On Borrowed Time: Measurement-Informed Understanding of the NTP Pool's Robustness to Monopoly Attacks

NDSS 2026
February 26, 2026

Rob Beverly <rbeverly@sdsu.edu>
Erik Rye <rye@jhu.edu>

SDSU | San Diego State University

Johns Hopkins University

Our Contributions:

- First complete and exhaustive characterization of the NTP Pool (servers, accounts, zones, scores, traffic)
- Analysis of the NTP Pool's server composition, finding only ~20% are truly independent
- Enhance Perry, et al., NDSS 2021 by precisely computing required resources to "monopolize" each NTP zone
- Show that the informed attacker can capture preponderance of NTP traffic in 90% of all countries with < 10 attack servers

Background

Network Time Protocol (NTP)

- Distributed time consensus over packet switched network
  - One of the oldest core Internet protocols (RFC 958, 1985)
  - NTP servers participate in a hierarchy
  - End-hosts (computers, phones, IoT) synchronize with set of NTP servers
- Correct time critical for applications and security:
  - TLS certificates, DNS, BGP, blockchain, etc.

Prior Attacks on NTP

- DDoS:
  - UDP with spoofed source reflection + amplification
- Time shifting:
  - Malhotra, et al., NDSS 2016; Deutsch, et al., NDSS 2018
- Adding malicious servers to the NTP Pool:
  - Perry, et al., NDSS 2021; Kwon, et al., USENIX 2023

So, how do devices get time?

- Microsoft, Apple, Google, Facebook, etc:
  - run their *own* NTP infrastructure
- What about Linux and open-source Operating Systems?
  - The “NTP Pool”

NTP Pool

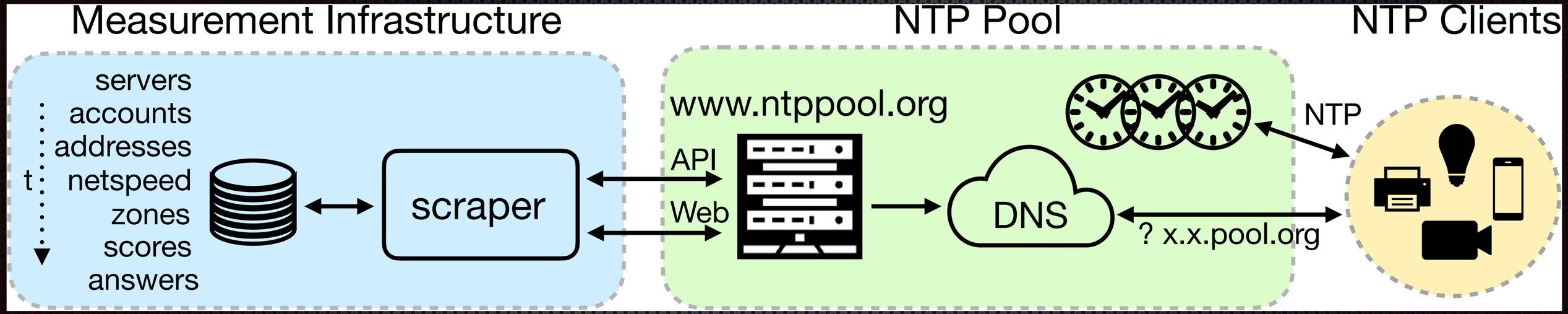
- Crowd-sourced NTP:
  - Administratively distributed, volunteer based
  - Anyone can signup and add their server
  - A monitoring system checks quality of time
  - “Good” servers are included in the pool
- 29 geographic zones (countries): .us, .de, .jp, etc.
- Clients directed to NTP pool servers within their geographic service region via the DNS

Does the NTP pool matter?

- IoT devices use embedded Linux; implies large-scale use of NTP pool
- Critical infrastructure!
  - At a DNS root, NTP pool receives most (90 / 126M) of all NTP lookup queries (Moura et al)
  - At IPv6 observatory, 5.5M fritz!box routers, 1.6M amazon devices, 289k Sonos speakers sent IPv6 NTP queries within one week
  - This work finds global DNS query rate to the pool of > 400k queries / sec

Methodology

Methodology



- Prior work: issue (many, many) DNS queries (from many locations) to identify active NTP pool servers
- Instead, we develop a method to query ntppool.org to exhaustively and completely to enumerate: servers, accounts, netspeeds, scores, answers, etc. (both active and inactive)

Scraping methodology

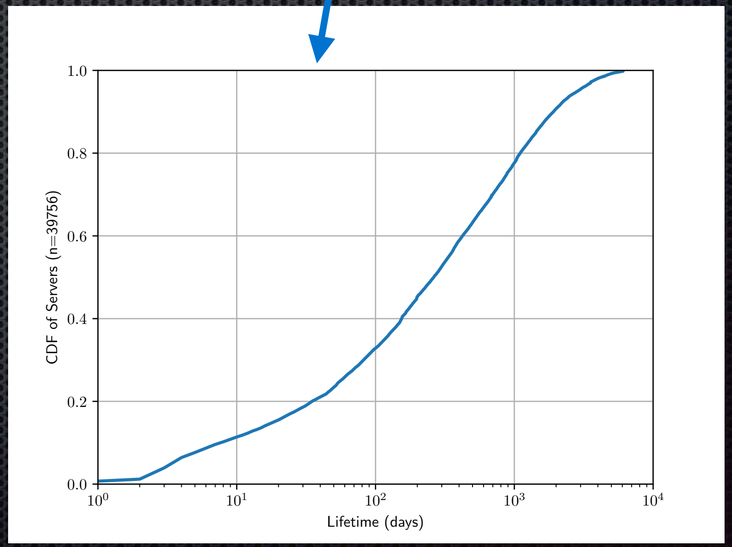
Endpoint	Parameters	Response Type	Returns
`/scores/{%d}`	Server ID	HTTP 301	Redirect to `/scores/{ip}`
`/scores/{%s}`	Server IP	HTML	Server Info
`/scores/{%s}/json`	Server IP	JSON	Server Scores
`/api/data/server/dns/answers/{%s}`	Server IP	JSON	Per-zone DNS answers
`/api/data/zone/counts/{%s}`	Zone	JSON	Per-zone Servers and “netspeed”

- Key observation: Pool assigns each server an ID from a monotonically increasing counter, starting from 1.
- Every 3 hours, try to fetch next ID
- Enumerate all servers (>15k), including those registered, but not included in pool responses

What the data can show us

Endpoint	Parameters	Response Type	Returns
`/scores/{%d}`	Server ID	HTTP 301	Redirect to `/scores/{ip}`
`/scores/{%s}`	Server IP	HTML	Server Info
`/scores/{%s}/json`	Server IP	JSON	Server Scores
`/api/data/server/dns/answers/{%s}`	Server IP	JSON	Per-zone DNS answers
`/api/data/zone/counts/{%s}`	Zone	JSON	Per-zone Servers and "netspeed"

	IPv4	IPv6
Servers (IPs)	9,955	5,725
Autonomous Systems	2,107	841
Zones	29	29
Active Servers	3,967	2,275
Servers w/ Accts	4,277	2,948
Stratum 1 Servers	548	282
Monitor-Only Servers	1,672	1,007
Anycast Servers	7	5



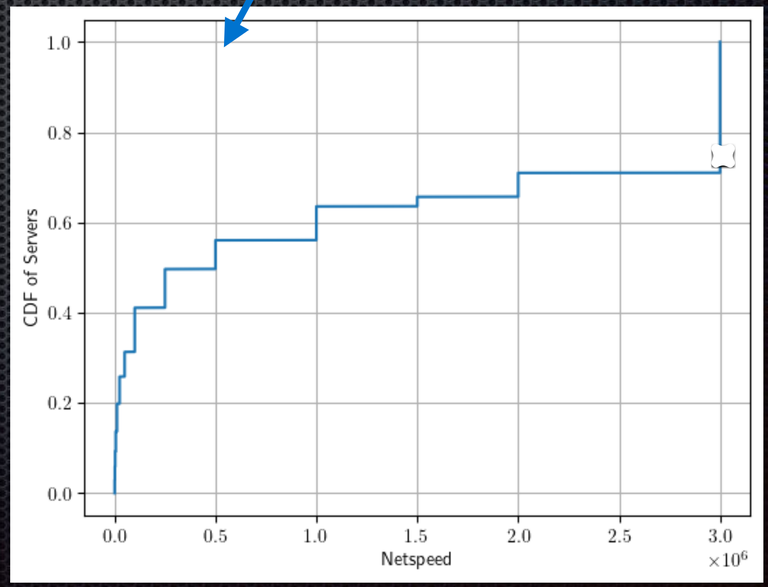
>10% servers alive for 10 or fewer days

What the data can show us

Endpoint	Parameters	Response Type	Returns
`/scores/{%d}`	Server ID	HTTP 301	Redirect to `/scores/{ip}`
`/scores/{%s}`	Server IP	HTML	Server Info
`/scores/{%s}/json`	Server IP	JSON	Server Scores
`/api/data/server/dns/answers/{%s}`	Server IP	JSON	Per-zone DNS answers
`/api/data/zone/counts/{%s}`	Zone	JSON	Per-zone Servers and "netspeed"

	IPv4		IPv6	
Zone	Servers	Rate (DNS/sec)	Servers	Rate (DNS/sec)
@	3211	194,653	1941	17,201
us	677	54,924	428	4,804
br	29	15,608	20	1,454
de	562	8,599	496	914
cn	34	8,238	43	768
uk	216	7,235	122	611
ru	404	6,917	77	509
in	45	6,244	29	658
fr	219	5,122	138	487
ca	119	4,473	71	402
Total	3867	389,257	2228	34,399

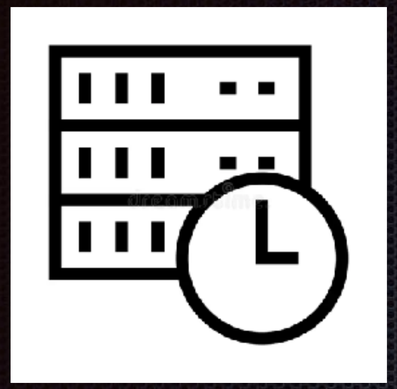
Global query rate ~100k DNS / sec



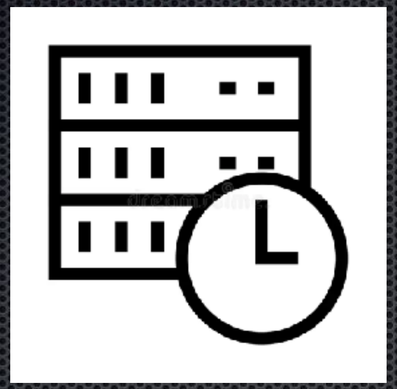
Only 25% of servers have max net speed

How Resilient is the Pool?

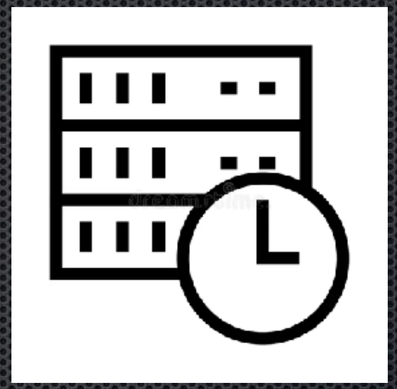
How Resilient is the NTP Pool?



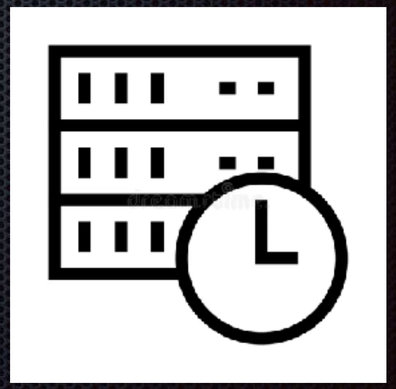
1.1.1.1



1.1.1.2

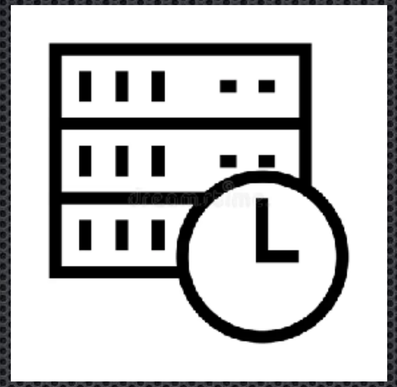


1.1.1.3



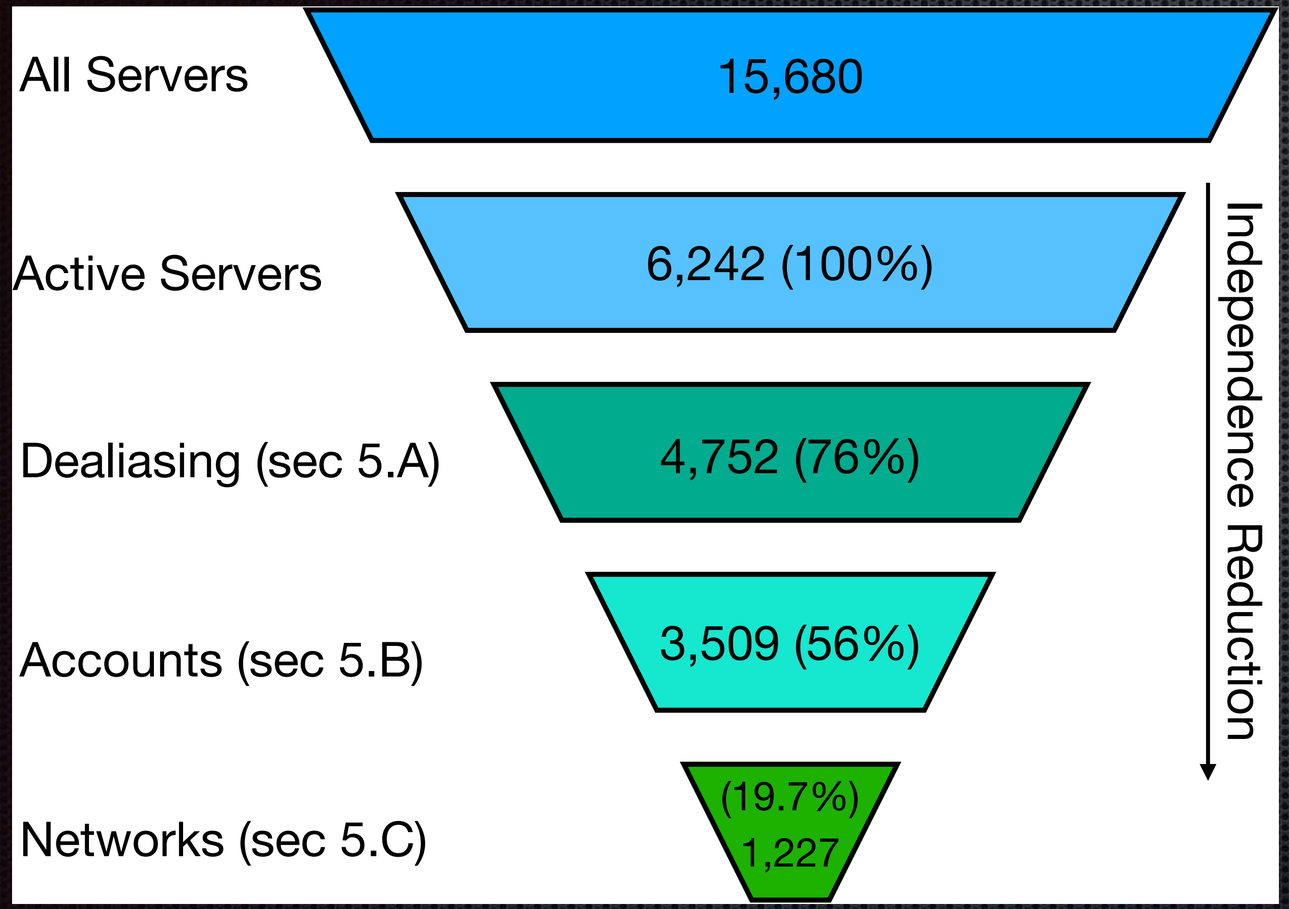
1.1.1.4

How resilient is the NTP Pool?

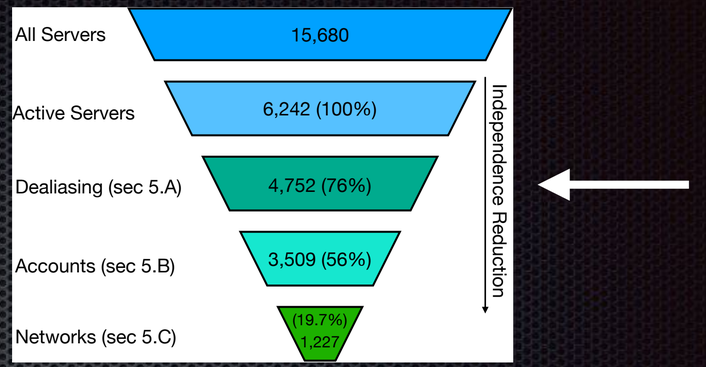


1.1.1.1
1.1.1.2
1.1.1.3
1.1.1.4

How diverse is the pool?

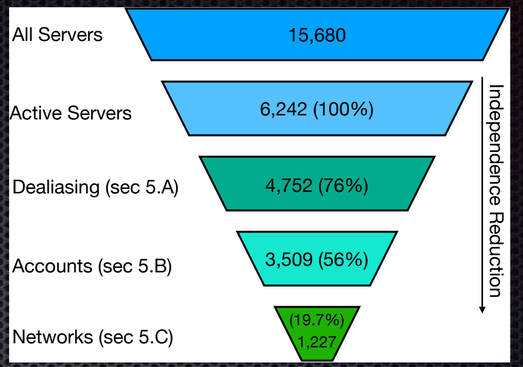


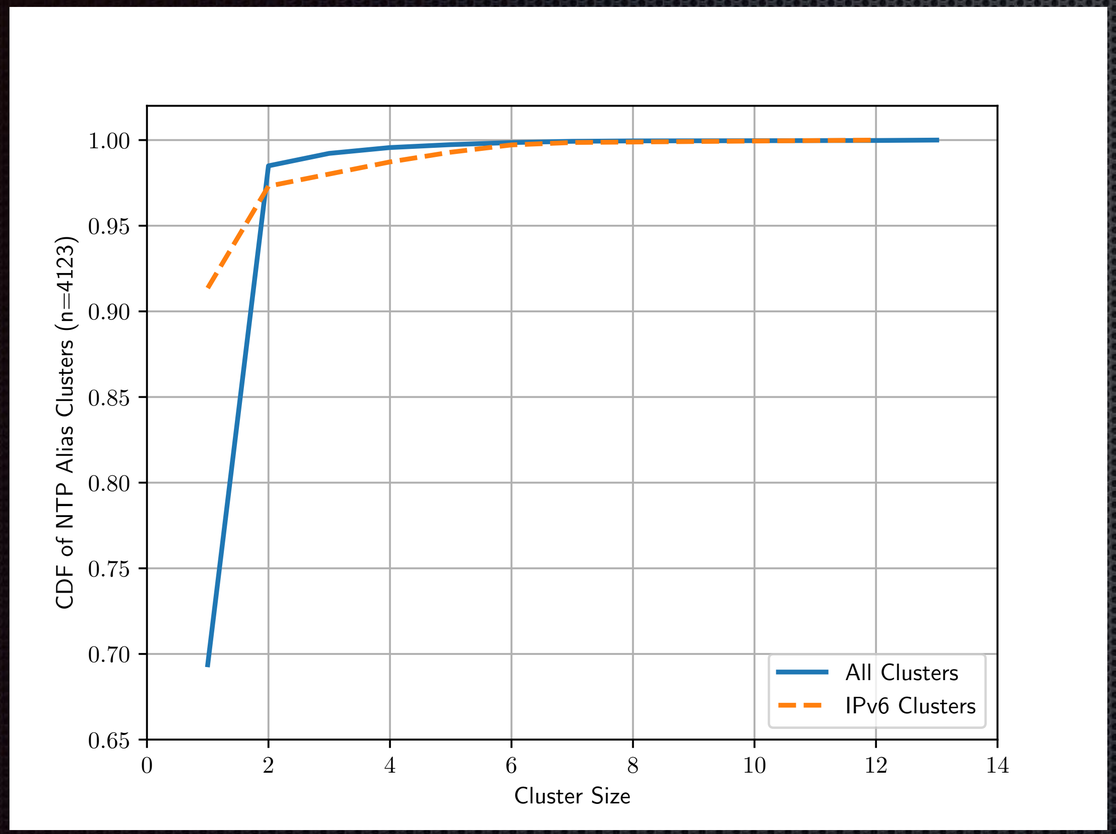
NTP Pool Server aliases



- Volunteers register NTP servers based on their IP address
- A “server” in the NTP pool is an IP address providing NTP service
- Thus, the same machine with IPv4 and IPv6 addresses are two “servers”
- Implemented an NTP server fingerprinter to find aliases:
  - Stratum, version, refID, precision, poll, etc

NTP Pool Server aliases

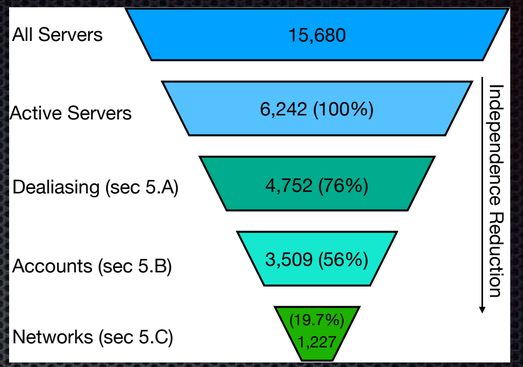


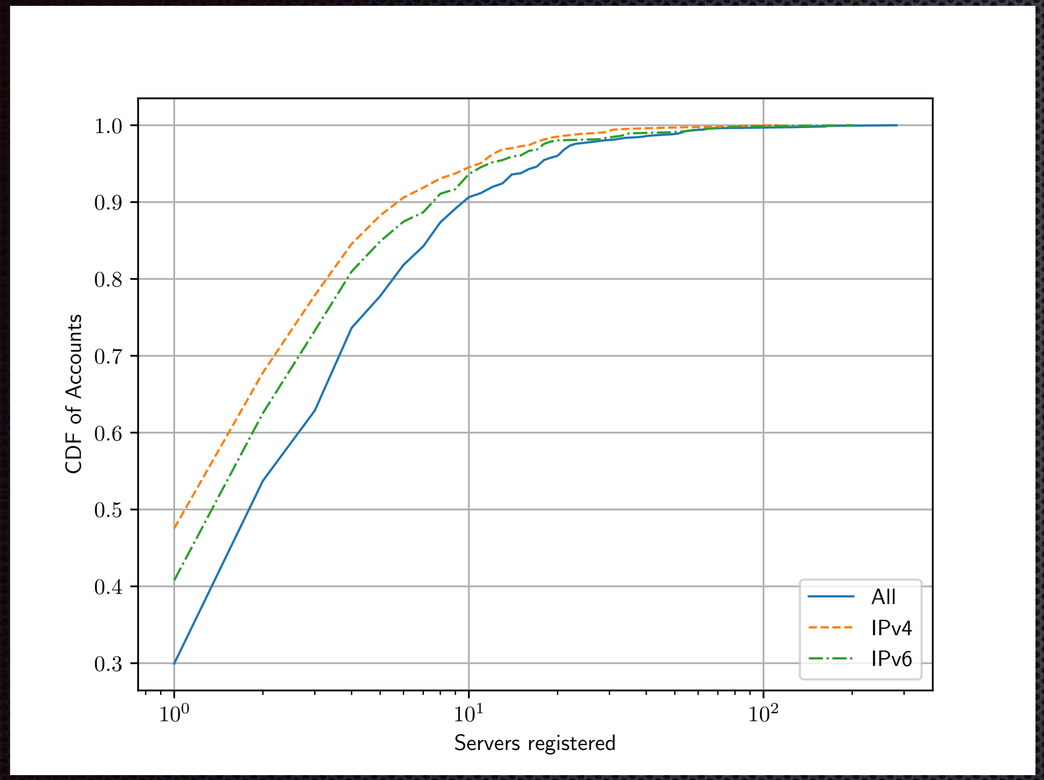


- 69% of addresses belong to singleton cluster
- Lots of IPv4/IPv6 pair clusters
- Large IPv6 clusters:

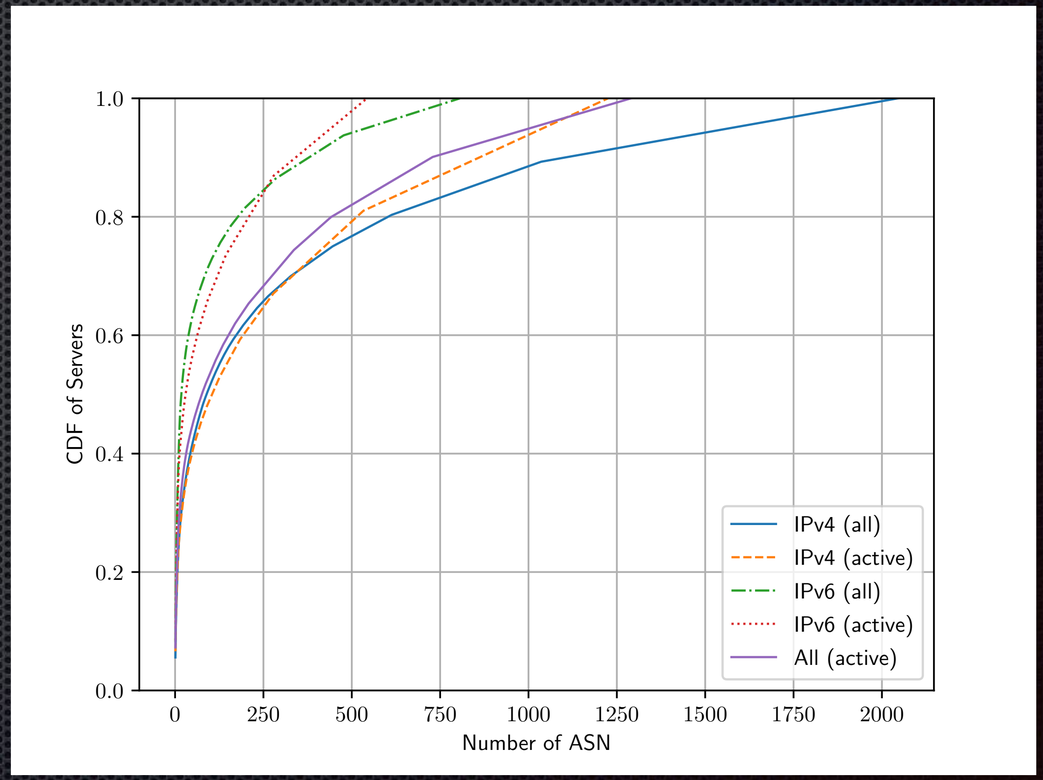
```
['2a00:6d41:200:2::11',
'2a00:6d41:200:2::12',
'2a00:6d41:200:2::13',
'2a00:6d41:200:2::14',
'2a00:6d41:200:2::15']
        Addresses in cluster: 5 Covering
prefix: 2a00:6d41:200:2::10/125
```

Pool Server Fate Sharing





Some accounts control many servers



Servers concentrated in small number of ASNs

Monopolization Attack

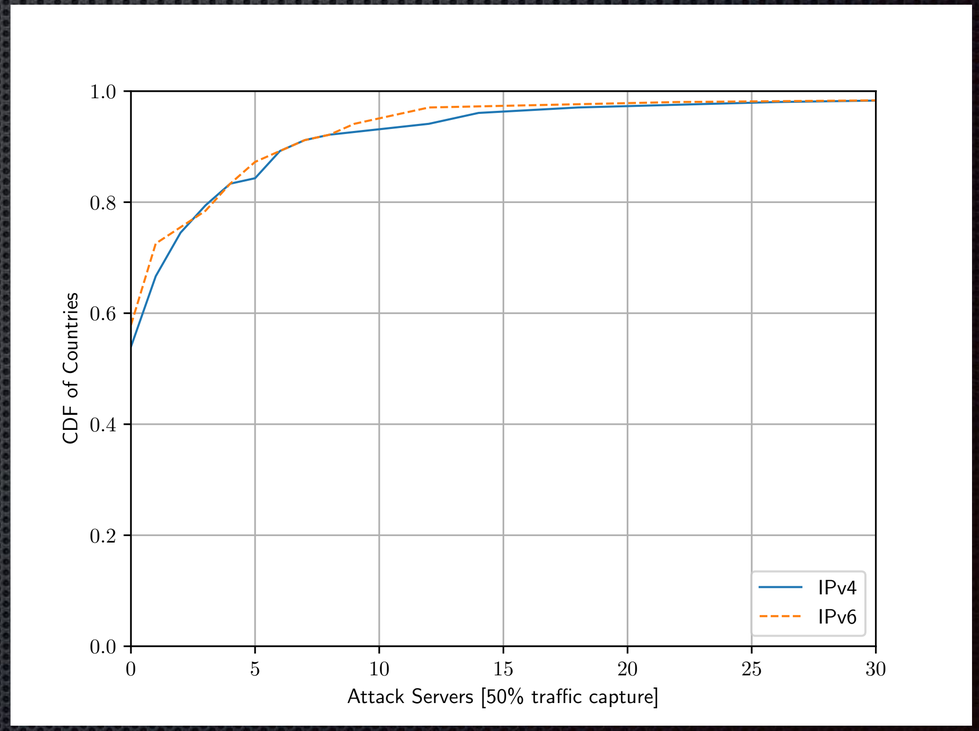
Pool Monopolization Attack

- Capture a preponderance of NTP pool traffic in a country
- Each server has a user-specified “netrate”, 512kbps -> 3Gbps
- Each zone has an aggregate netrate that is the sum of all servers
- DNS responses include a given server in proportion to its netrate / aggregate rate
- E.g.,:

```
US [v4]: servers: 625 agg netspeed: 299076068 single server attack: 0.99% to get .5: 50
US [v6]: servers: 375 agg netspeed: 395249992 single server attack: 0.75% to get .5: 66
HU [v4]: servers: 25 agg netspeed: 9447256 single server attack: 24.10% to get .5: 2
HU [v6]: servers: 8 agg netspeed: 8121000 single server attack: 26.98% to get .5: 2
```

Pool Monopolization Attack

- Capture a preponderance of NTP pool traffic in a country
- Q: assuming an adversary can add N servers to a zone with maximum netrate of 3Gbps, what N is required to capture half of the NTP traffic for each country?



90% of countries require
10 or fewer attacking servers

Implementing the Monopoly Attack

- August 5, 2025:
  - Target .hu domain
  - six active IPv6 servers in .hu
  - Examine “zone” and “answers” API endpoint (how often each server was included in DNS responses from pool)
  - Ethics: our “attack” servers return good/valid time
- Baseline: 4.101Gbps aggregate
- Added two .hu attack servers, each at 3Gbps
- These two were used for 46.8% of all .hu DNS responses; ~61k DNS/hour

Disclosure

- Shared results with NTP Pool developers:
  - Suggestions for protecting privacy of pool and users
  - Suggestions for improving DNS responses

Thanks!

- Questions?