



OARC 43

Characterizing the DDoS Amplification Power of Open DNS Resolvers to Facilitate Prioritized Mitigation

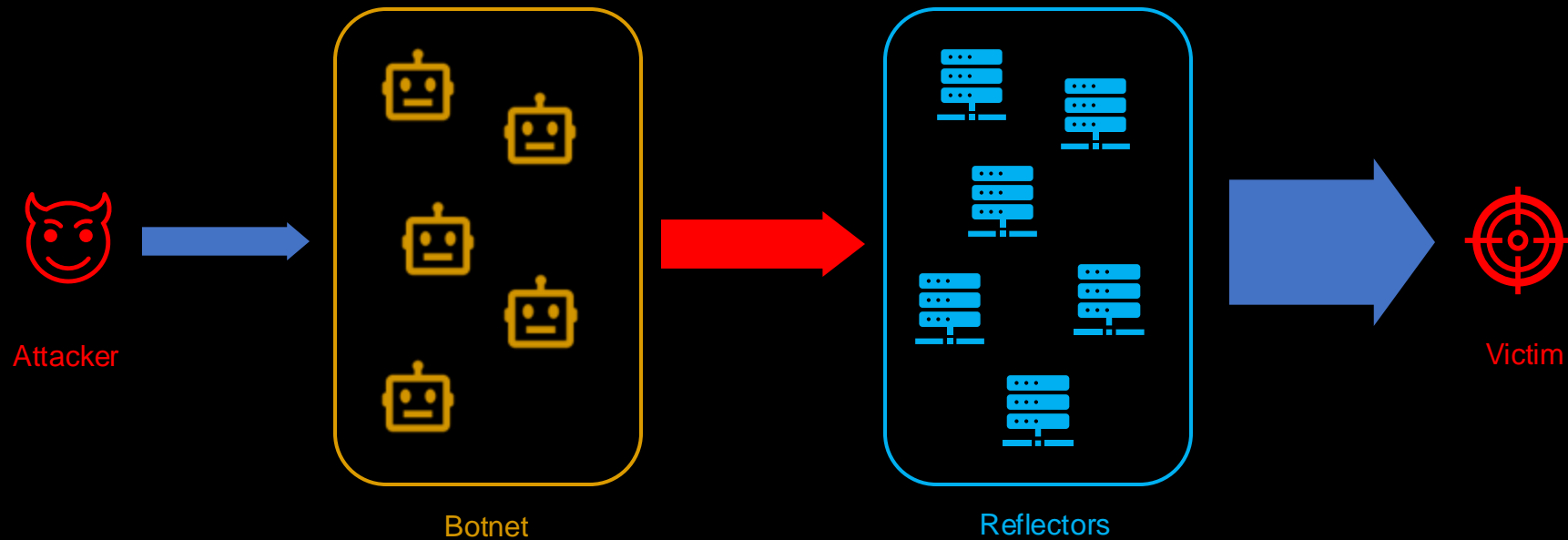
Ramin Yazdani

DNS-OARC 43
27 October 2024
Prague

UNIVERSITY
OF TWENTE.

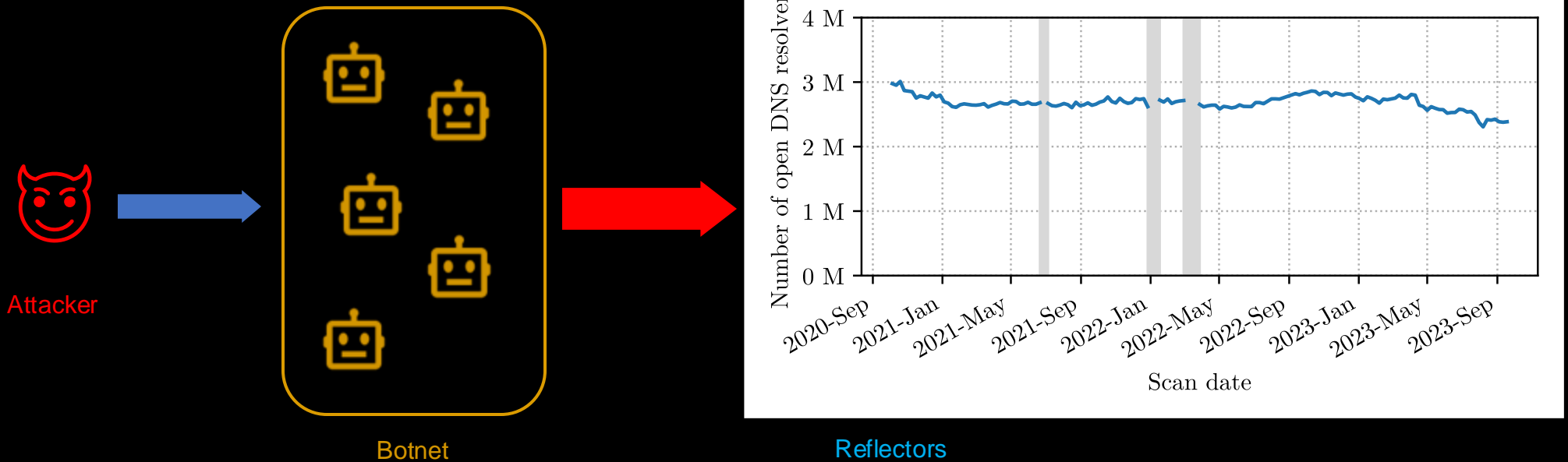
An Old but Persistent Problem

Reflection-based DDoS attacks continue to disrupt networks and services to date



An Old but Persistent Problem

Reflection-based DDoS attacks continue to disrupt networks and services to date



From Mirai to Meris to Mantis



Multiple hundred thousands of IoT devices

2016



Tens of thousands of Mikrotik routers

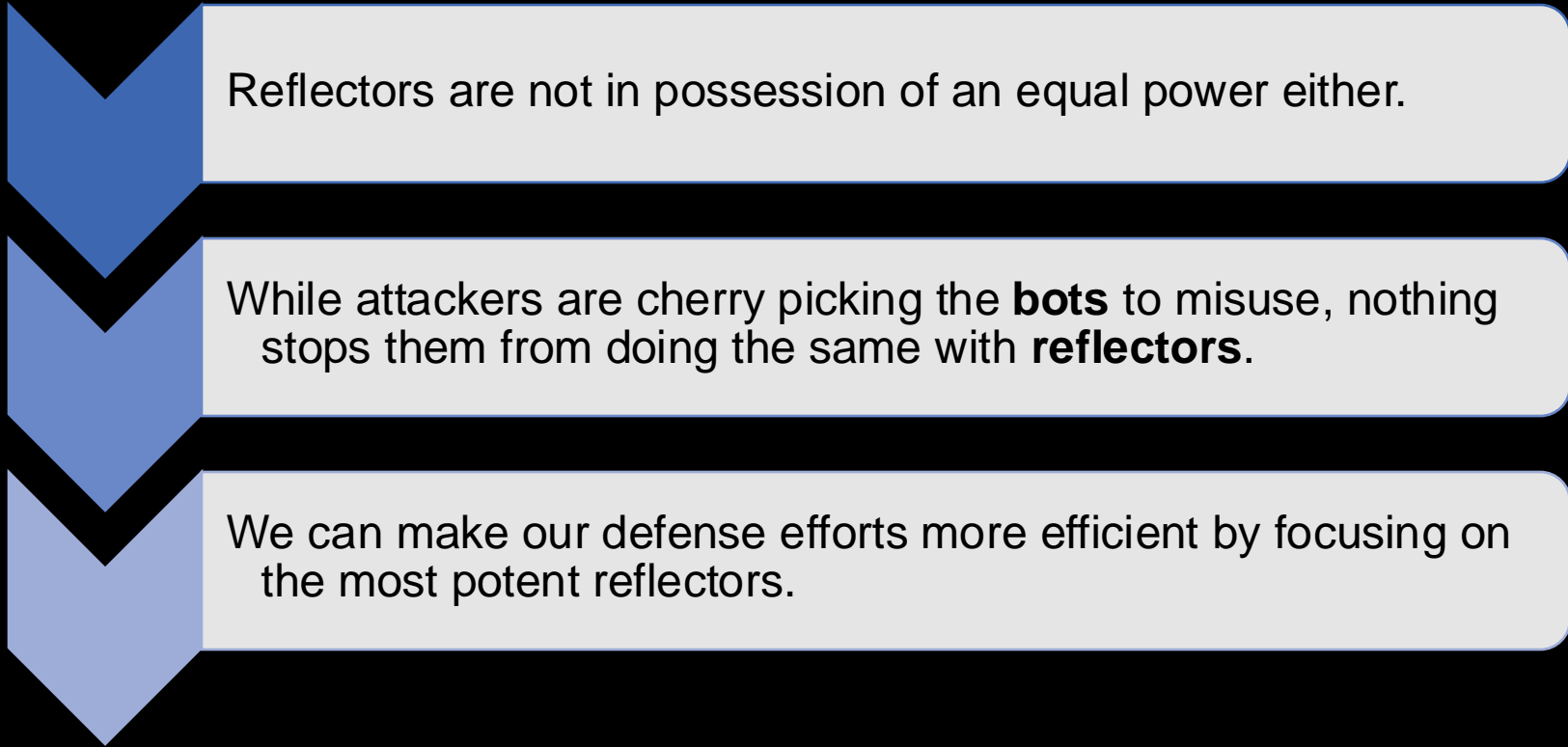
2021



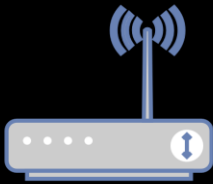
Thousands of servers and virtual machines

2022

Our Motivation

- 
- Reflectors are not in possession of an equal power either.
 - While attackers are cherry picking the **bots** to misuse, nothing stops them from doing the same with **reflectors**.
 - We can make our defense efforts more efficient by focusing on the most potent reflectors.

Aspects that we Study



Network connectivity

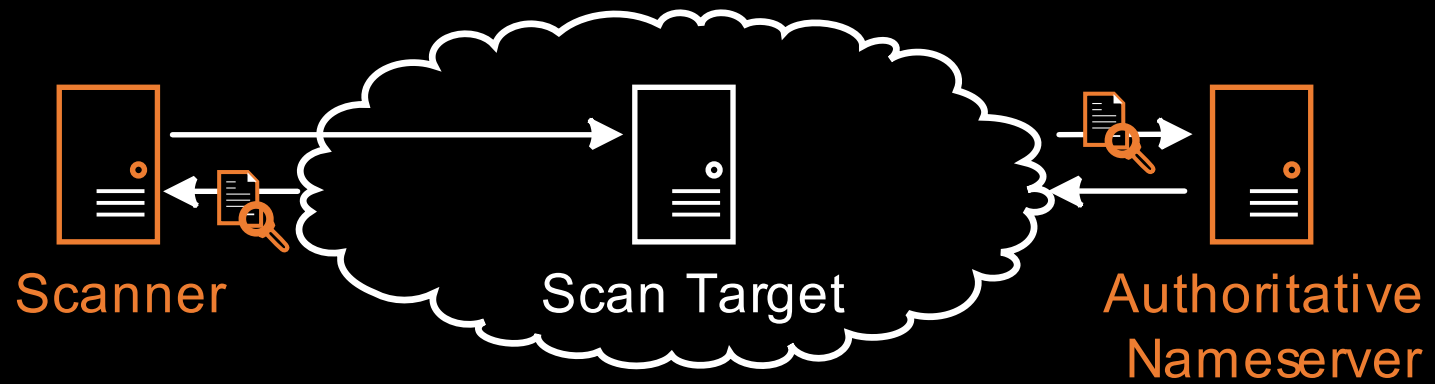


Bandwidth Amplification

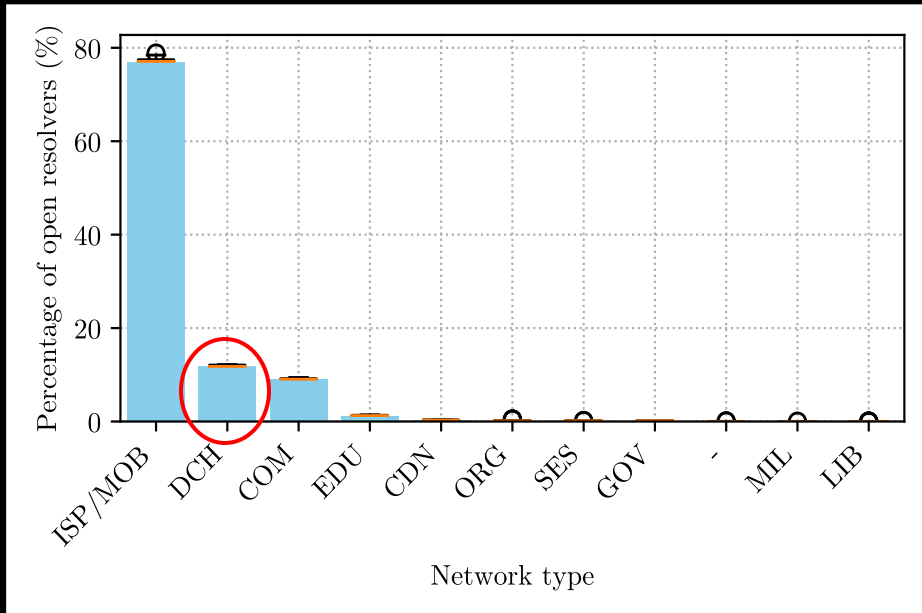


Packet Amplification

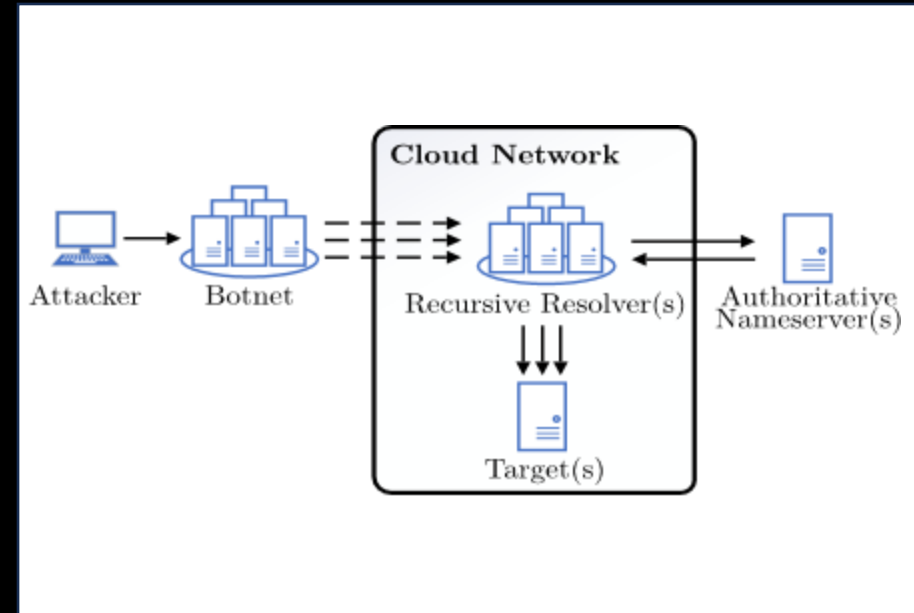
Measurement Setup



Key Findings (Network Connectivity)



A non-negligible share of reflectors are hosted in datacenters/clouds.

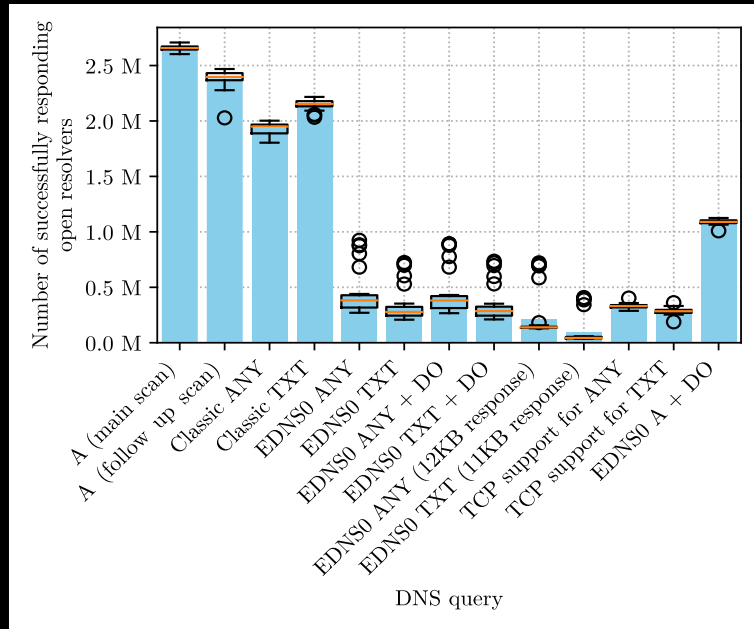


Some cloud providers expose their infrastructure to reflection-based DDoS attacks.

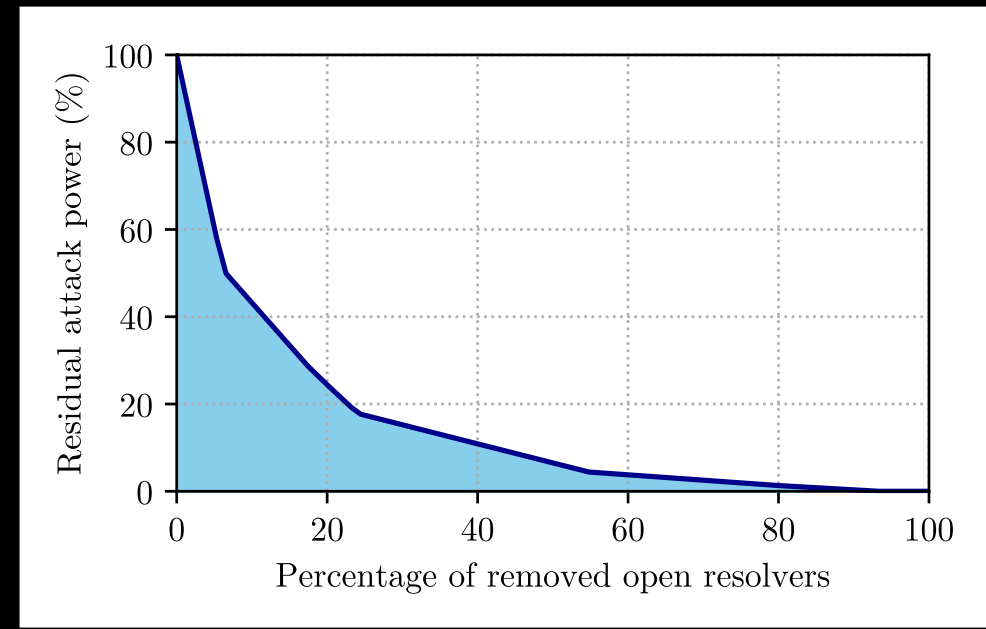


[1] R. Yazdani et al., *Mirrors in the Sky: On the Potential of Clouds in DNS Reflection-based Denial-of-Service Attacks*, RAID'22.

Key Findings (Bandwidth Amplification)



A large group of open resolvers lack DNSSEC support. This stands to substantially limit attackers when misusing DNSSEC.

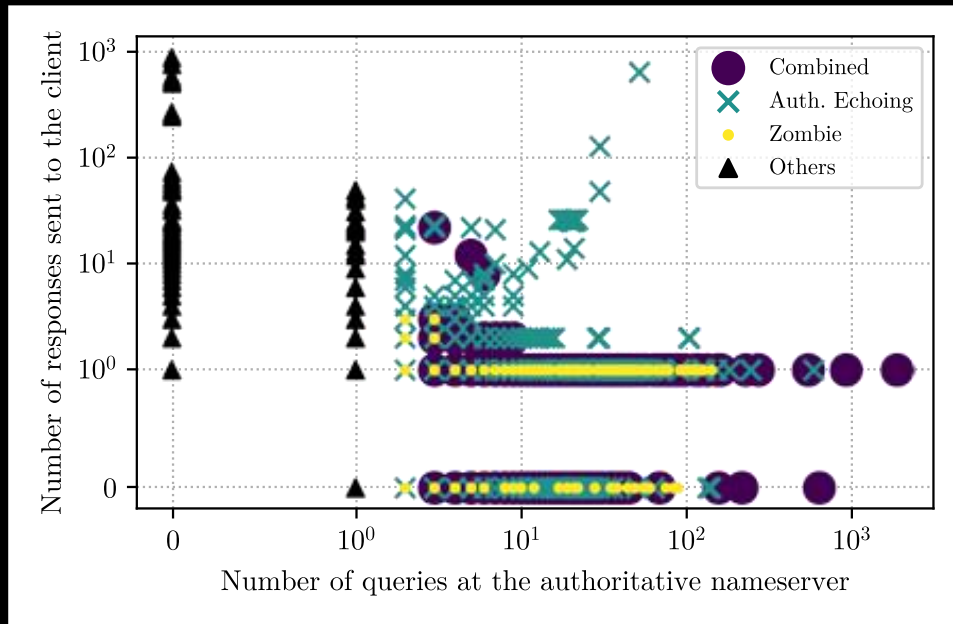


By focusing on just the 20% most potent amplifiers, we can reduce the Internet-wide DNS-reflection attack potential by up to 80%.

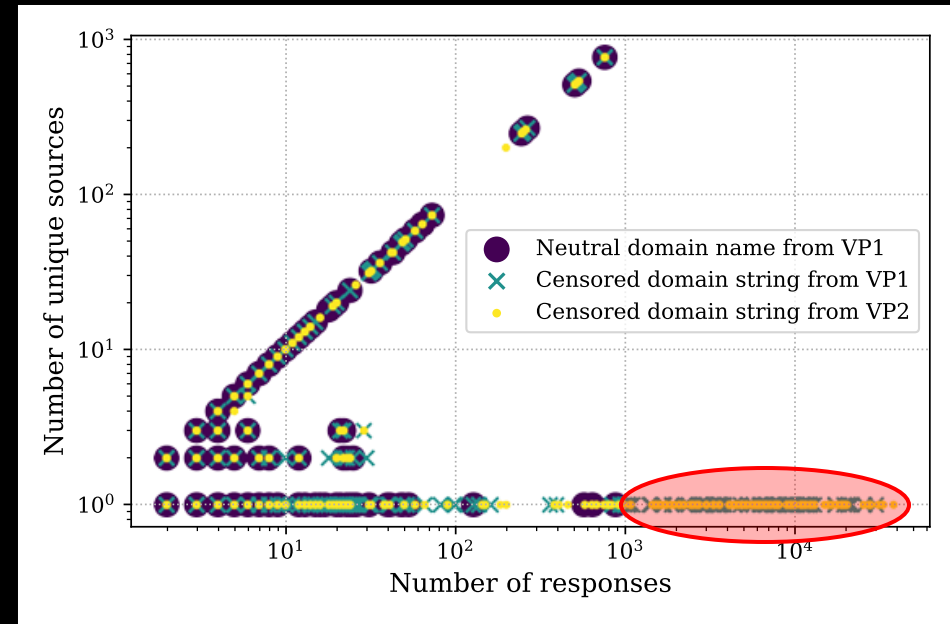


[2] R. Yazdani et al., *A Matter of Degree: Characterizing the Amplification Power of Open DNS Resolvers*, PAM'22.

Key Findings (Packet Amplification)



Packet amplification happens both on the client end as well as the authoritative nameserver end.

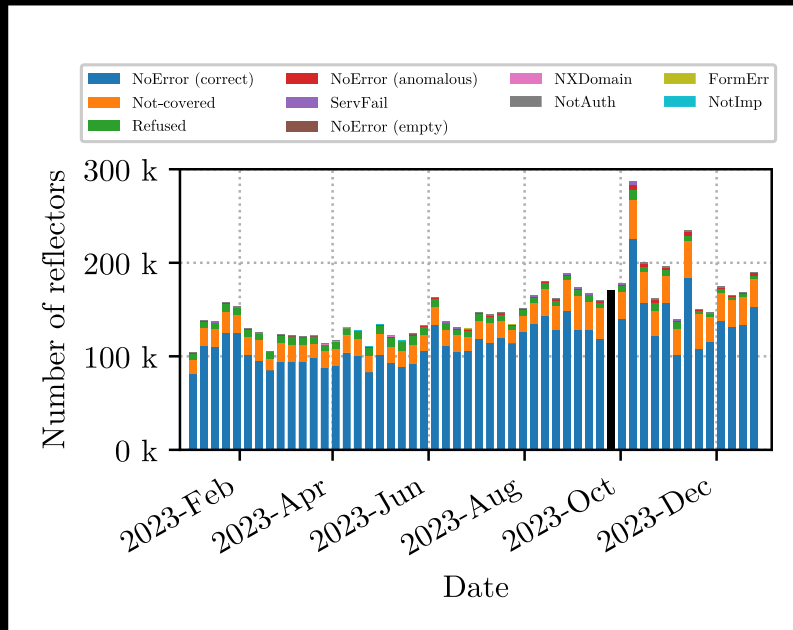


DNS middleboxes can be triggered to send tens of thousands of responses, hence increasing their abuse potential in DDoS attacks.

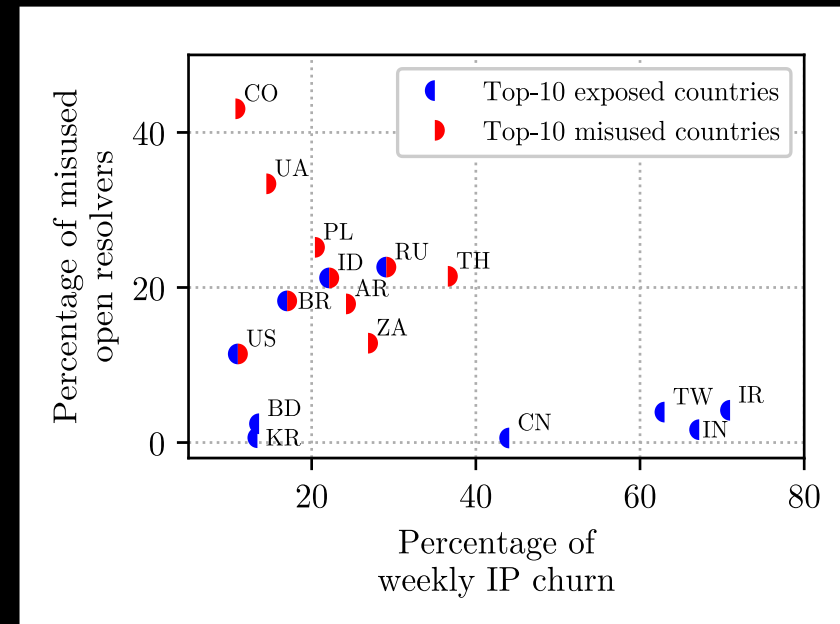


[3] R. Yazdani et al., *Hazardous Echoes: The DNS Resolvers that Should Be Put on Mute*, TMA'23.

Key Findings (Reflectors in Attacks)



Open recursive resolvers are not the only contributors to DNS-based DDoS attacks.



Open resolvers with a higher IP churn are involved less in DDoS attacks.

[4] R. Yazdani et al., *Glossy Mirrors: On the Role of Open DNS Resolvers in Reflection and Amplification DDoS Attacks*, *CNSM'24*.

Conclusions

- The number of exposed open resolvers is much higher than what attackers typically misuse.
- Our characterization shows differences in the amplification power of open resolvers that can be leveraged for a prioritized mitigation.
- Attackers do not yet fully leverage the diversity among open resolvers, meaning that we can expect the intensity of DNS-based DDoS attacks to grow if we do not take action.

Thanks!

