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

Xiang Li [1]  Dashuai Wu [1]  Haixin Duan [1 2 3] ✉  Qi Li [1] ✉

[1] Tsinghua University  [2] Zhongguancun Laboratory  [3] Quan Cheng Laboratory  ✉ Corresponding Author(s)

NISL Lab
Tsinghua University

## DNS Resolution and Mechanisms

- Translate human-friendly domain names into machine-readable IP addresses and vice versa.
- **Multiple resolver roles:** stub, forwarder, recursive, and authoritative.
- **Iterative resolution process:** C/S style, recursive resolution, and caching.

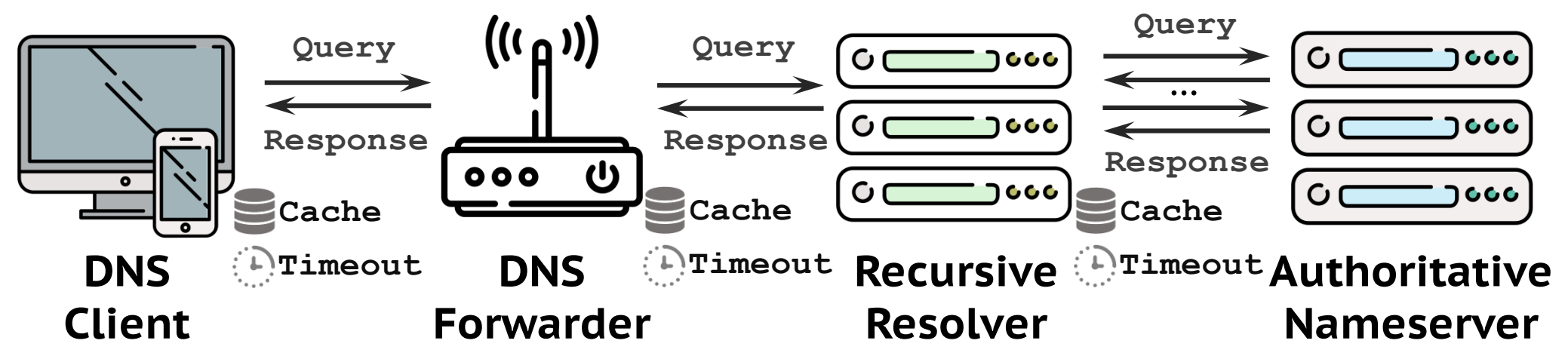

Figure 1. General DNS resolver roles and domain name resolution process.

- **DNS resolution timeout:** waiting for responses from the auth. (**Guaranteeing availability**).
- **DNS query aggregation:** issuing one resolver-query for multiple simultaneous client-requests on the same domain name (**Protecting security**).
- **DNS response fast-returning:** returning responses to the client when receiving valid responses from the auth. (**Enhancing reliability**).
- **ENDS0** (Increasing the packet size). **IP defragmentation timeout**.

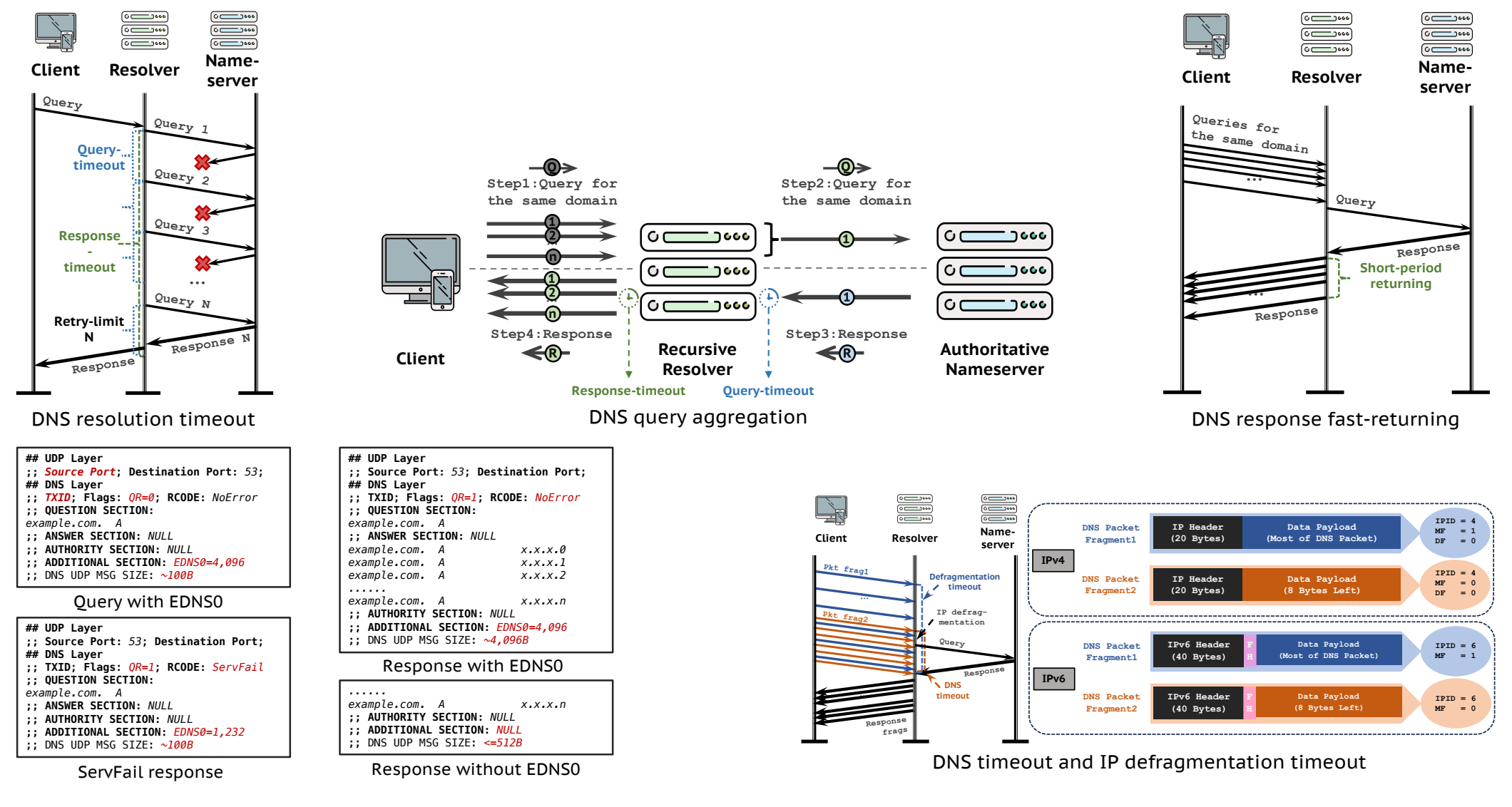

Figure 2. DNS mechanisms.

## DNS DoS Attacks

- **Flooding a target** with amount of DNS traffic via amplification (**Can be easily detected**).

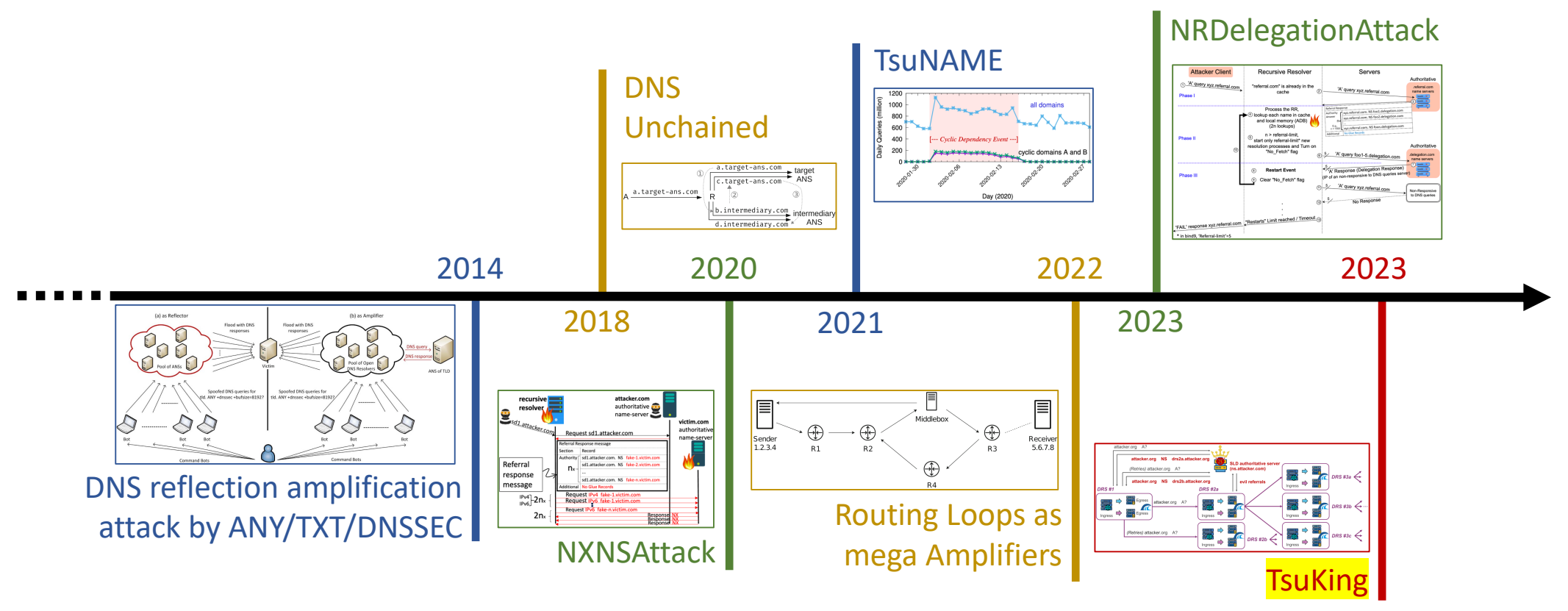
DNS Unchained
TsuNAME
NRDelegationAttack
2014
2018
2020
2021
2022
2023
2023
DNS reflection amplification attack by ANY/TXT/DNSSEC
NXNSAttack
Routing Loops as mega Amplifiers
TsuKing

Figure 3. Timeline of DNS DoS attacks.

## Pulsing DoS Attack

- **Method:** concentrating a low-rate traffic into **a high-rate pulsing** to occupy bandwidth.
- **Impact:** cannot be detected by traditional IDS (**Low-rate among a while**), causing packets loss.
- **Shortcomings:** state-of-the-art pulsing DoS attacks could only yield **a low amplification factor** or require **a large pulse period (not practical and powerful enough)**.

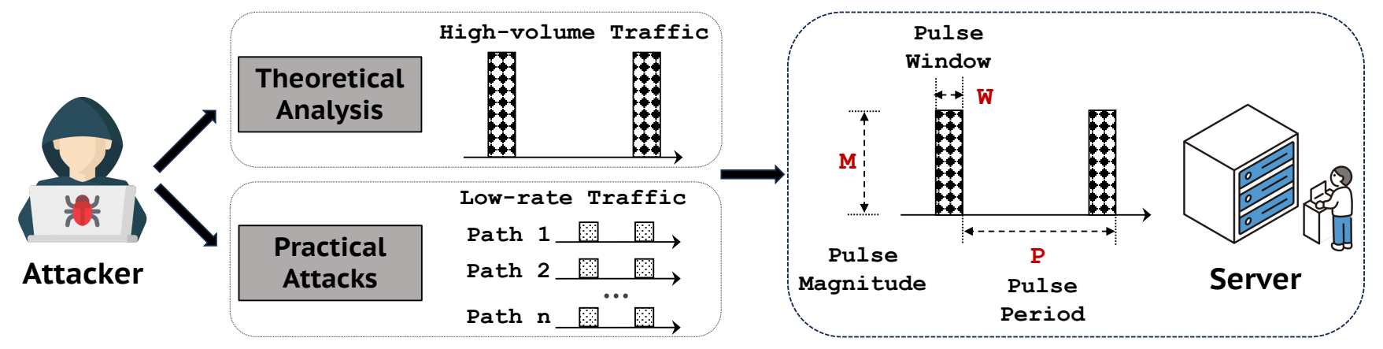

Figure 4. Pulsing DoS attack model.

## DNSBomb Attack [1]

- A new practical and powerful DNS-based **pulsing DoS attack**, like a bomb (Blast wave).
- Exploiting three inherent DNS mechanisms (**Defense**) to DoS (**Attack**): **timeout**, **query aggregation**, and **response fast-returning**. Peak pulse: **>8.7Gb/s**. BAF: **>20,000x**.

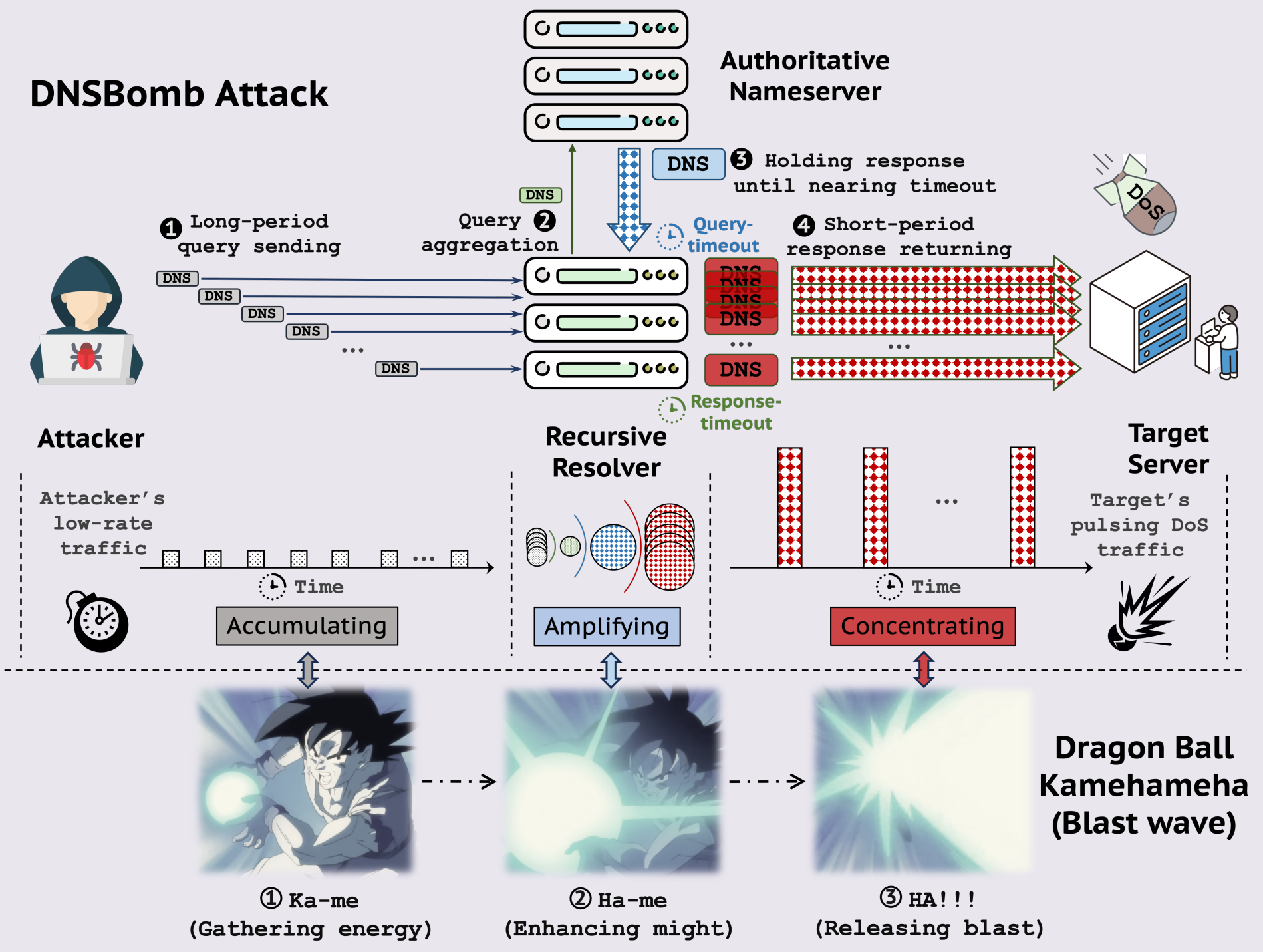
DNSBomb Attack
Authoritative Nameserver
DNS
❸ Holding response until nearing timeout
❶ Long-period query sending
Query ❷ aggregation
Query-timeout
❹ Short-period response returning
DoS
Response-timeout
Attacker
Recursive Resolver
Target Server
Attacker's low-rate traffic
Time
Target's pulsing DoS traffic
Accumulating
Amplifying
Concentrating
Dragon Ball Kamehameha (Blast wave)
① Ka-me (Gathering energy)
② Ha-me (Enhancing might)
③ HA!!! (Releasing blast)

Figure 5. DNSBomb attack.

## Local Experiments

- **10 DNS software:** testing attack factors (Timeout, pkt. size, returning-time) and experiments.

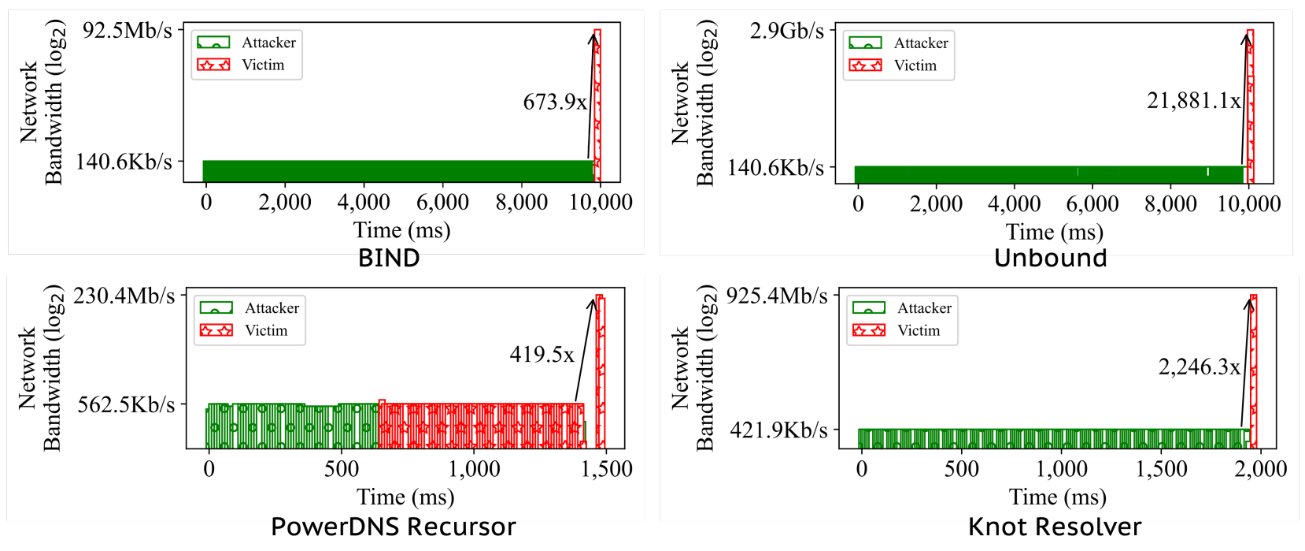

Figure 6. Part of local experiments.

## DNSBomb Attack Evaluation

- **Long-term evaluation (Unbound):** sending 1k queries in each round (10s) for 10m (**Stable**).
- **Attack experiments:** occupying bandwidth, and attacking a DNS resolver, HTTP/2 and HTTP/3 website. **Bandwidth, resolver, and HTTP/2 are well impacted**, while HTTP/3 not.

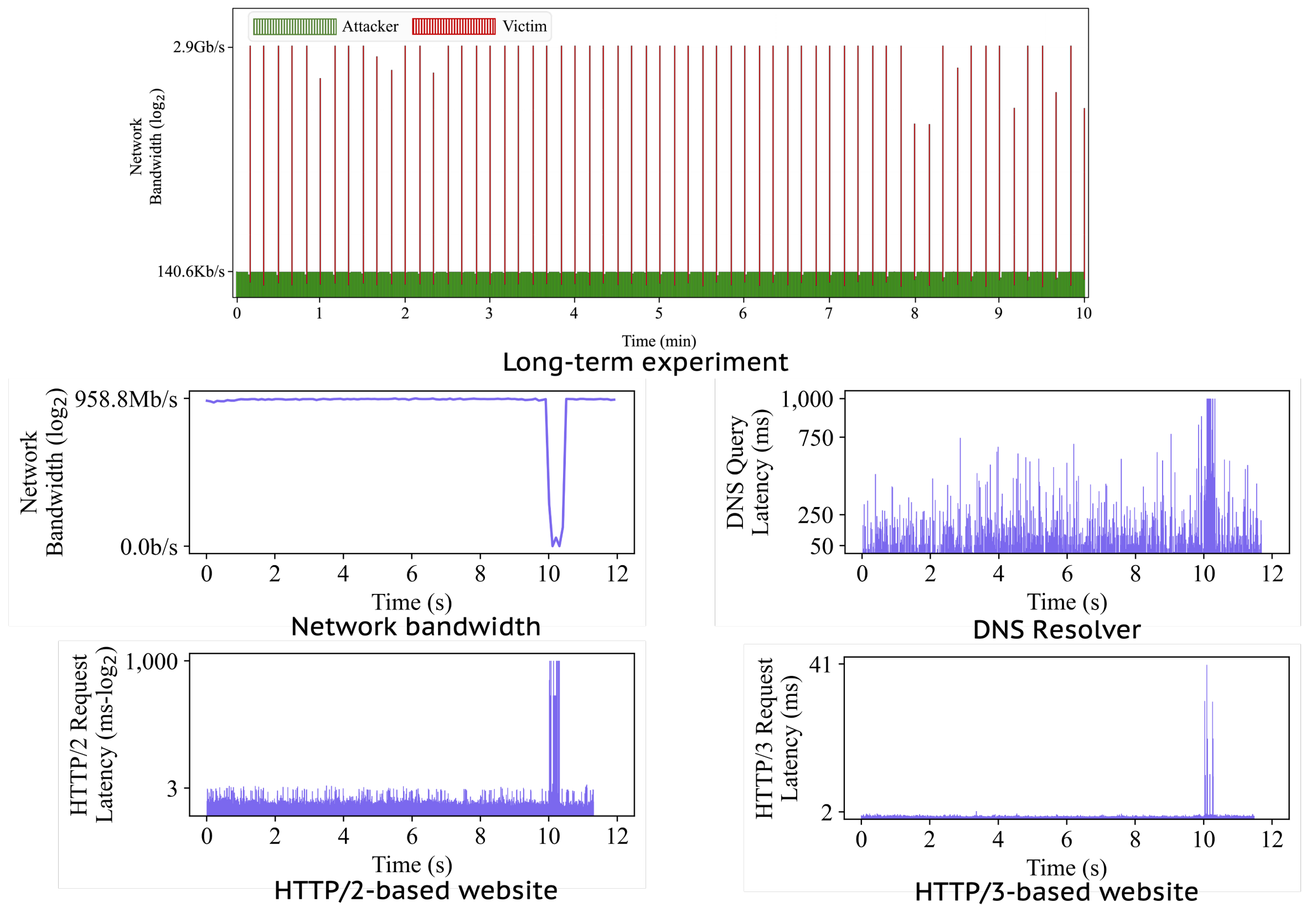

Figure 7. DNSBomb attack evaluation.

## Vulnerable Population and Mitigation Solution

- **Vulnerable:** **10/10** DNS software, **46/46** public services, and **1.8M** open resolvers (**all DNS implementations** are affected with one industry-wide **CVE-2024-33655**).
- **Mitigation:** restricting **timeout**, **rate-limit**, **packet size**, and **response-returning time**.
- **Disclosure:** **20 vendors** confirmed TuDoor with **10 CVEs** assigned for DNS software.

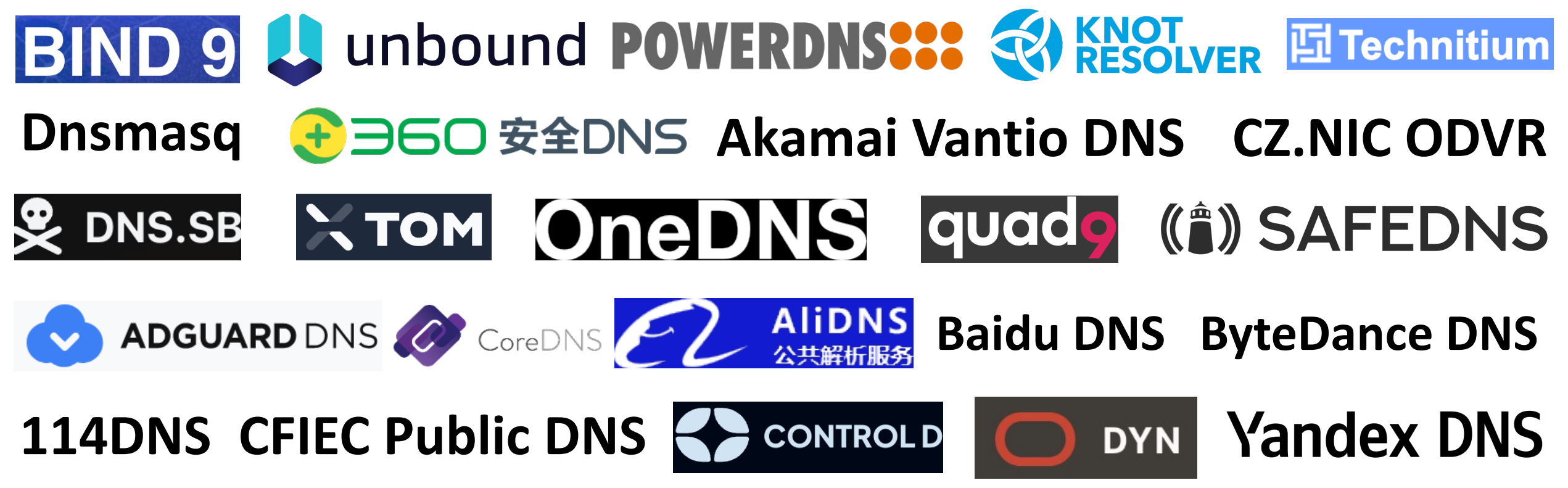

Figure 8. Part of vulnerable DNS vendors.

## References

[1] Xiang Li, Dashuai Wu, Haixin Duan, and Qi Li.
DNSBomb: A New Practical-and-Powerful Pulsing DoS Attack Exploiting DNS Queries-and-Responses.
In *Proceedings of 2024 IEEE Symposium on Security and Privacy*, IEEE S&P '24, 2024.