# DNS Resilience and Centralization: A Data Oriented Analysis

Raffaele Sommese, Gautam Akiwate,
Mattijs Jonker, Geoff Voelker, Roland van Rijswijk,
Stefan Savage, Anna Sperotto, KC Claffy

University of Twente, Stanford University, UC San Diego, CAIDA

# Centralization or Resilience:
# A False Dilemma?

# centralization, n.

**1.** The action or process of bringing to or gathering at a centre; the fact of being centralized in this way; *esp*. the action or process of concentrating governmental or administrative power and control in a central place or authority, from which subsidiary agencies are controlled and to which they are responsible

–

Oxford Dictionary

# Many Ways to Define Centralization in DNS

- Infrastructure Centralization?
  - Increasing dependence on limited infrastructure
- Organizational Centralization?
  - Increasing dependence on limited organizations
- Namespace Centralization?
  - Increasing dependence on limited namespace
- Software Centralization?
  - Increasing dependence on limited software

# resilience, n.

**5.** The quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness, etc.; robustness; adaptability.

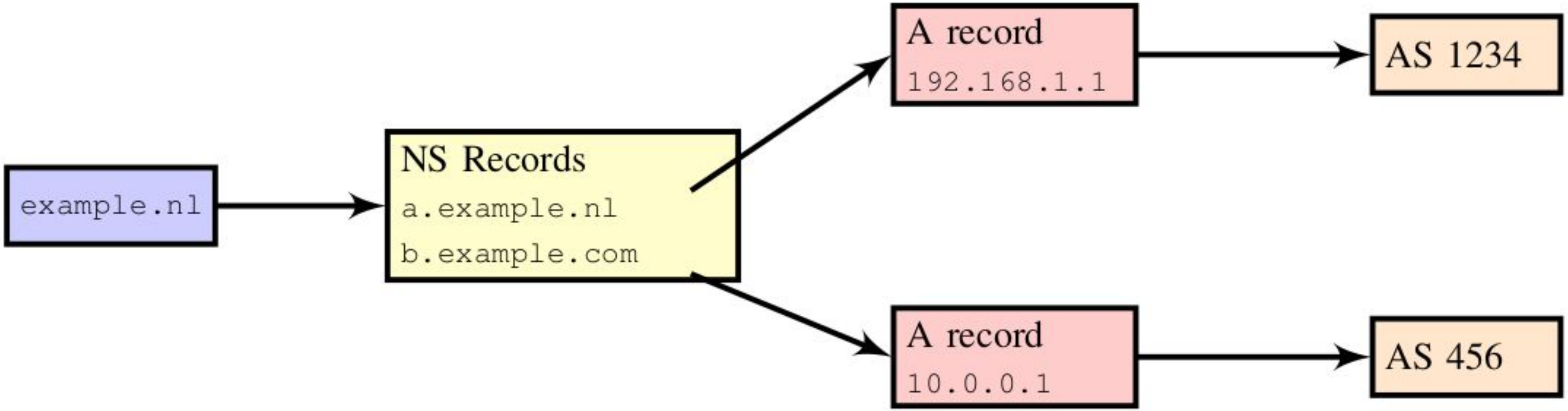
–

Oxford Dictionary

# Many Ways to Define Resilience in DNS…

- Infrastructure Resilience?
- Organizational Resilience?
- Namespace Resilience?
- Software Resilience?

# Traditional Model of Resilience – Infrastructure Resilience



# DNS Resilience and Centralization

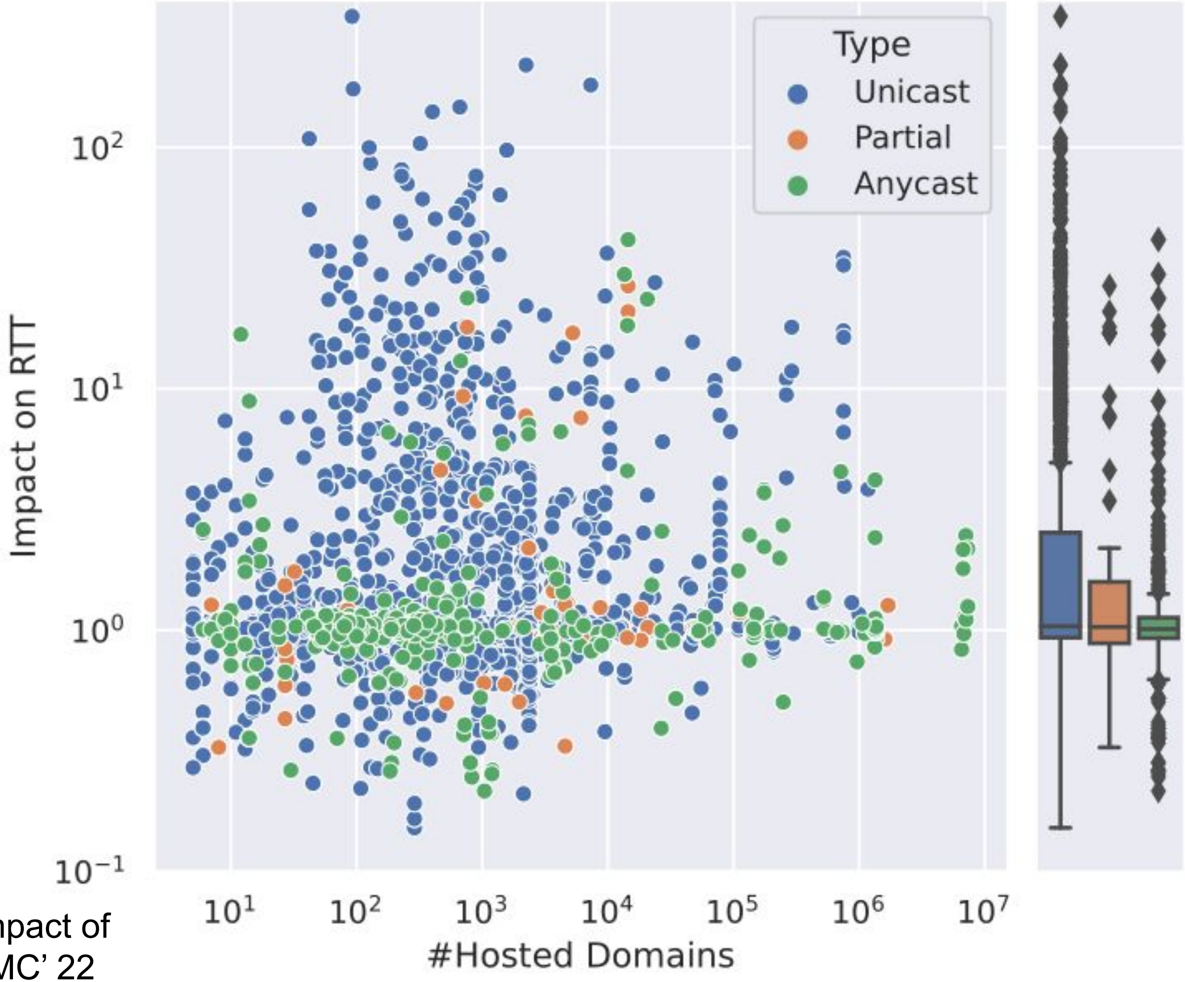
- DNS was built with “infrastructure resilience” in mind
  - Two nameservers + Two /24s
- How widely adopted are those mechanisms?
- Does reliance on same nameservers decrease resilience?
  - i.e., more centralization mean less infrastructure resilience?
- Ideally, yes…
  - But Anycast

# IP Anycast for DNS resilience

- Traditionally, Resilience relies on explicit nameservers replication and resolver failover (multiple NS records).
- Over time, another network-layer mechanism emerged: IP Anycast
- Anycast proved to be one of the key solutions to overcome DDoS Attacks

# Anycast vs DDoS

- Anycast adopting providers suffer less performance impairment compared to unicast ones.
- Smaller providers suffer more than larger ones.



R. Sommese et. al, Investigating the impact of DDoS attacks on DNS infrastructure, IMC' 22

# Anycast vs Disruptive DDoS

- Over one year and five months of attacks, the only ones causing complete failure in the resolution were related to unicast infrastructure.
- Network and Provider diversity has proven to be fundamental against large attacks aiming to complete operation disruption.

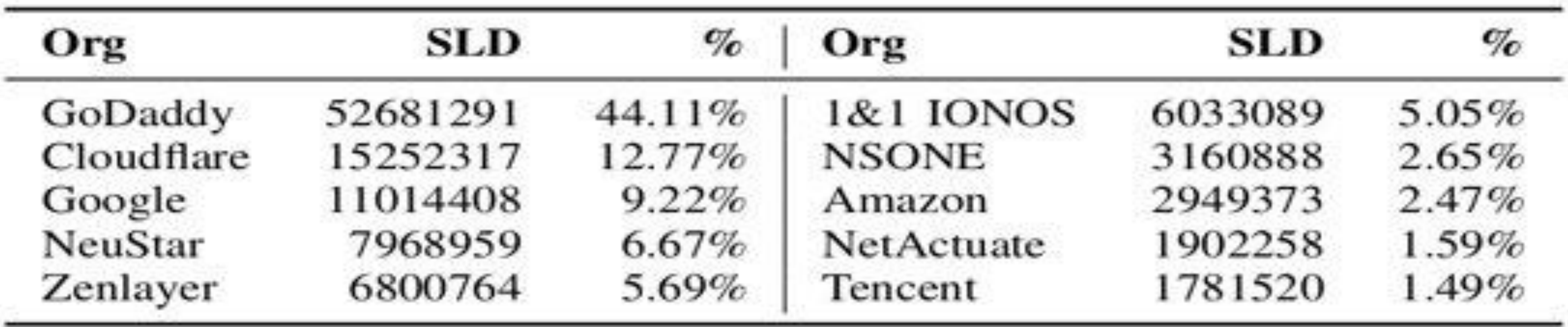
# Good (?) news on Anycast adoption

- 97% of the TLDs were using Anycast in 2021.
- PCH alone manages 25% of the ccTLDs authoritative infrastructure.
- Half of the DNS SLDs namespace relies on Anycast!
- But only 2.3% of the nameservers are Anycast!

R. Sommese et al., Characterization of Anycast Adoption in the DNS Authoritative Infrastructure, TMA' 21

# Bad (?) news Anycast implies concentration?

- Top 10 anycast organizations in 2017 and in 2021 are responsible for ~92% of domains adopting anycast.
- Top 10 unicast organizations count only for the 63%.
- GoDaddy alone accounted for half of domains adopting anycast, and a **quarter of the entire DNS namespace.**

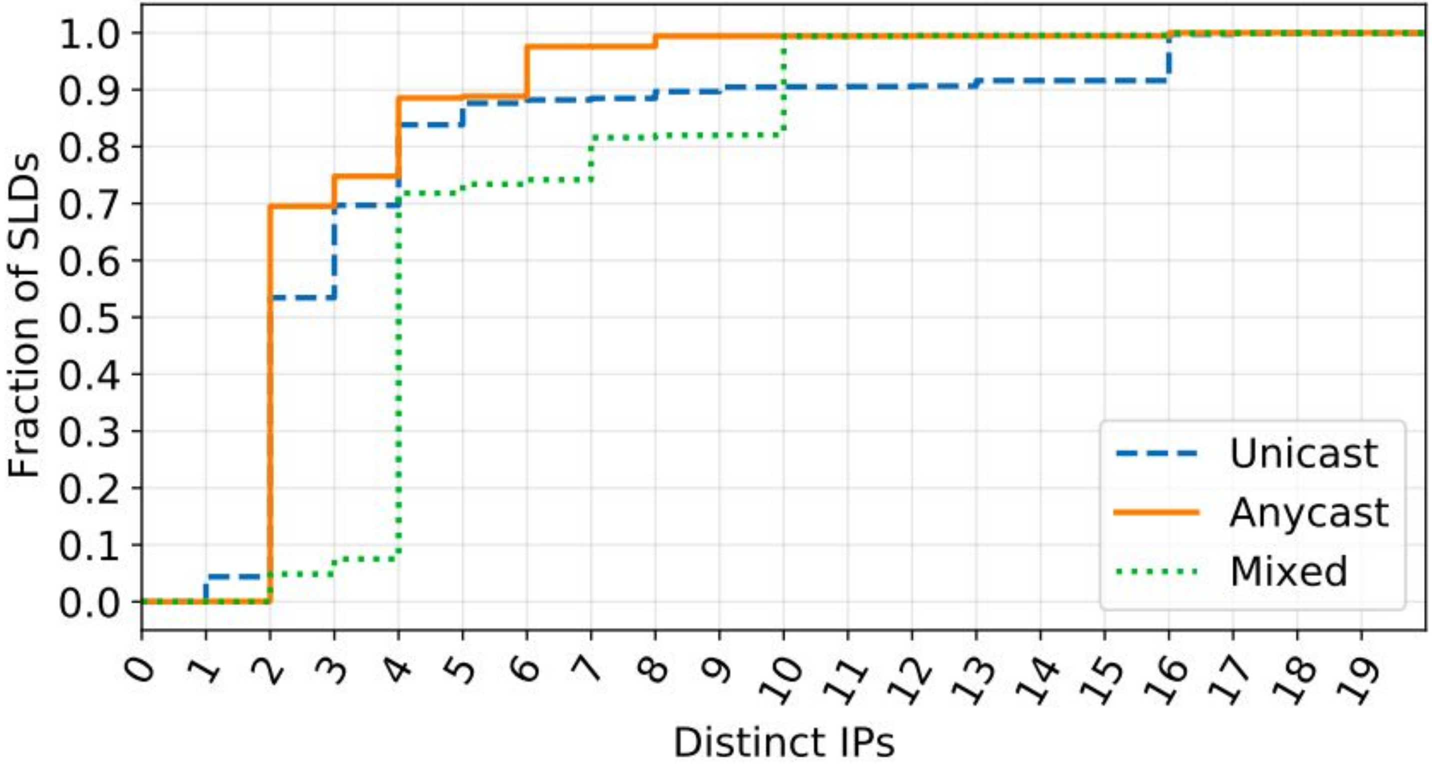


| Org | SLD | % | Org | SLD | % |
|---|---:|---:|---|---:|---:|
| GoDaddy | 52681291 | 44.11% | 1&1 IONOS | 6033089 | 5.05% |
| Cloudflare | 15252317 | 12.77% | NSONE | 3160888 | 2.65% |
| Google | 11014408 | 9.22% | Amazon | 2949373 | 2.47% |
| NeuStar | 7968959 | 6.67% | NetActuate | 1902258 | 1.59% |
| Zenlayer | 6800764 | 5.69% | Tencent | 1781520 | 1.49% |

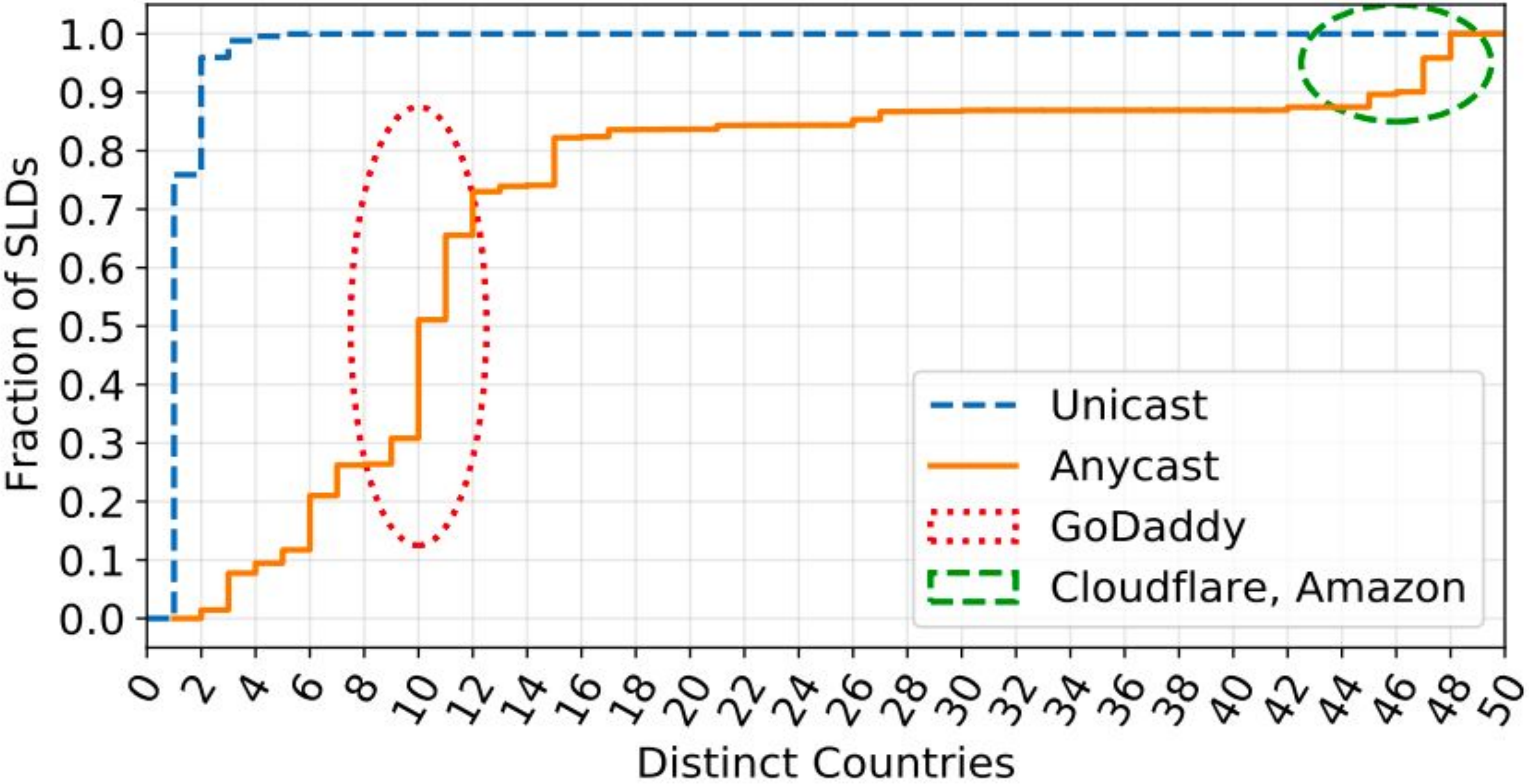
# Resilience: An operator driven choice (?)

- OVH, a popular European hosting provider, offers optional* anycast service for DNS nameservers for €1.21/year.
- Nearly all SLDs using OVH's authoritative infrastructure use unicast.
- We measured 4,156,201 domains using OVH's unicast infrastructure.
- Only 130,951 domains were using anycast.

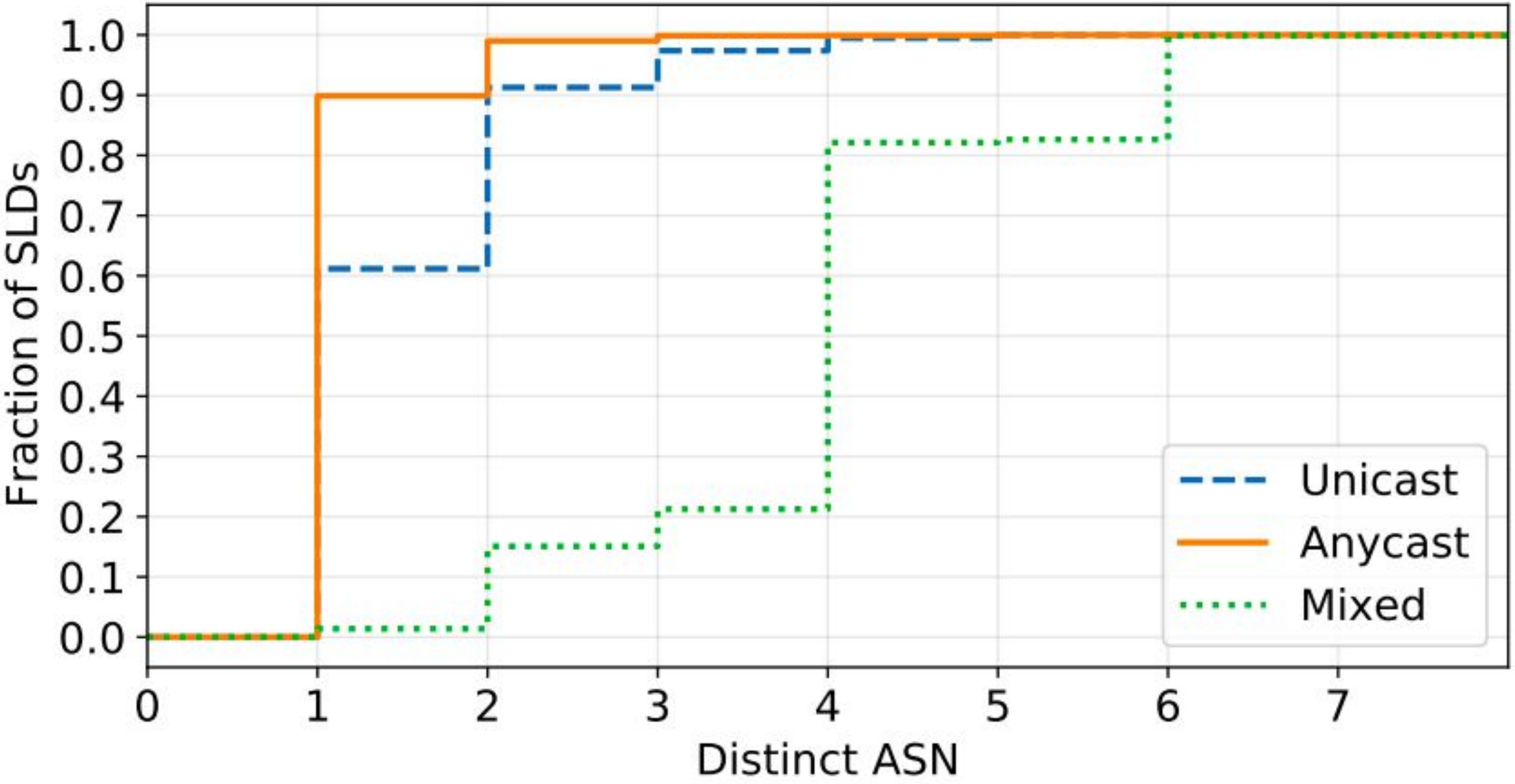
# Anycast vs Resilience: IP Diversity



# Anycast vs Resilience: Geo Diversity



# Anycast vs Resilience: Provider Diversity



# Anycast adoption increasing

Comparing 2021 to 2017, we found:

- An increase of 10% in Anycast adoption.
- A significant increase in number of anycast replicas.
- Mainly linked to large operators.

# Hosting Centralization

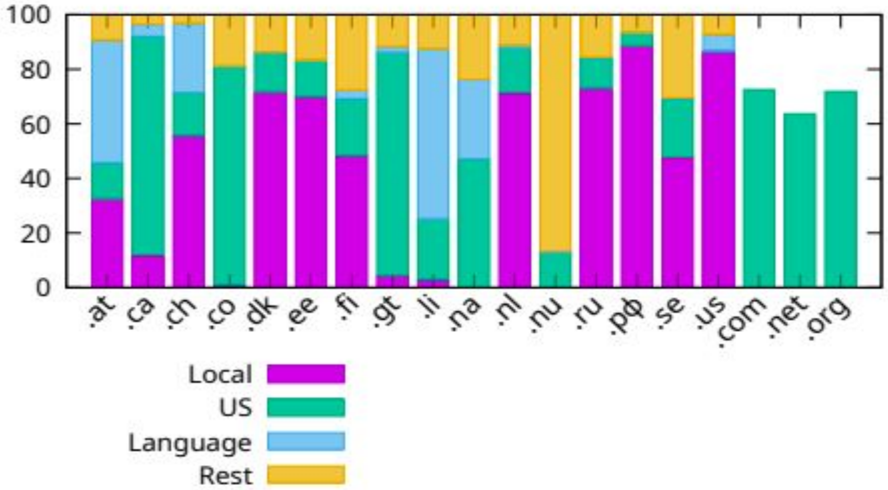
Web hosting is heavily concentrated too

- More than 1/3 of 150 million domains are hosted by five large US hosting providers.
- A policy change by CloudFlare shifted ~17 M domains to Google Cloud, turning Google into the largest provider in 2021, with 18% of all domains.
- Most ccTLDs concentrate at least 40% of domains in their top five hosting providers.

L. Zembruzki et al., Hosting Industry Centralization and Consolidation,  NOMS' 21

# Country Based Centralization

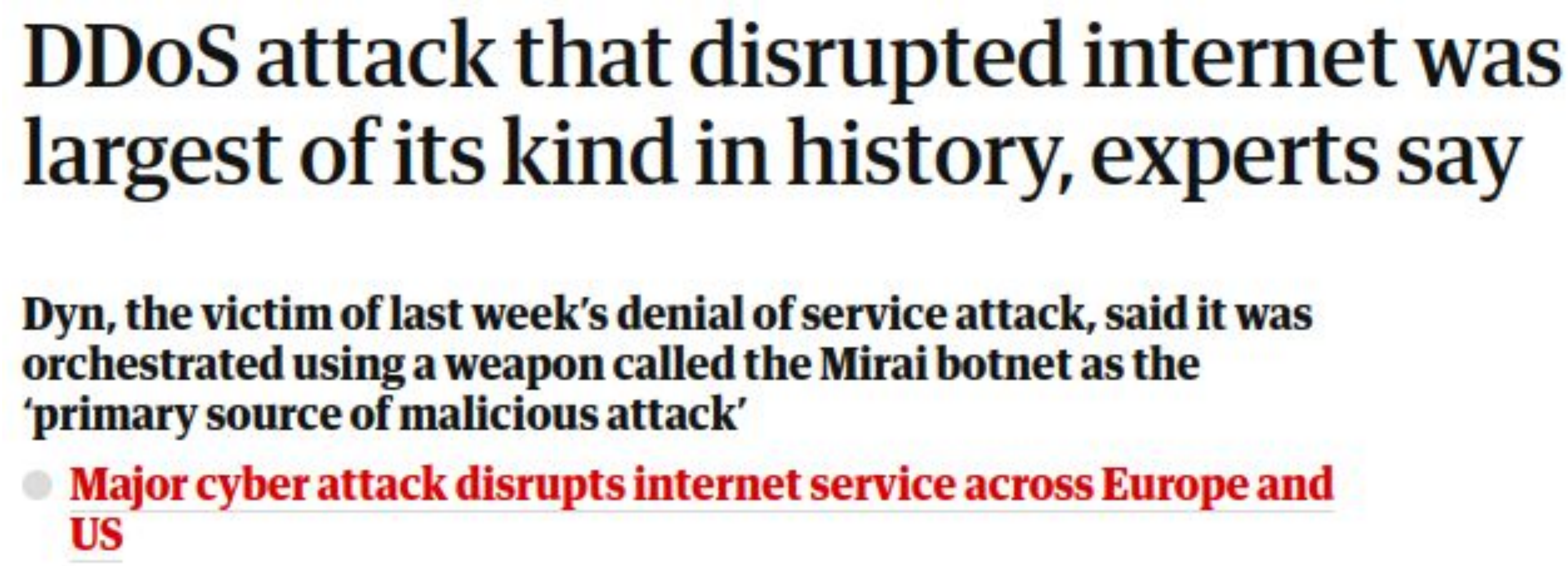
- Solid centralization of local hosting industry in most European countries and Russia.
- Hosting provider language plays a fundamental role..



# Centralization Risks: DDoS Attacks

- Dyn was responsible for many relevant services (Spotify, Twitter, etc..)
- TransIP was responsible for the 8% of the .nl domains.
- Nic.ru responsible for more than 10K .ru domains.

# Dyn Attack



## DDoS attack that disrupted internet was largest of its kind in history, experts say

**Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'**

- **Major cyber attack disrupts internet service across Europe and US**

# TransIP Attack

- Under attack on December 2020 and March 2021.
- Performance impairments of more than 10-fold increase of standard RTT.
- Failure in resolution of 20% of the observed domains.

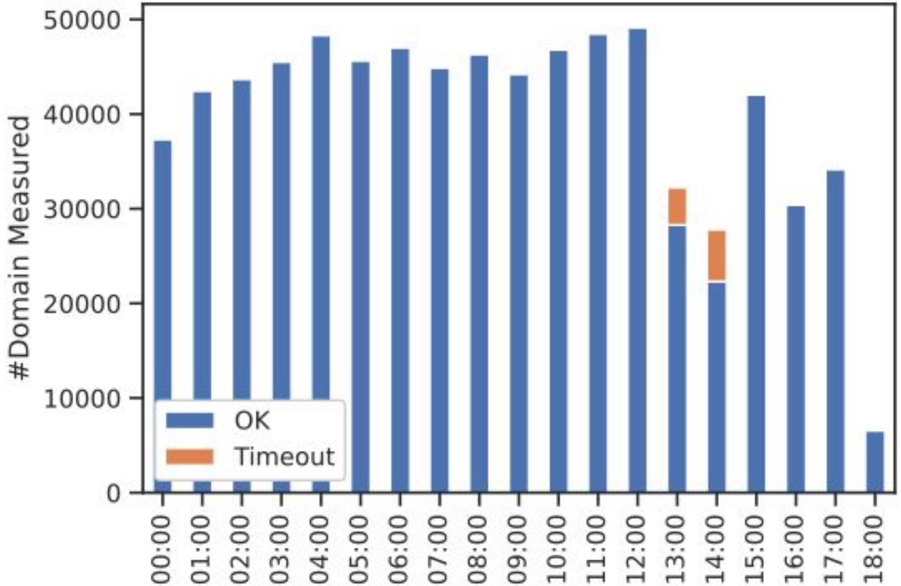


**Figure 3: Timeout errors during the March 2021 attack on TransIP reached 20% of observed domains, leading to resolution failures for end users**

# Nic.ru Attack

- Part of the March 2022 attacks against russian infrastructures.
- Failed resolution for 100% of domains hosted.
- Causing failure for more than 10 thousands domains.

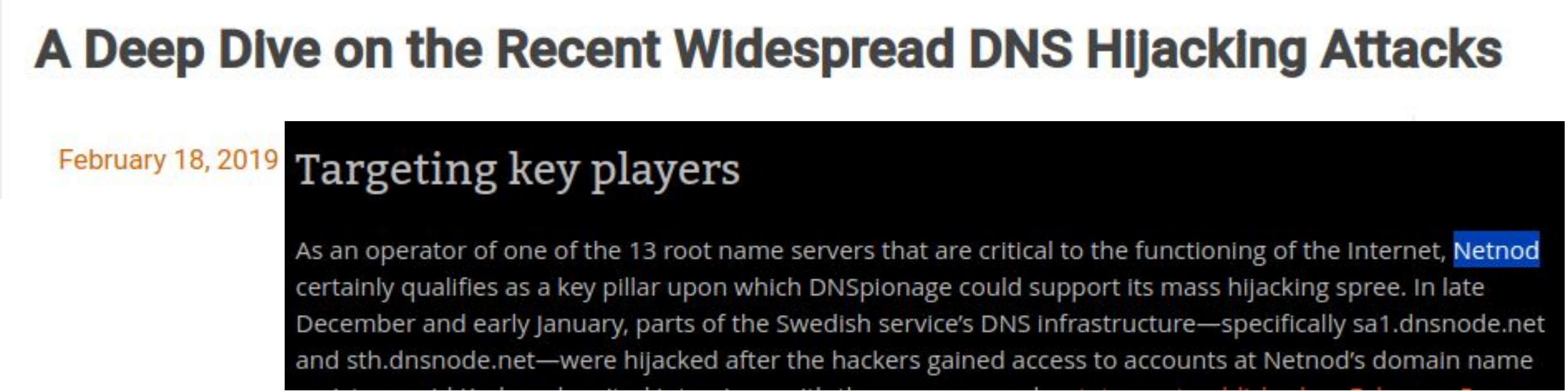
# DDoS Attacks: The “too big to fail”?

- The previous cases show that even providers “too big to fail” can actually suffer catastrophic consequences from attacks.
- Large providers can deploy more effective resilience and mitigation strategies to overcome DDoS attacks.
- But attacks are not the only issue!

# Centralization Risks: Configuration Mistakes

- Loopia AB serves ~500K domains (mostly in .se) via anycast from a single /24 block.
- Loopia relies as its only resilience mechanism uniquely on anycast.
- Consequences of mistakes in BGP announcements can be catastrophic.

# Centralization Risks: Hijacks

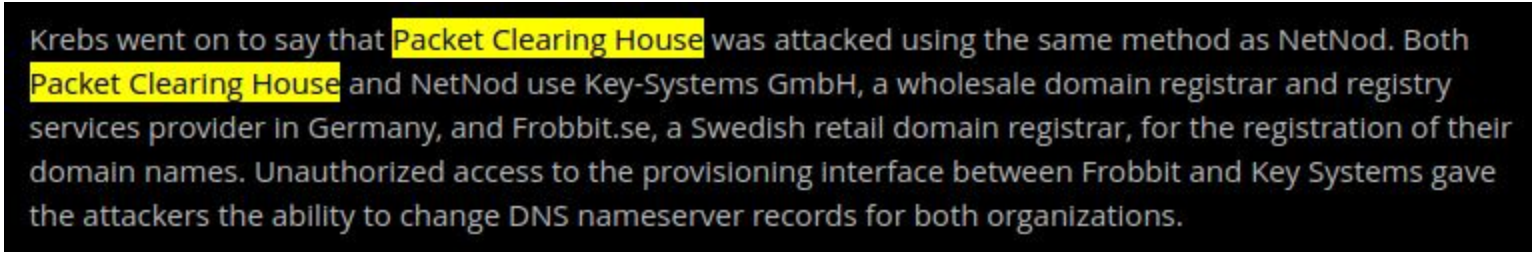


## A Deep Dive on the Recent Widespread DNS Hijacking Attacks

February 18, 2019

### Targeting key players

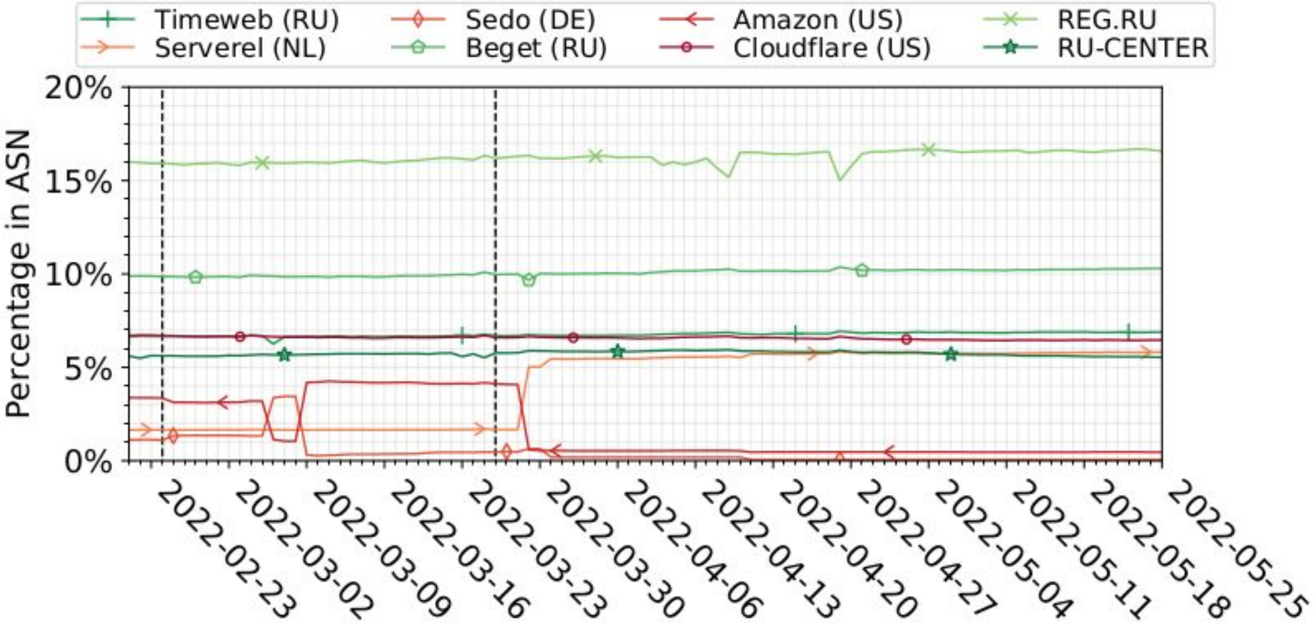
As an operator of one of the 13 root name servers that are critical to the functioning of the Internet, Netnod certainly qualifies as a key pillar upon which DNSpionage could support its mass hijacking spree. In late December and early January, parts of the Swedish service's DNS infrastructure—specifically sa1.dnsnode.net and sth.dnsnode.net—were hijacked after the hackers gained access to accounts at Netnod's domain name



Krebs went on to say that Packet Clearing House was attacked using the same method as NetNod. Both Packet Clearing House and NetNod use Key-Systems GmbH, a wholesale domain registrar and registry services provider in Germany, and Frobbit.se, a Swedish retail domain registrar, for the registration of their domain names. Unauthorized access to the provisioning interface between Frobbit and Key Systems gave the attackers the ability to change DNS nameserver records for both organizations.

# Centralization Risks: Sovereignty vs Sanctions

- Exodus of service providers from Russia.



# Centralization Risks: Government Compellence

- Centralization means fewer organizations for governments to compel.
- Hostile governments can disrupt services of foreign countries.
- Data and Infrastructure at risk.

# Resilience without Centralization

- Economics aspect of resilience pushes customers towards centralizations.
- Using different providers.
- Challenging configuration.
- E.g., RIPE NCC secondary nameserver service

# Conclusion

- DNS is heavily concentrated.
- Small providers suffer more from DDoS attacks.
- Centralization has side risks.
- How to achieve a balance between less centralization and more resilience?

# Questions?

Reach us:

r.sommese@utwente.nl

gakiwate@cs.stanford.edu