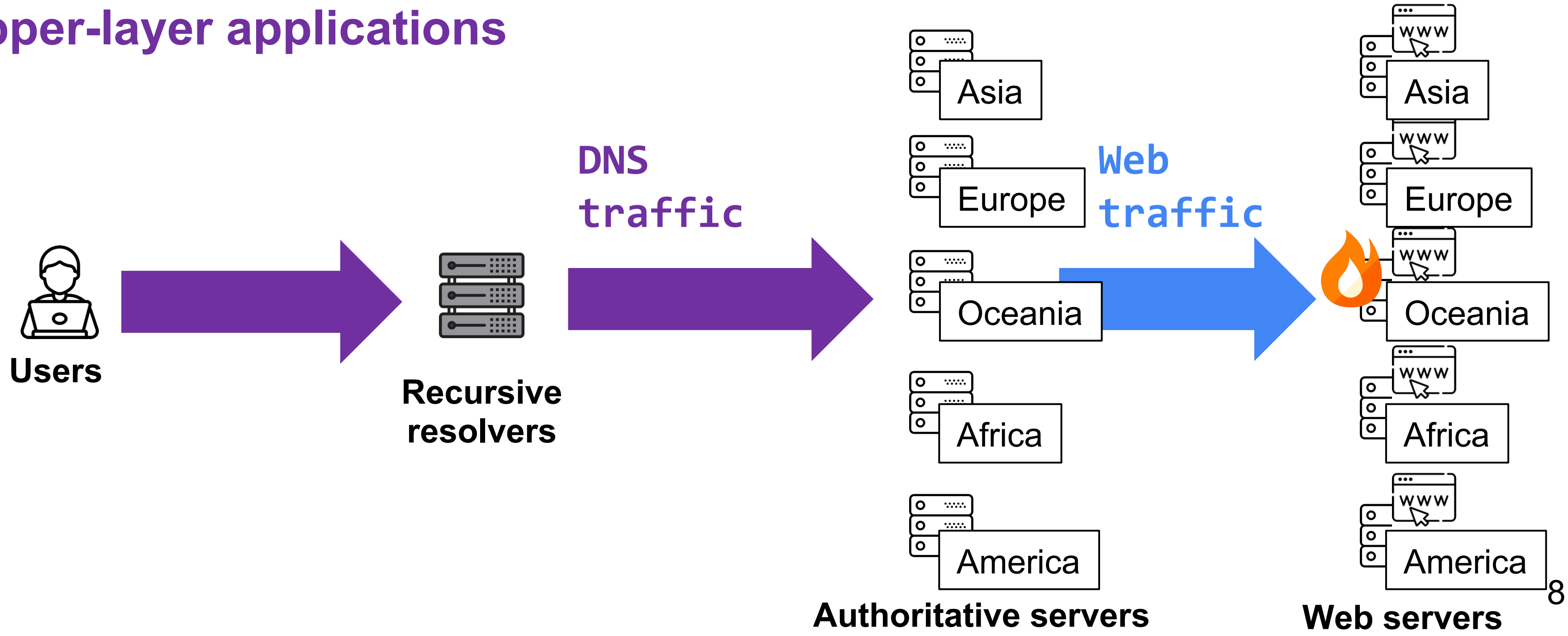
Security impacts of disrupting DNS load balancing

Impact 1: overloading authoritative DNS servers with legitimate traffic



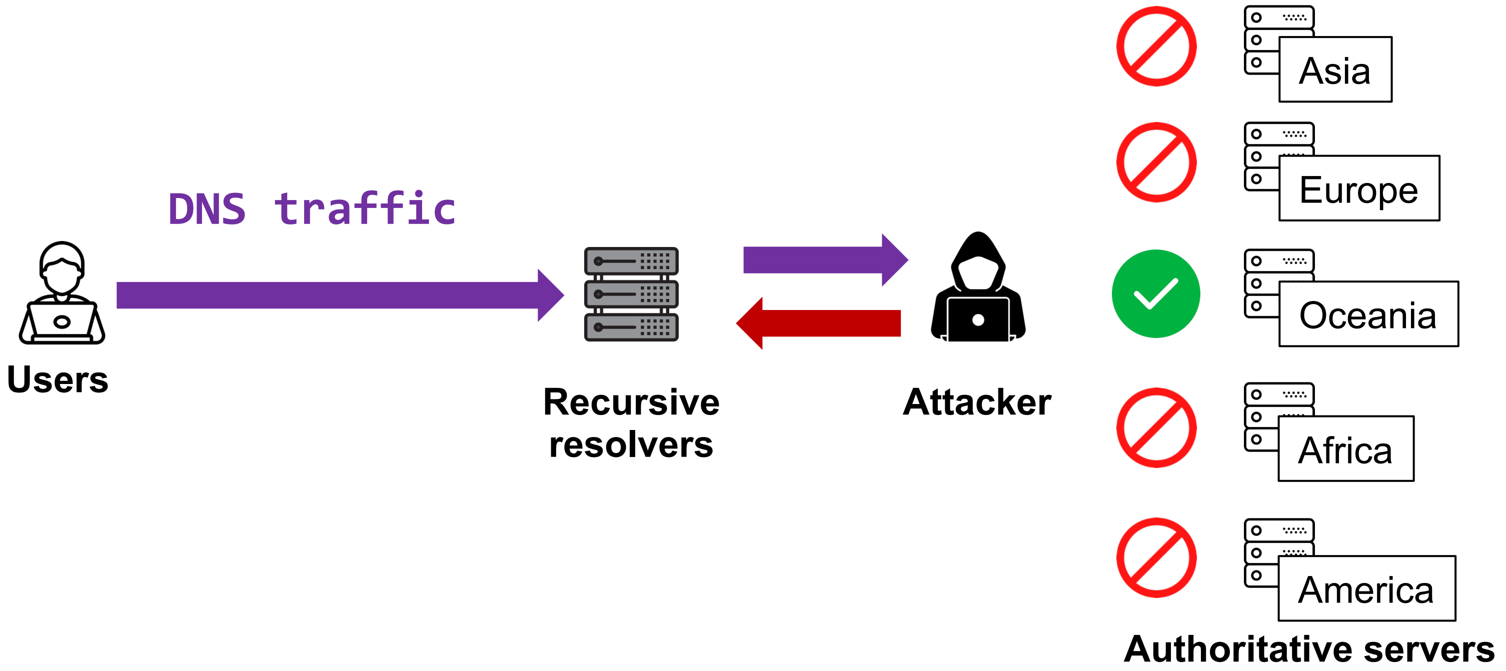
Security impacts of disrupting DNS load balancing

Impact 2: disrupting DNS-based load balancing of upper-layer applications



Security impacts of disrupting DNS load balancing

Impact 3: Lowering the bar of traffic hijacking and cache poisoning



Our study: Disablance (DNS Load Balancing Disabler)

Uncovered a new attack that disrupts the load balancing mechanism of authoritative DNS servers

Our study: Disablance (DNS Load Balancing Disabler)

Uncovered a new attack (Disablance) that disrupts the load balancing mechanism of 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 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)

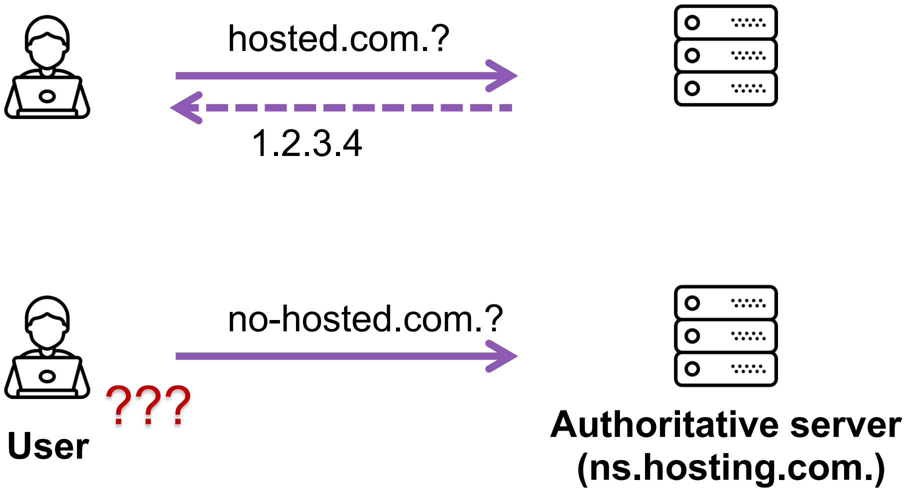
Uncovered a new attack (Disablance) that disrupts the load balancing mechanism of authoritative DNS servers

- **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

The Disablance Attack

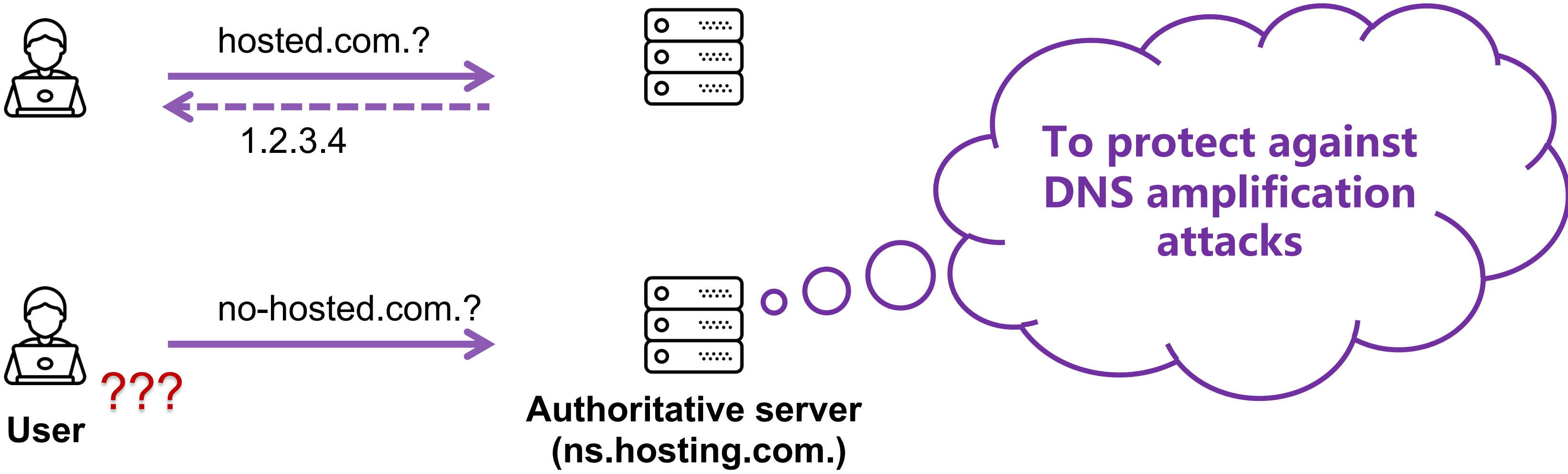
“Silence is golden”: a strategy of authoritative servers

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**



While resolvers meeting a “silent” authoritative server

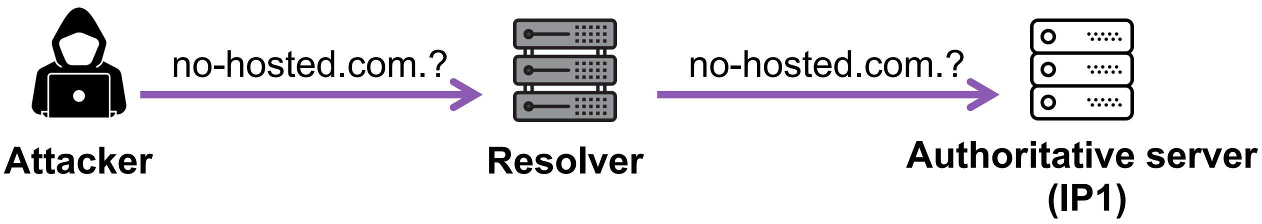
Recursive resolvers:

- **prefer** an authoritative server with the best performance
- **avoid** an authoritative server failing to respond
- **share** the status of an authoritative server **across all authoritative domains.**

While resolvers meeting a "silent" authoritative server

Recursive resolvers:

- **prefer** an authoritative server with the best performance
- **avoid** an authoritative server failing to respond
- **share** the status of an authoritative server **across all authoritative domains.**

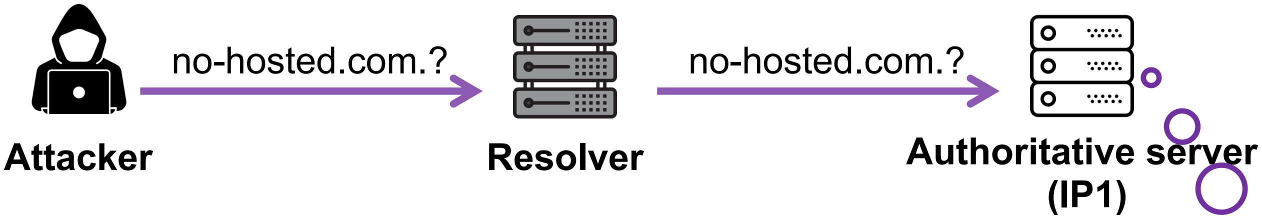


candidate	priority
IP1	100
IP2	100

While resolvers meeting a “silent” authoritative server

Recursive resolvers:

- **prefer** an authoritative server with the best performance
- **avoid** an authoritative server failing to respond
- **share** the status of an authoritative server **across all authoritative domains.**

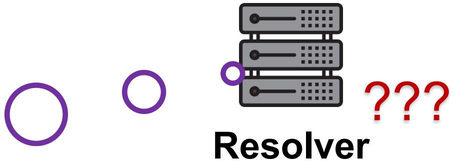


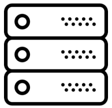
candidate	priority
IP1	100
IP2	100

While resolver meeting a “silent” authoritative server

Recursive resolvers:

- **prefer** an authoritative server with the best performance
- **avoid** an authoritative server failing to respond
- **share** the status of an authoritative server **across all authoritative domains.**



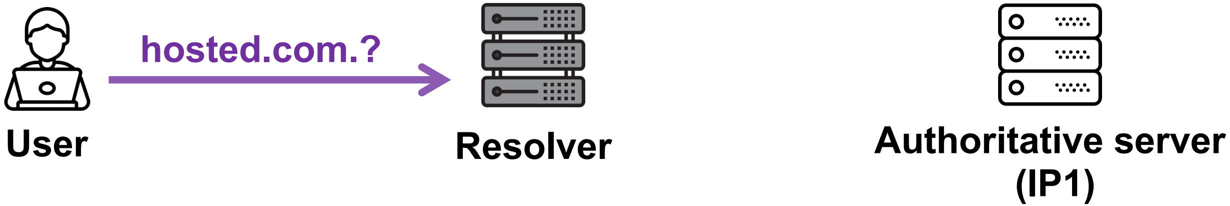


candidate	priority
IP1	100 -> 1
IP2	100

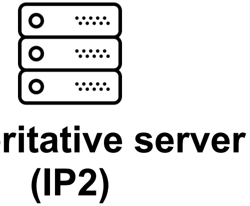
While resolver meeting a “silent” authoritative server

Recursive resolvers:

- **prefer** an authoritative server with the best performance
- **avoid** an authoritative server failing to respond
- **share** the status of an authoritative server **across all authoritative domains.**



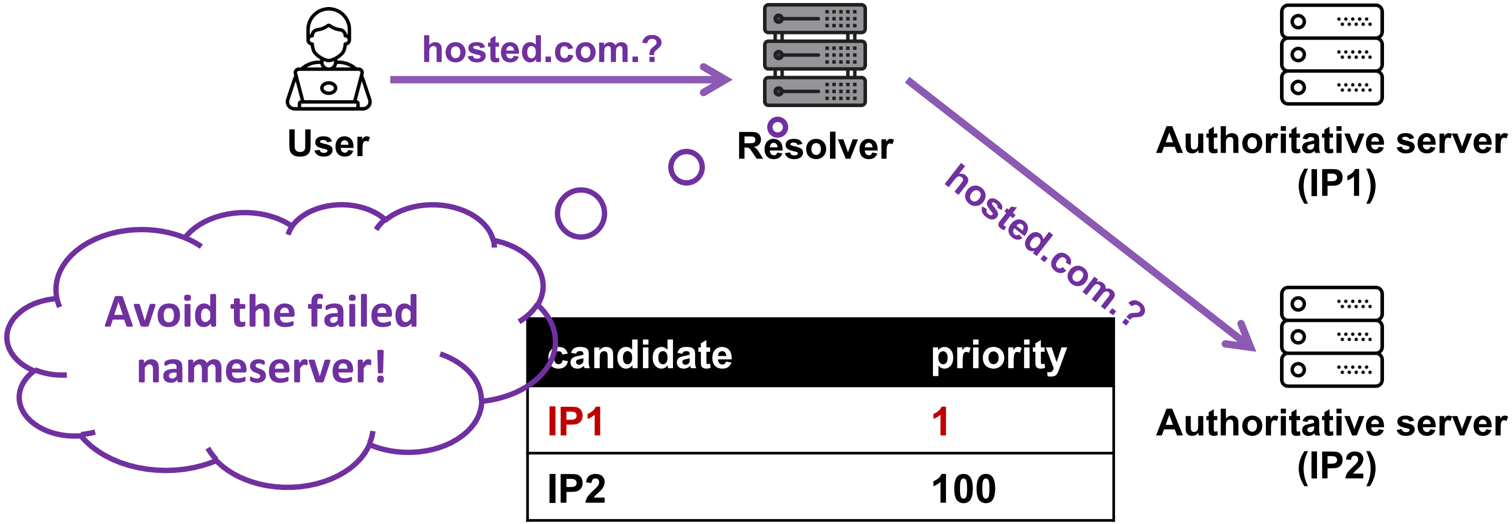
candidate	priority
IP1	1
IP2	100



While resolver meeting a “silent” authoritative server

Recursive resolvers:

- **prefer** an authoritative server with the best performance
- **avoid** an authoritative server failing to respond
- **share** the status of an authoritative server **across all authoritative domains.**



candidate	priority
IP1	1
IP2	100

An example: Disablance Attack

- IP1 – IP4 are authoritative servers assigned by the vendor.

```
$ dig hosted.com NS

 ...

;; ADDITIONAL SECTION
ns.hosted.com.  600  IN  A  IP1
ns.hosted.com.  600  IN  A  IP2
ns.hosted.com.  600  IN  A  IP3
ns.hosted.com.  600  IN  A  IP4
```

An example: Disablance Attack

- IP1 – IP4 are authoritative servers assigned by the vendor.
- Attackers aim to redirect DNS traffic to IP1.
- `attack.com` is **not hosted** on the targeted authoritative server.

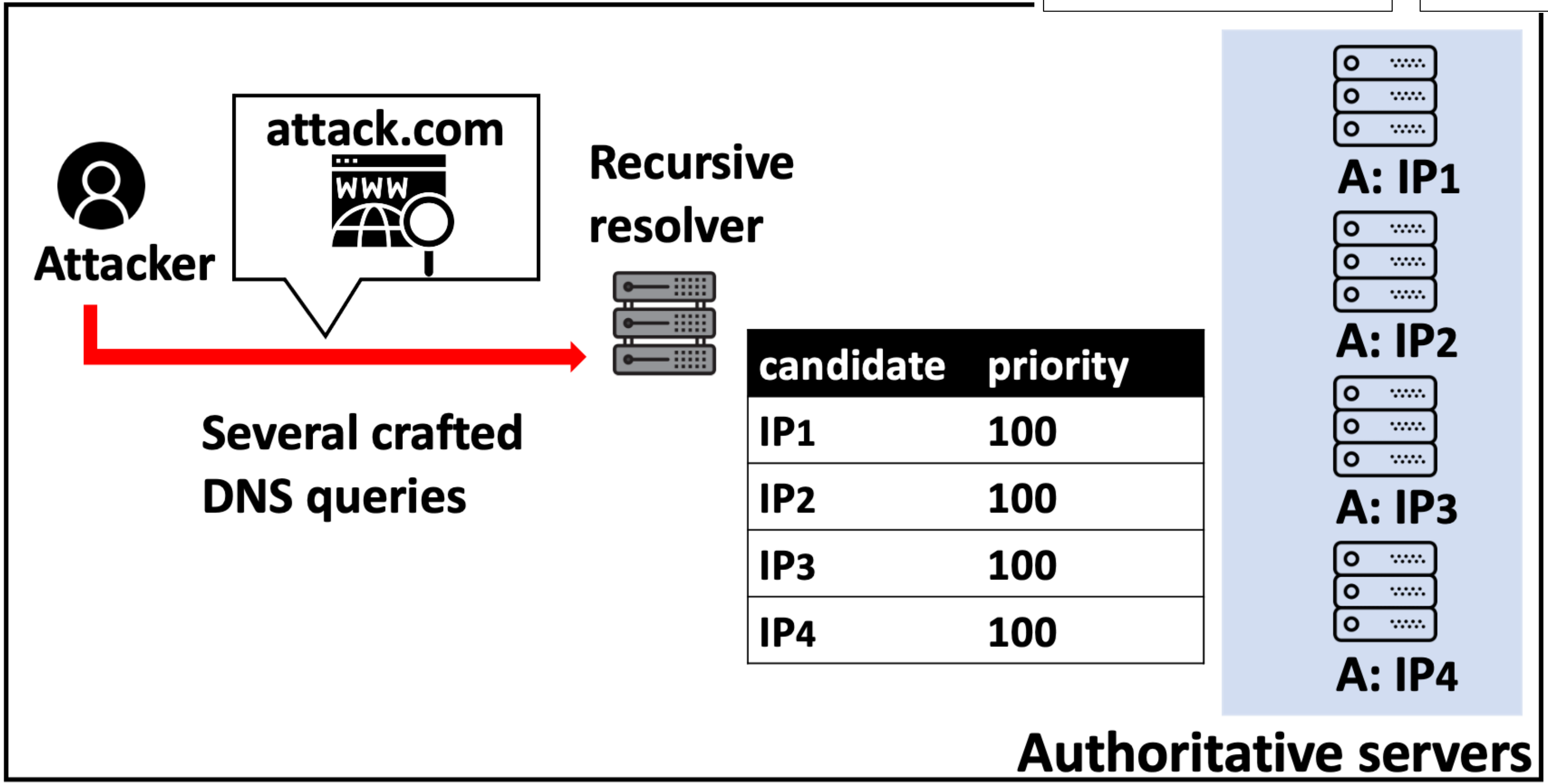
```
$ dig hosted.com NS

  ...

;; ADDITIONAL SECTION
ns.hosted.com.   600  IN  A  IP1
ns.hosted.com.   600  IN  A  IP2
ns.hosted.com.   600  IN  A  IP3
ns.hosted.com.   600  IN  A  IP4
```

```
$ dig attack.com NS

  ...

;; ADDITIONAL SECTION

ns.attack.com.   600  IN  A  IP2
ns.attack.com.   600  IN  A  IP3
ns.attack.com.   600  IN  A  IP4
```

An example: Disablance Attack

```
$ dig hosted.com NS

 ...

;; ADDITIONAL SECTION
ns.hosted.com.   600  IN  A  IP1
ns.hosted.com.   600  IN  A  IP2
ns.hosted.com.   600  IN  A  IP3
ns.hosted.com.   600  IN  A  IP4
```

```
$ dig attack.com NS

 ...

;; ADDITIONAL SECTION

ns.attack.com.   600  IN  A  IP2
ns.attack.com.   600  IN  A  IP3
ns.attack.com.   600  IN  A  IP4
```

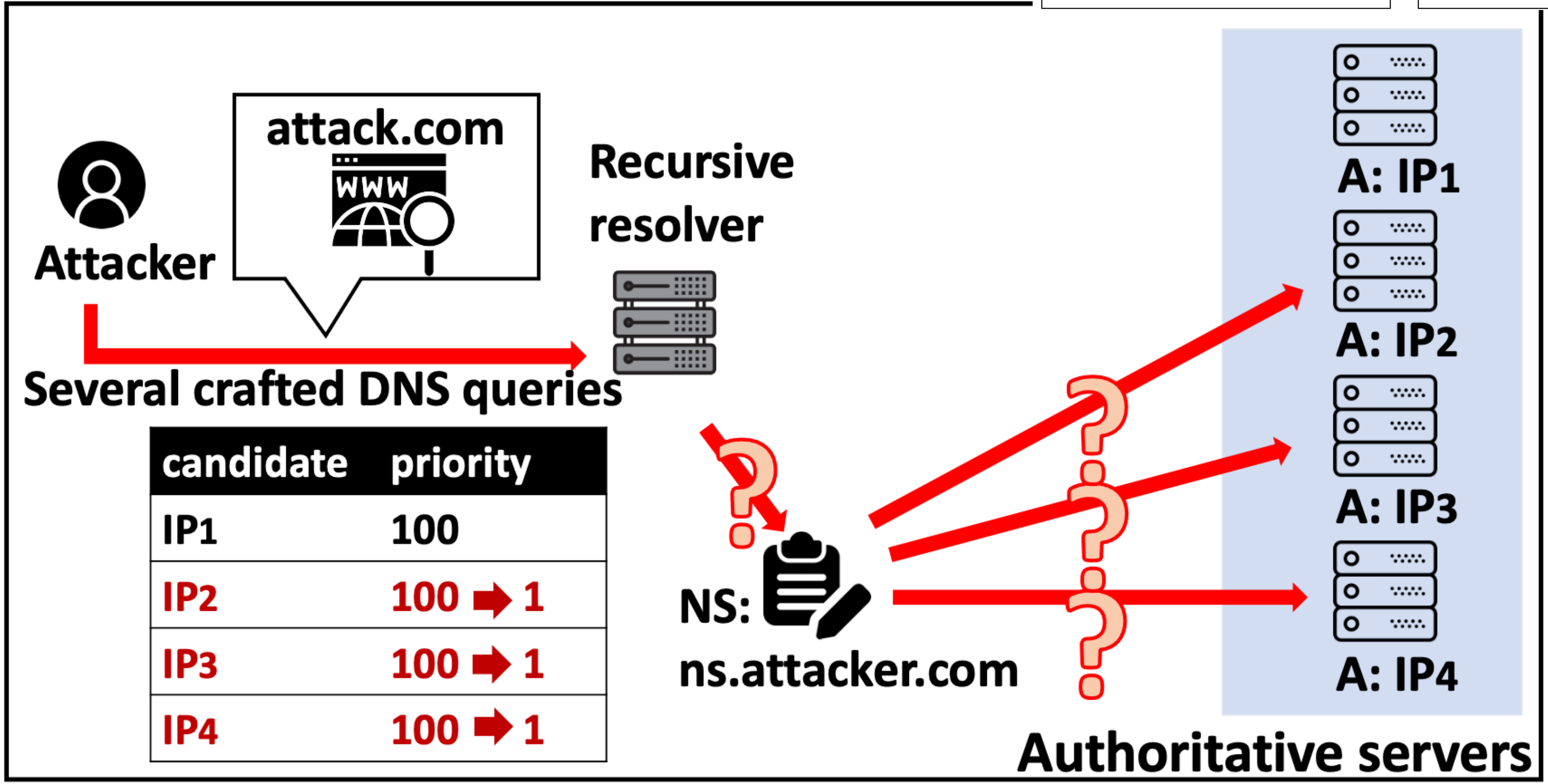


candidate	priority
IP1	100
IP2	100
IP3	100
IP4	100

An example: Disablance Attack

```
$ dig hosted.com NS
 ...
;; ADDITIONAL SECTION
ns.hosted.com.  600  IN  A  IP1
ns.hosted.com.  600  IN  A  IP2
ns.hosted.com.  600  IN  A  IP3
ns.hosted.com.  600  IN  A  IP4
```

```
$ dig attack.com NS
 ...
;; ADDITIONAL SECTION

ns.attack.com.  600  IN  A  IP2
ns.attack.com.  600  IN  A  IP3
ns.attack.com.  600  IN  A  IP4
```

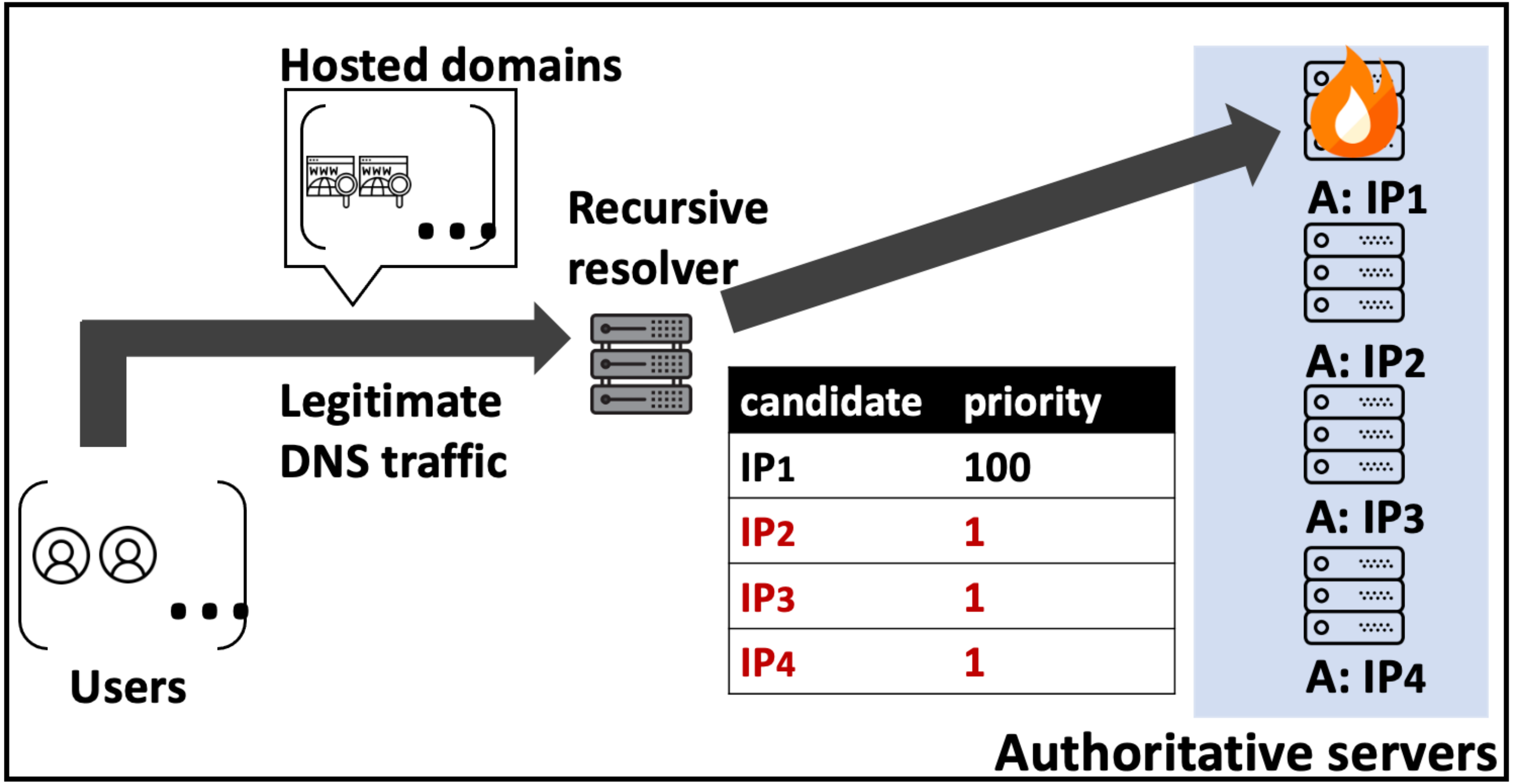


candidate	priority
IP1	100
IP2	100 ➡ 1
IP3	100 ➡ 1
IP4	100 ➡ 1

An example: Disablance Attack

```
$ dig hosted.com NS
 ...
;; ADDITIONAL SECTION
ns.hosted.com.  600  IN  A  IP1
ns.hosted.com.  600  IN  A  IP2
ns.hosted.com.  600  IN  A  IP3
ns.hosted.com.  600  IN  A  IP4
```

```
$ dig attack.com NS
 ...
;; ADDITIONAL SECTION

ns.attack.com.  600  IN  A  IP2
ns.attack.com.  600  IN  A  IP3
ns.attack.com.  600  IN  A  IP4
```

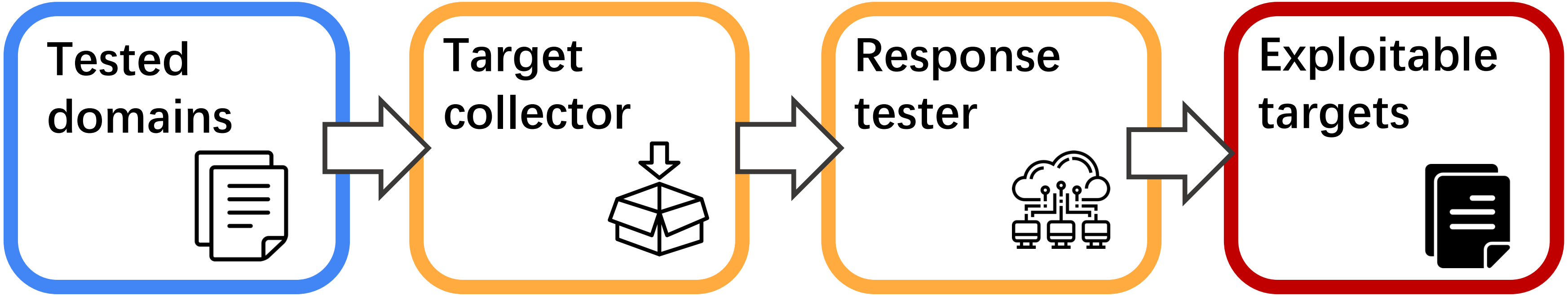


candidate	priority
IP1	100
IP2	1
IP3	1
IP4	1

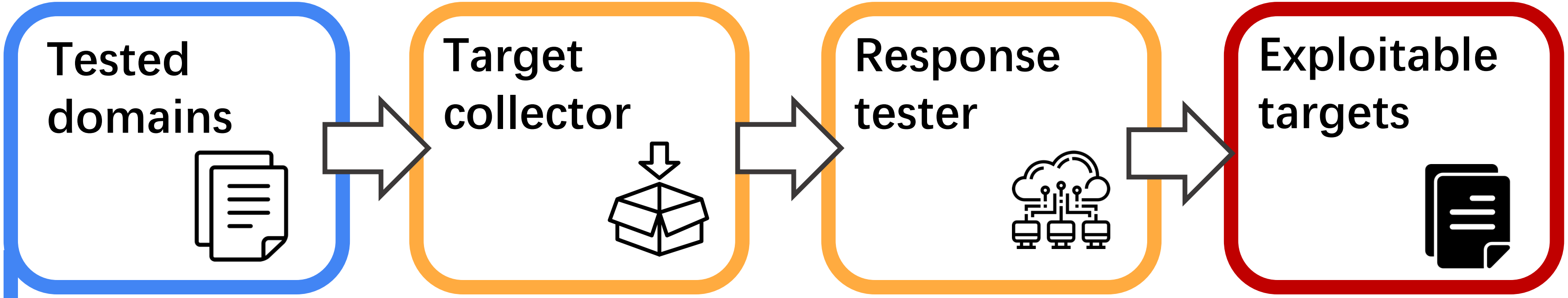
Evaluating Exploitable Targets

Part I: hosted domains, authoritative servers, and vendors

Methodology

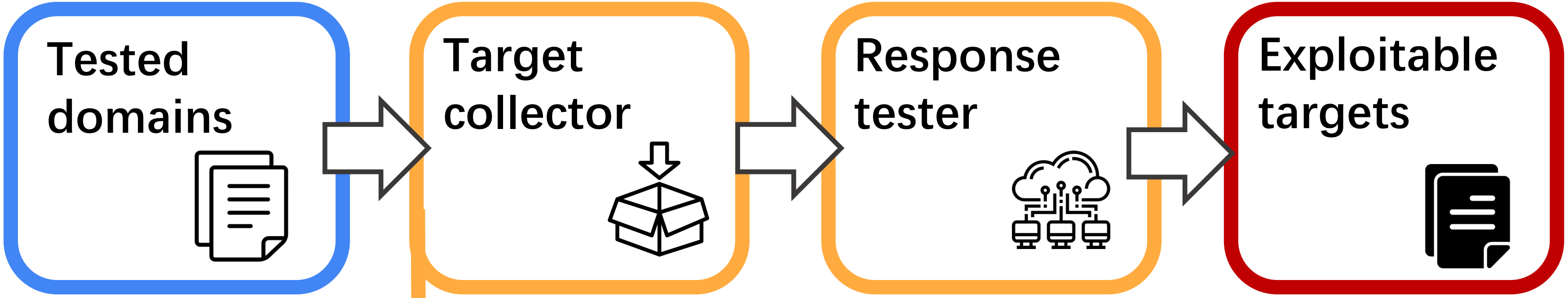


Methodology



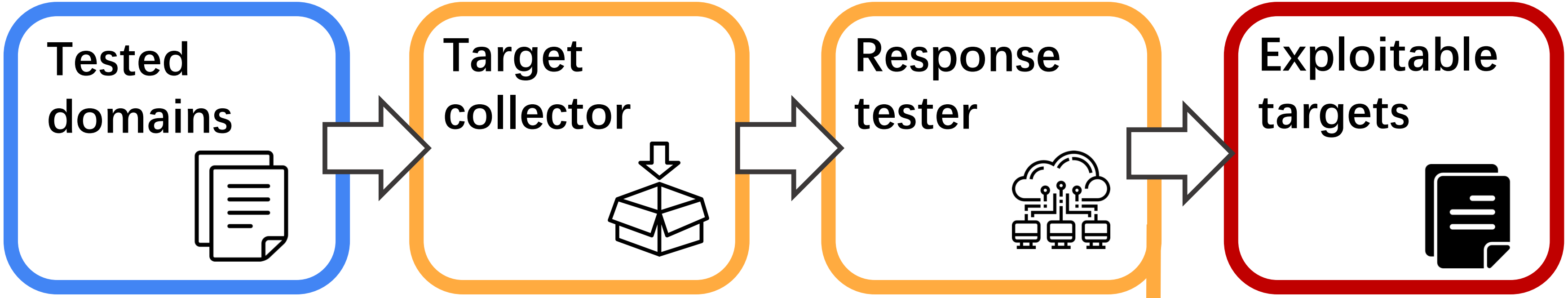
- Top 1M SecRank FQDNs
- Top 1M Tranco SLDs

Methodology



For each targeted domain:
Request their nameservers

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%

Exploitable domains among **the top 100 FQDNs**:

- API for a mobile operating system
- Medical service
- E-commerce
- Short-form video applications

Exploitable authoritative servers and vendors

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

Exploitable authoritative servers and vendors

- **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**

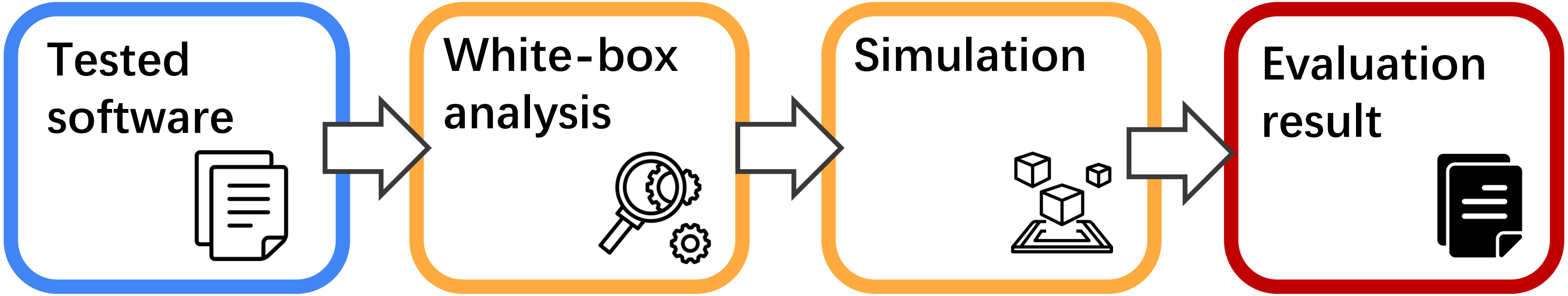
Top 10 affected providers for the top sites

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**

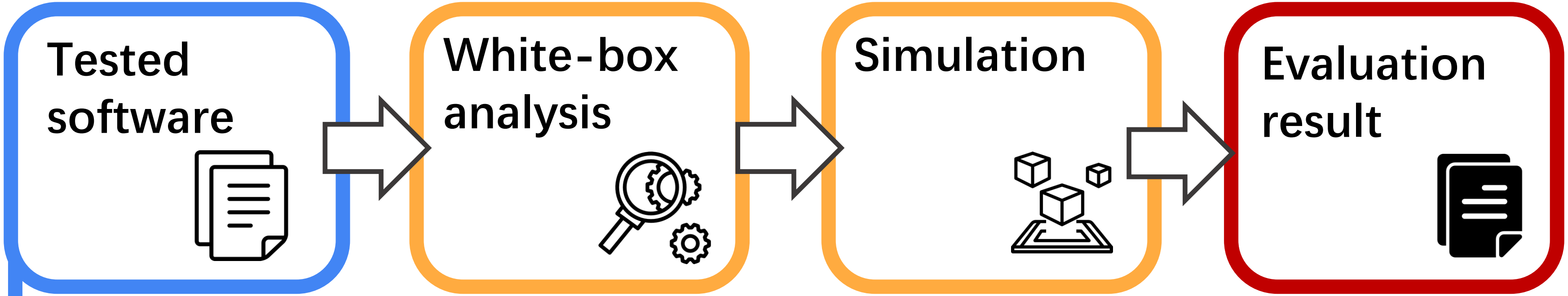
Evaluating Exploitable Targets

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

Methodology: software analysis

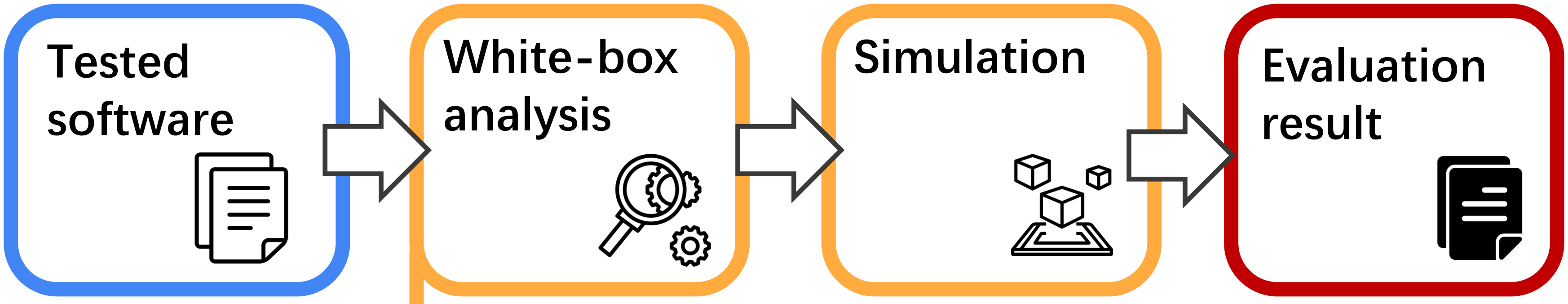


Methodology: software analysis



- BIND9
- Unbound
- PowerDNS
- Knot Resolver
- Microsoft DNS

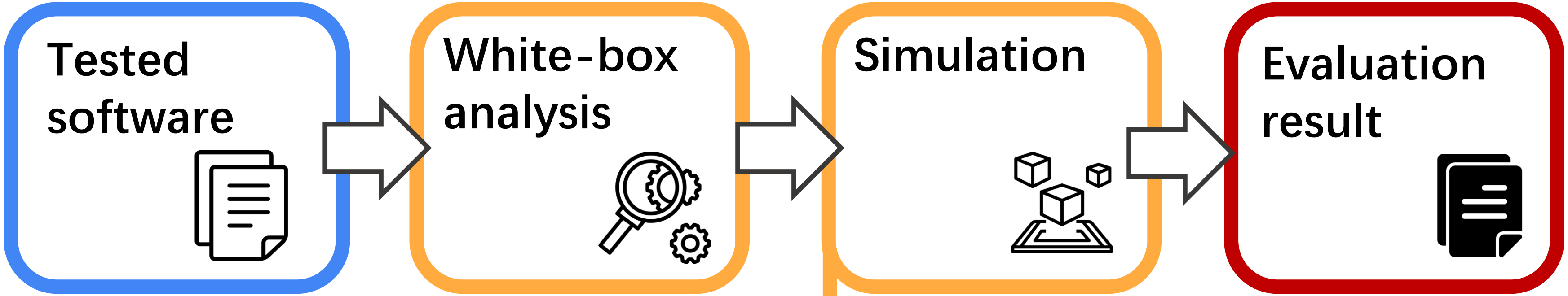
Methodology: software analysis



For open-source software:

- Code reviewing
- Dynamic debugging

Methodology: software analysis



Conducting software simulation covering all conditions affecting attacking efficiency

Result: software analysis

Three vulnerable software enjoys a **high market share** [1] are vulnerable

BIND 9 — Market share: 60.2+%

POWERDNS — Market share: 3.2+%

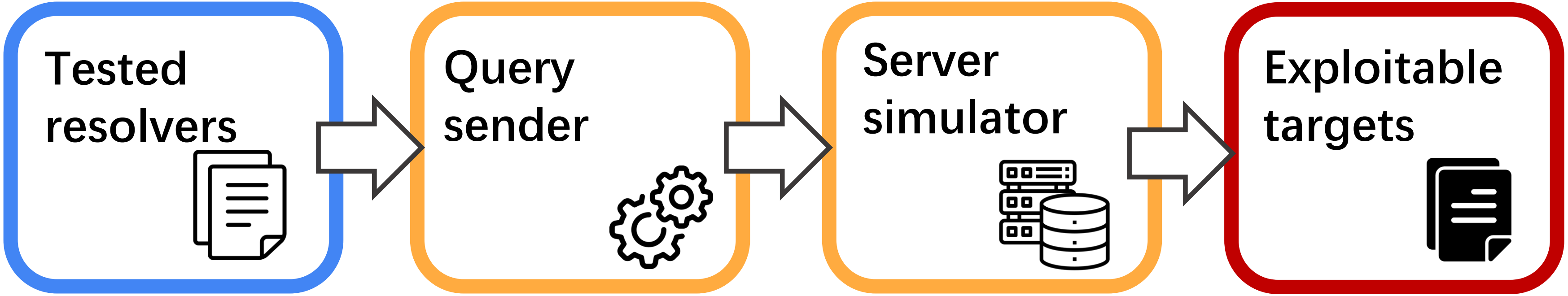
Microsoft — Market share: 2.5+%

The **attacking efficiency is high**

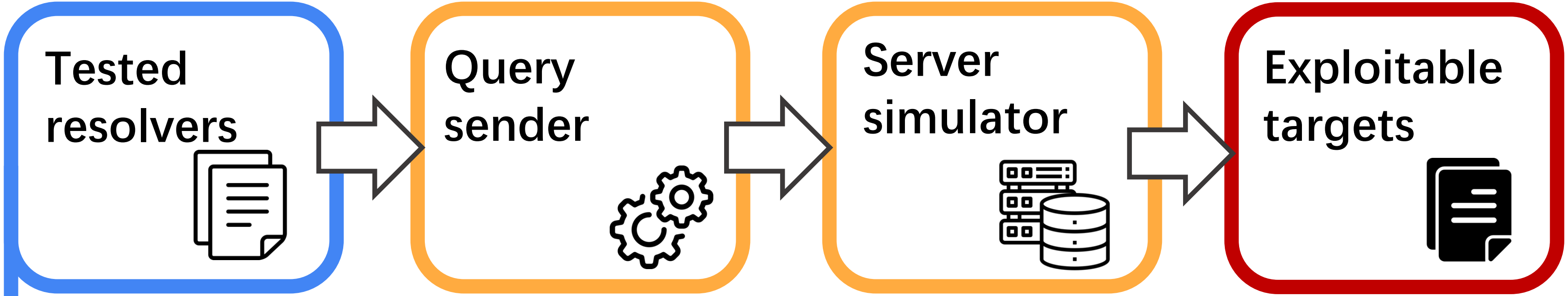
- Example: after receiving **one attacking query**, BIND9 sent around **5,730 legitimate queries** to the targeted nameserver

[1] 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.

Methodology: measurement

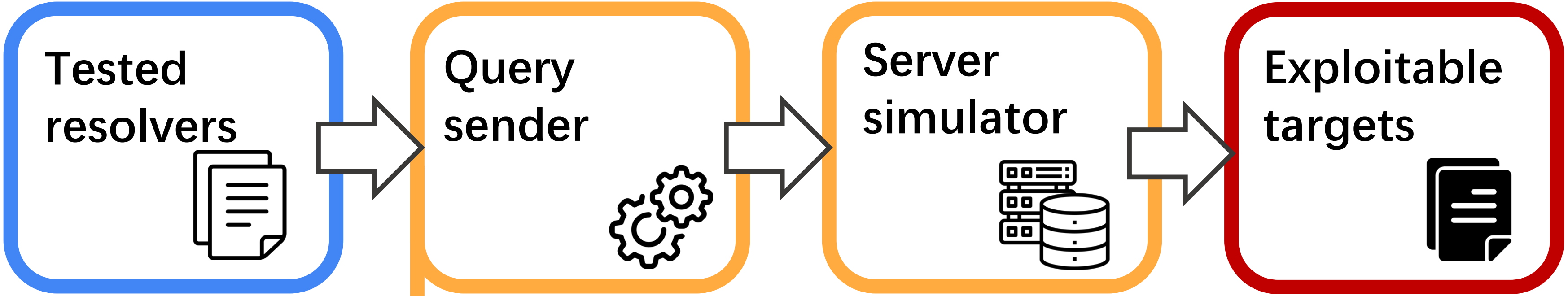


Methodology: measurement



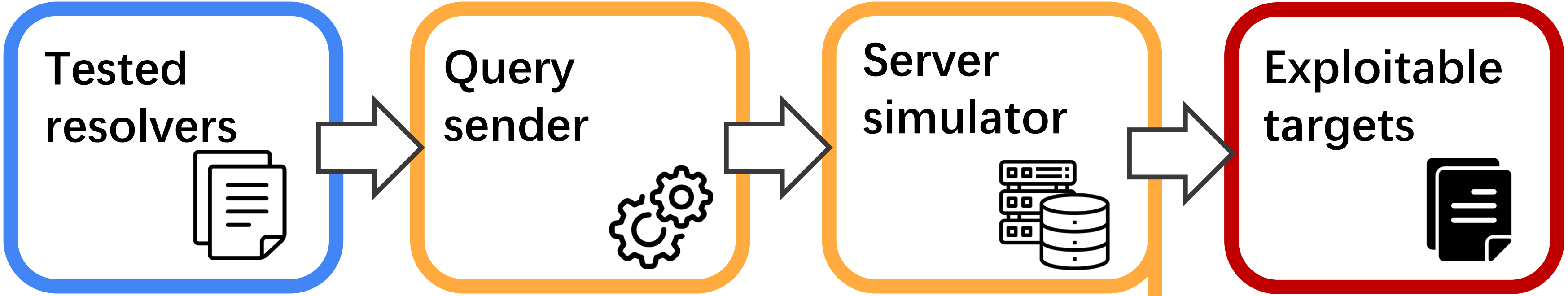
- 37,843 stable open resolvers
- 14 public DNS services

Methodology: measurement



Simulate the attacker and
benign clients to send queries

Methodology: measurement

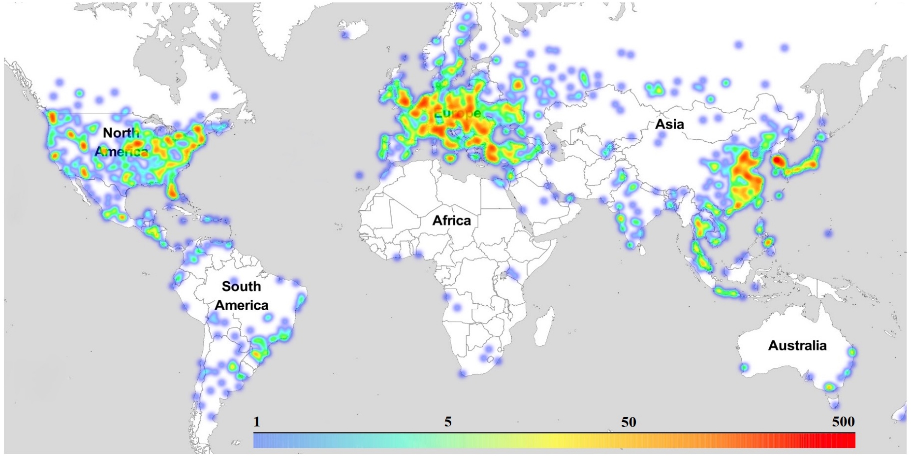


- established a set of vulnerable nameservers
- utilized our own domains

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**



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

Mitigation: fix from the side of authoritative servers

Root reason: authoritative servers dropping queries for non-authoritative domains to protect against DNS amplification attacks.

RFC 8906: Failing to respond at all is always incorrect.

Mitigation: fix from the side of authoritative servers

Root reason: authoritative servers dropping queries for non-authoritative domains to protect against DNS amplification attacks.

RFC 8906: Failing to respond at all is always incorrect.

Recommendation: returning REFUSED with an EDNS error code

- REFUSED does not generate more packets than attackers'

Disclosure and feedback

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

Conclusion

Novel attack. Uncovered a vulnerability to disrupt 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

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

zfl23@mails.tsinghua.edu.cn