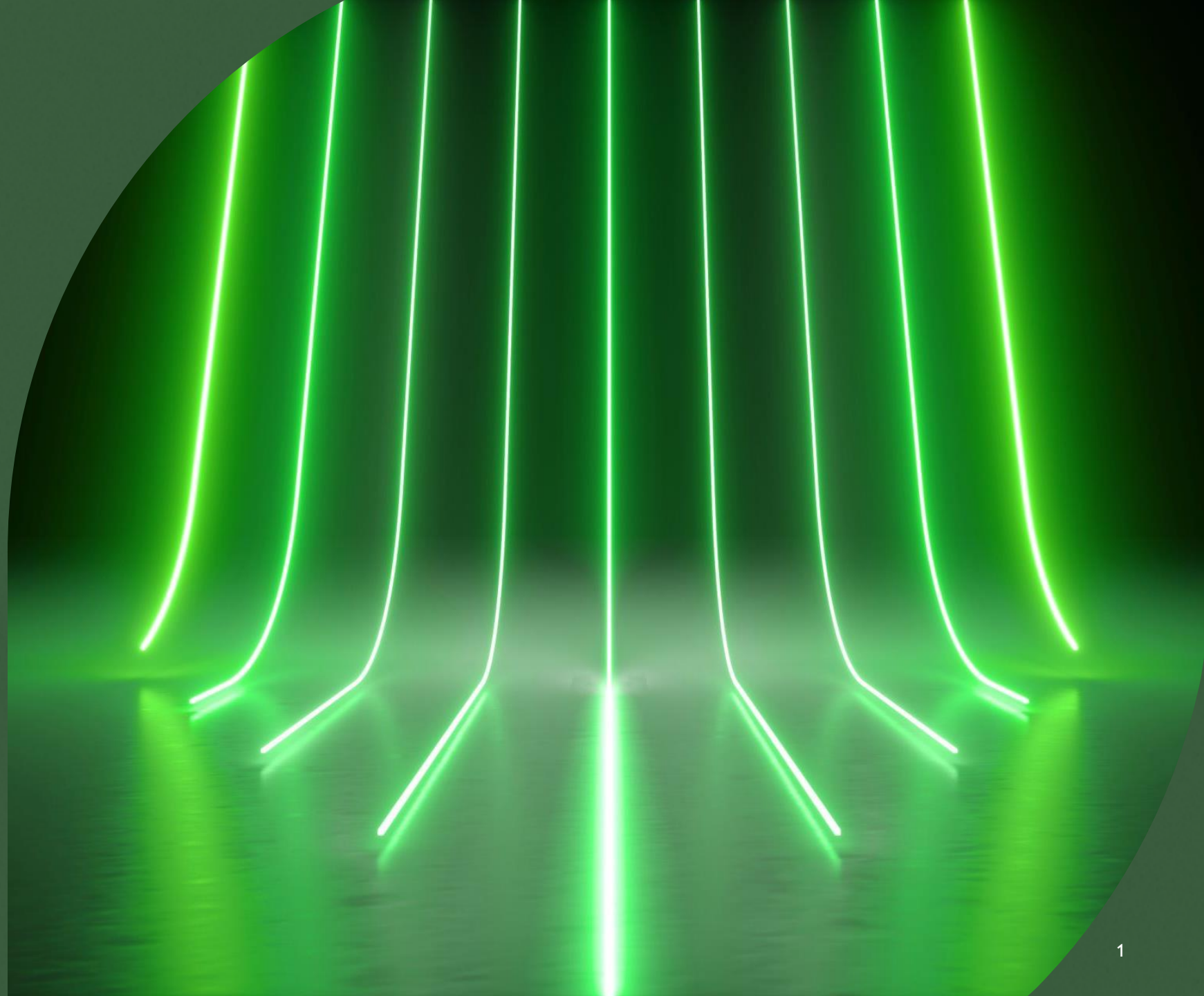
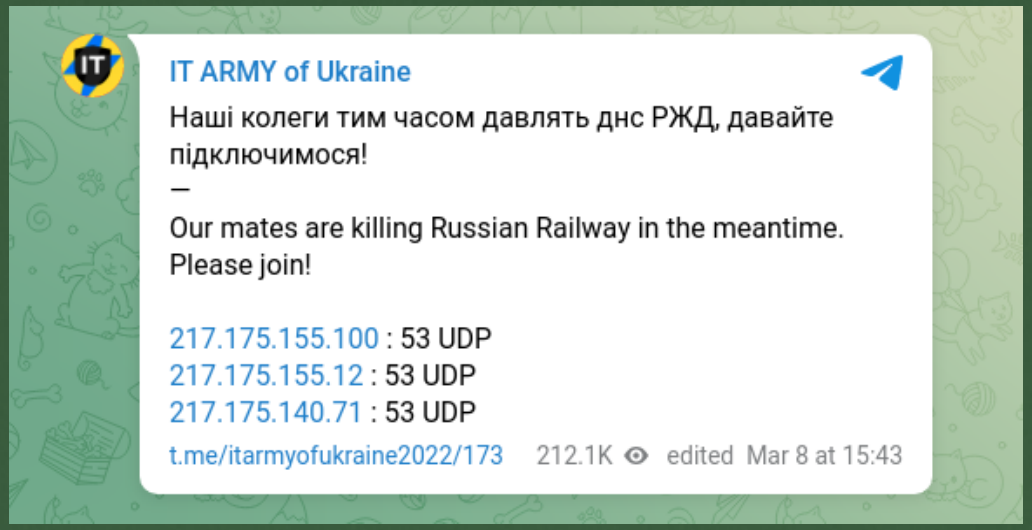
Investigating the impact of DDoS attacks on DNS infrastructure

Raffaele Sommese[1], KC Claffy[2], Roland van Rijswijk-Deji[1], Arnab Chattopadhyay[1], Alberto Dainotti[3], Anna Sperotto[1], Mattijs Jonker[1]

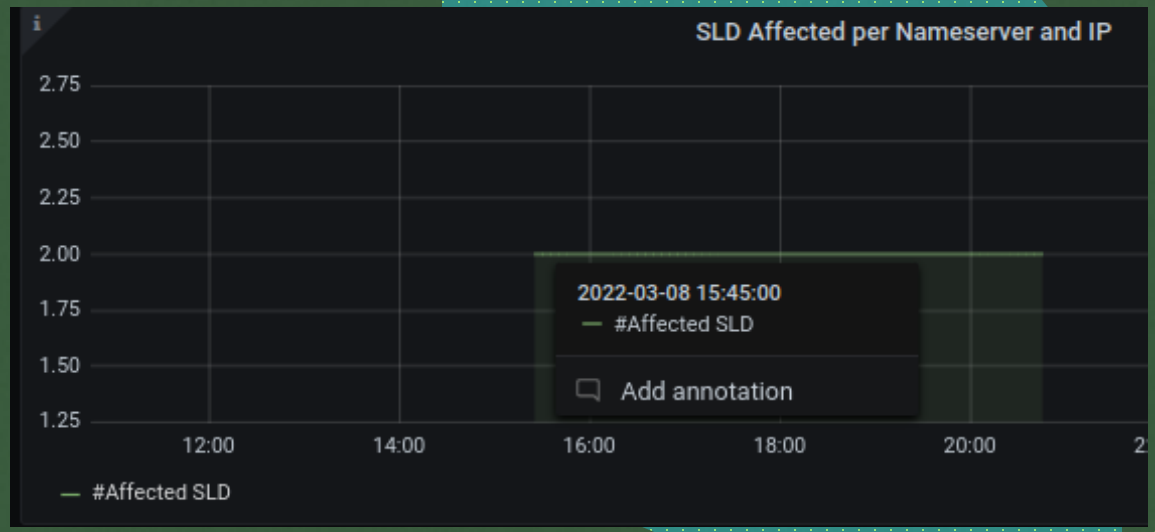
[1]University of Twente,
[2]CAIDA/UC San Diego,
[3]Georgia Institute of Technology



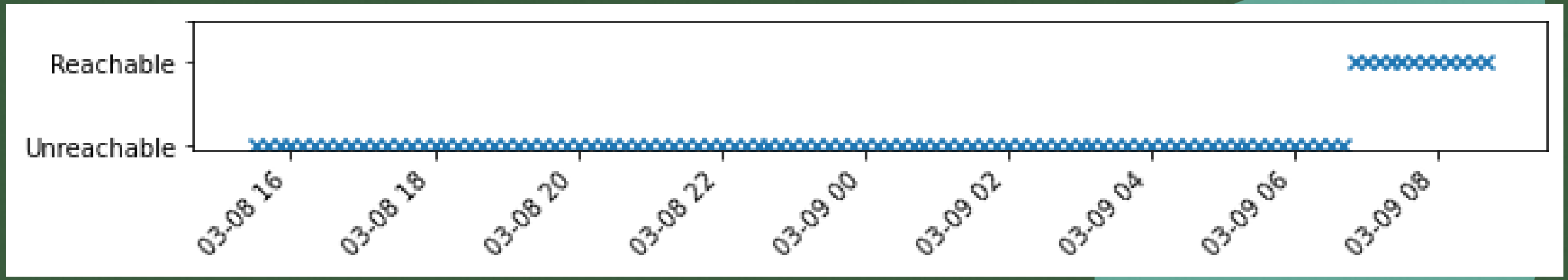
A teaser of this talk



Telegram coordination



Attack detected by UCSD Network Telescope



Reactive DNS Measurements

Outline

- The datasets used for this work.
- The insights on DDoS impact on the DNS ecosystem.
- A longitudinal analysis of 1 year and five months.
- Performance impairments and reachability related to those attacks.
- Effectiveness of DNS resilience techniques.

RSDoS Attacks

- Randomly spoofed attacks involve randomly spoofing the source IP address to overload targets.
- RSDoS feed from UCSD Network Telescope.
- 5-minute window of statistics feed of response packets sent by victims.
- A lower bound of DoS attacks against specific IP addresses.

RSDoS Attacks

Collected information we used in this work:

- Target IPs
- Number of /16 subnets in the telescope that receive packets from victim
- Protocol
- First observed port
- Number of unique ports targeted
- Peak observed packet rate during the window

4,039,485 inferred attacks from November 2020 to March 2022

OpenINTEL DNS Queries

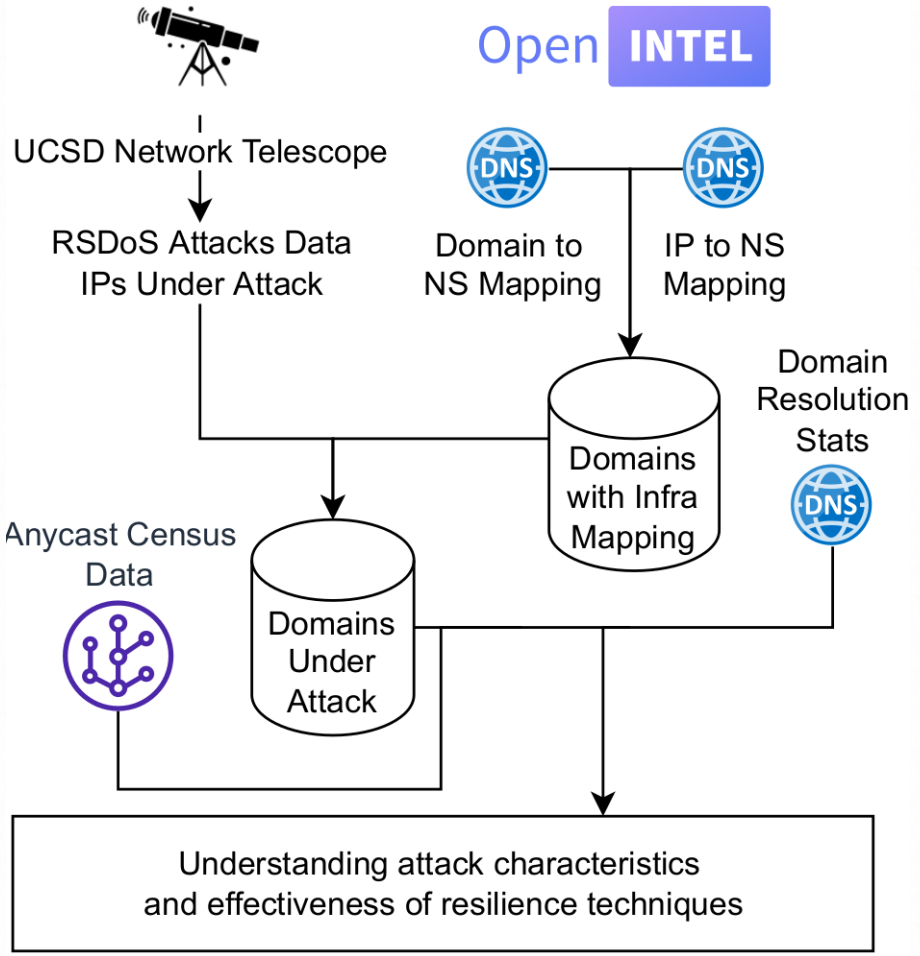
- OpenINTEL performs daily querying of a large portion of the DNS space including and storing:
  - **NS** queries
  - **round-trip time (RTT)**
  - response **status codes**
- OpenINTEL uses *unbound* to "randomly" select an authoritative nameserver.

Datasets: Anycast Census and Additional Datasets

- Quarterly IPv4 Anycast census from MAnycast2 Project.
- CAIDA's prefix-to-AS dataset to map IP addresses to the AS number(s).
- CAIDA's AS-to-organization to map AS numbers to organizations.
- Open resolver scans of Yazdani et al. to filter out IPs of open resolvers in the DNS authoritative.

Joining Datasets Together

1. RSDoS IPs under attack with the list of nameservers on the day before the attack => NSes under attack.
2. Resulting dataset with the list of domain names those nameservers hosted => Domains under attack.
3. The list of domains under attack with our RTT data => Performance
4. Additional metadata => Resilience (?)



Impact on DNS Resolution

- Performance Impairment:

$$Impact\_on\_RTT = \frac{Average\ RTT\ (5\ min)}{Average\ RTT\ (Day\ Before)}$$

- Resolution Failure:
  SERVFAIL, Timeout

Both are calculated on the NSSET!

NSSet

- OpenINTEL's agnostic DNS resolution implies we cannot know which authoritative nameserver responded to a query.
- All nameservers are queried, on large numbers.
- An NSSet is a set of nameservers authoritative for a certain domain.
- Resolution failure => ALL the nameservers unresponsive.
- Performance impairment => Average RTT of the NSSet affected.

The TransIP case

- December 2020, March 2021: Severe series of attacks against TransIP.
- In December, the RTT increased ten-fold for eight consecutive hours.
- In March, ~20% of the queries during the attack completely FAIL to resolve.
- No Anycast and a single ASN for their authoritative Nameservers.

Mil.ru:
How to not operate a DNS server

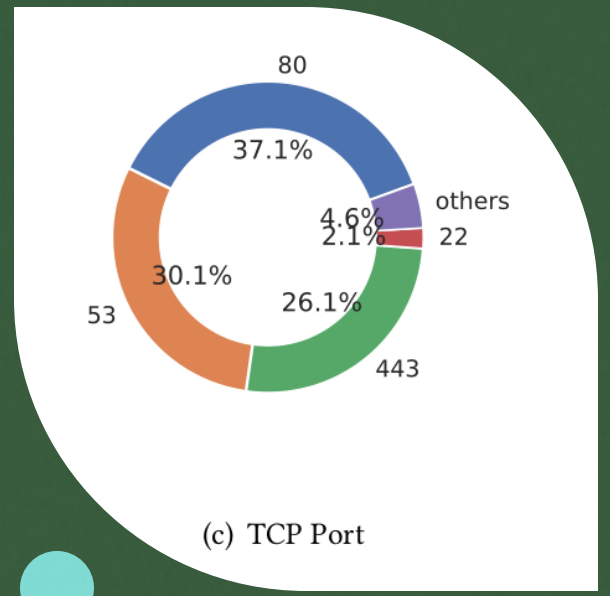
- Nameservers of mil.ru under attack for eight consecutive days, from March 11th to 18th.
- OpenINTEL failed to resolve mil.ru during the attack.
- The three nameservers were unicast, hosted behind the same ASN/company, and even on the same /24 subnet.

Attacks in 2020-2022

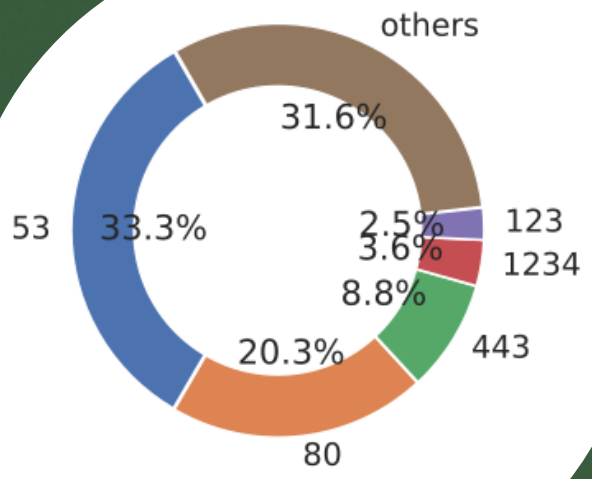
- One year and five months of attacks from November 2020 to March 2022.
- 0.5-2% of RS-DoS attacks observed reached DNS infrastructure!
- Frequent targets: open resolvers, large DNS providers, and hosting companies.
- The most targeted companies: Google, Unified Layer, Cloudflare, OVH and Hetzner.

Attacked Ports

- 80.7% of attacks on DNS authoritative infrastructure targeted a single port.
- Almost 90.4% of these attacks used TCP.
- Most of the TCP attacks targeted port 80
- Most of the UDP attacks targeted port 53.
- DNS itself may not be the primary target of those attacks.



(c) TCP Port

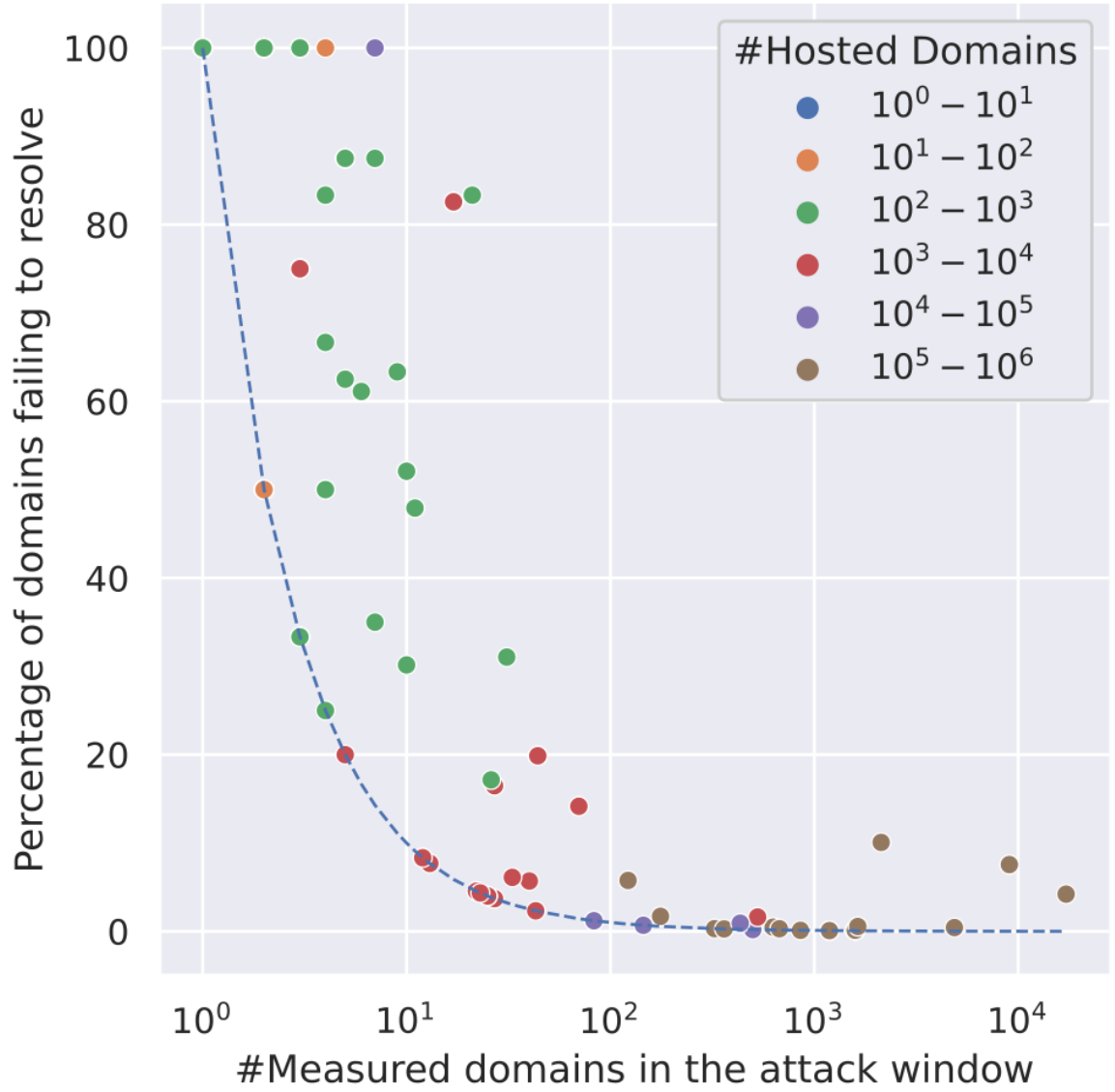


Performance Impact of Attacks

- NSSets with at least **five domains measured** during the attack.
- **12,691 distinct events of attacks** during OpenINTEL **measuring window.**
- In 99% of cases, low to moderate performance impairment.
- In 1% of cases, completely **resolution failure**

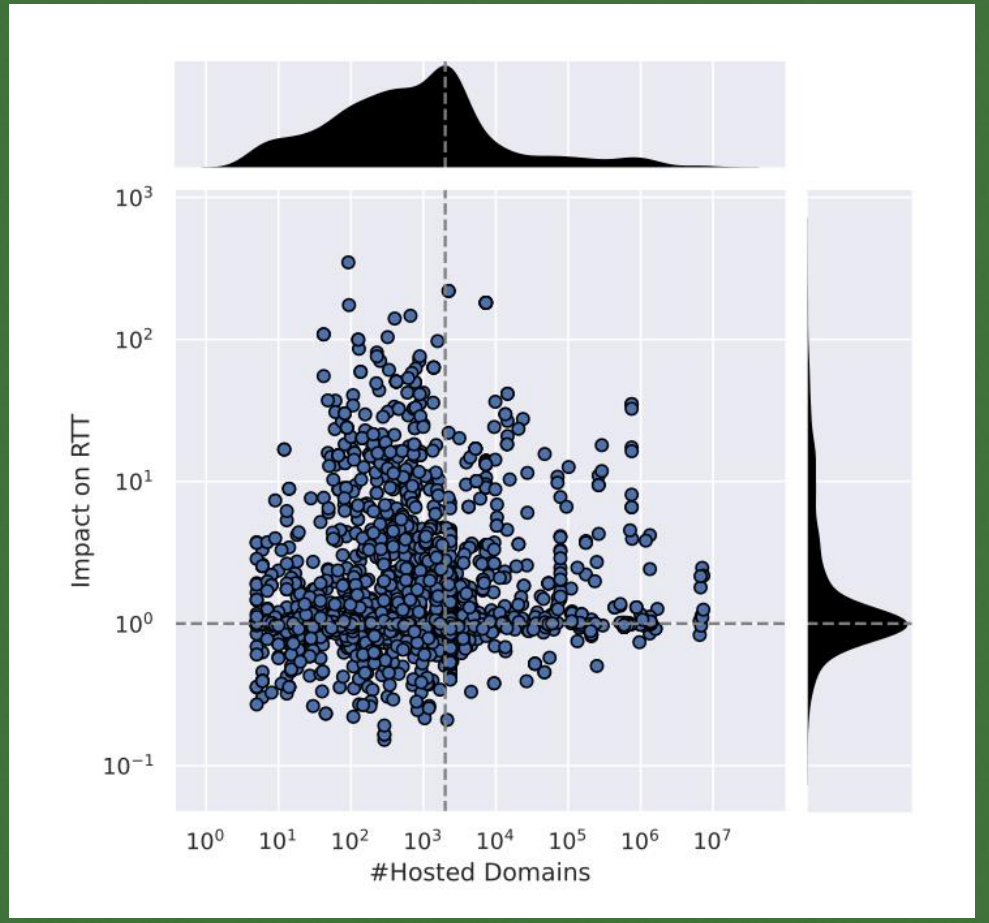
Failure in resolution

- Most domains failing to resolve belonged to small infrastructures.
- Largest attack (>10K domains) against nic.ru, a Russian registrar.
- 49% of successful attacks target port 53 (DNS).



Resolution performance impairments

- ≈ 5% of attacks (585) induced a 10-fold increase in RTT.
- In 198 cases, we see RTT peaking at more than **100-fold the baseline RTT.**
- High-impact attacks concentrated on **small-medium size infrastructure.**

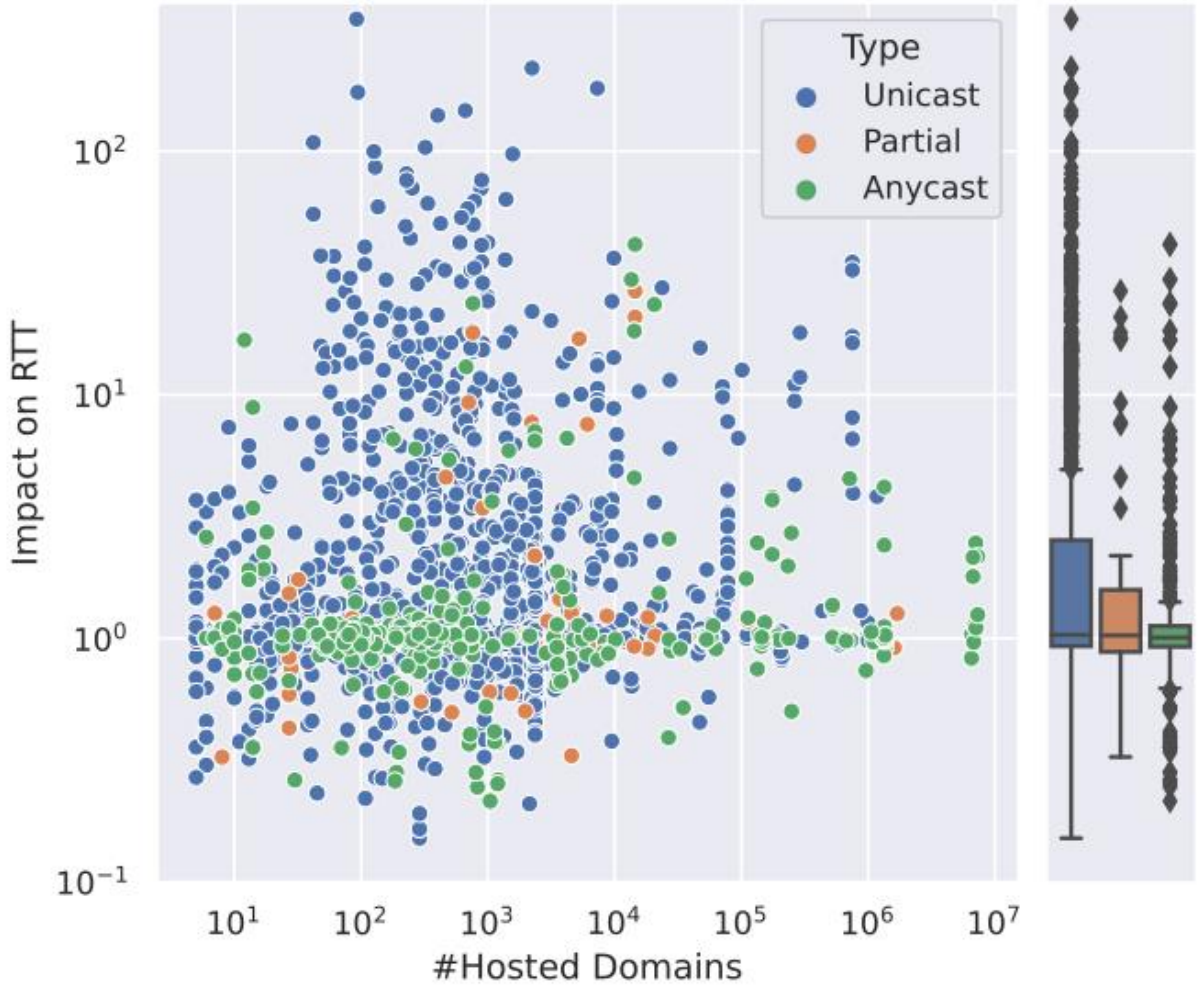


Attack Inferred Intensity/Duration Correlation

- No correlation between RSDoS impact and DNS impact
- Telescope data reveals signaling of ongoing attacks but does not enable prediction of performance impact.
- Impactful DNS attacks are short-lived (15-60 minutes).

Anycast efficacy vs DDOS

- Effective attacks => unicast.
- Resolution failure: domains relying on a unicast.
- Anycast as a resilience technique against DDoS attacks.

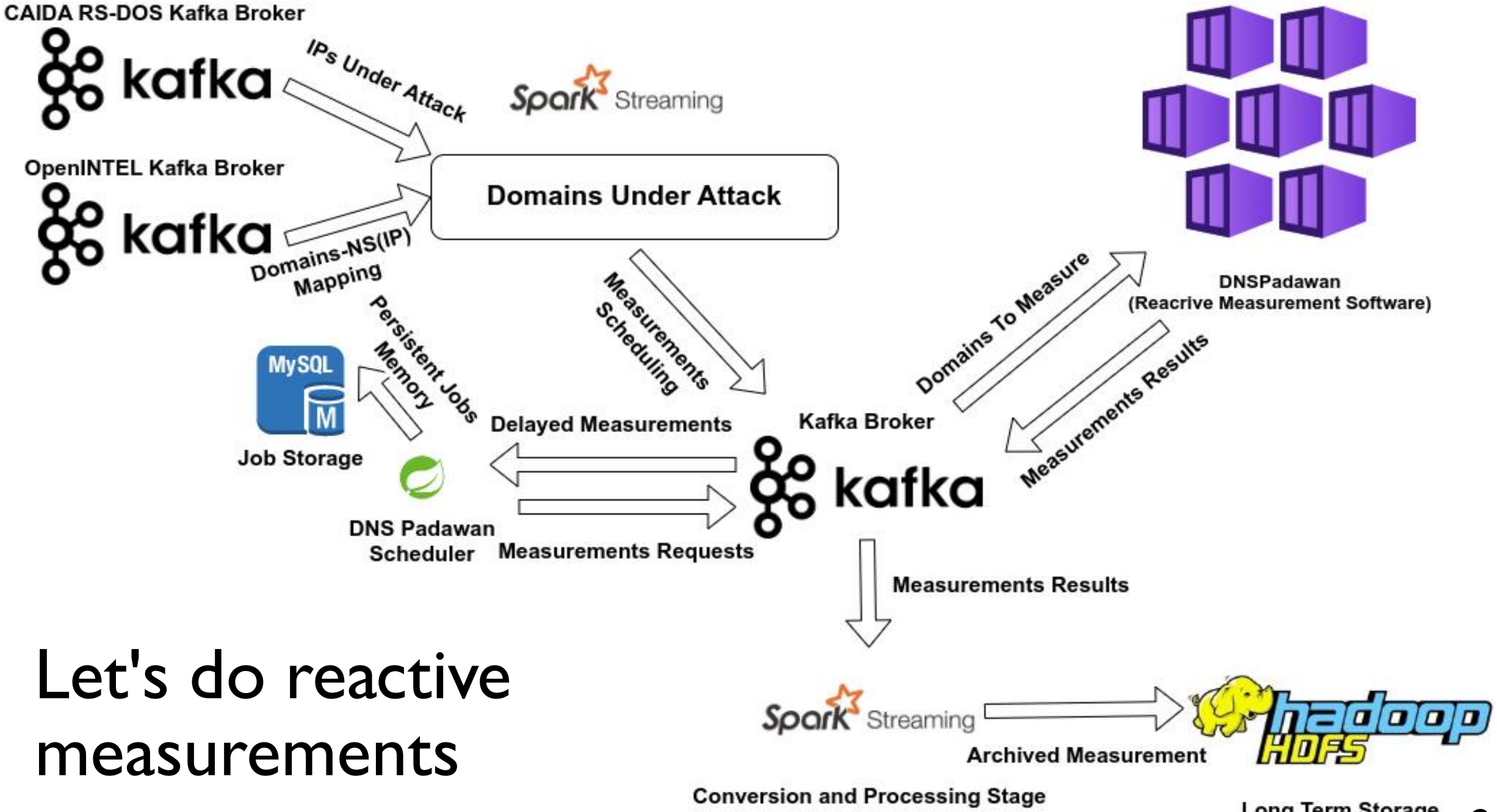


Network diversity vs DDoS

- 81% domain failing to resolve => single ASN Deployment.
- 60% domain failing to resolve => a single /24 prefix.
- *Anycast deployments suffer less from attacks, indicating increased DNS infrastructure resilience.*
- *Hosting nameservers across multiple prefixes or multiple ASNs increased resilience to devastating attacks.*

Future Directions

- Our inferences are incidental cases!
- Trigger active measurements of critical infrastructure under attack.
- Measuring all nameservers!
- From multiple vantage points!



Let's do reactive measurements

Conclusion

- Effectiveness of DNS resilience techniques.
- Well-provisioned DNS can withstand severe attacks.
- Small operators should rely on third-party as backup resilience.
- Continuous monitoring of the global DNS infrastructure needed.

Thanks for the attention

Contact me:
r.sommese@utwente.nl
https://academia.r4ffy.info

This work is based on research sponsored by NWODHS MADDVIPR project (628.001.031/FA8750-19-2-0004), the EU CONCORDIA project (830927) the U.S. NSF grants OAC-2131987 and OAC-1724853. The views and conclusions are those of the authors and do not necessarily represent endorsements, either expressed or implied, of the sponsors.

UNIVERSITY OF TWENTE.

Georgia Tech

Homeland Security

NWO
Netherlands Organisation for Scientific Research