Harness Your Internet Activity

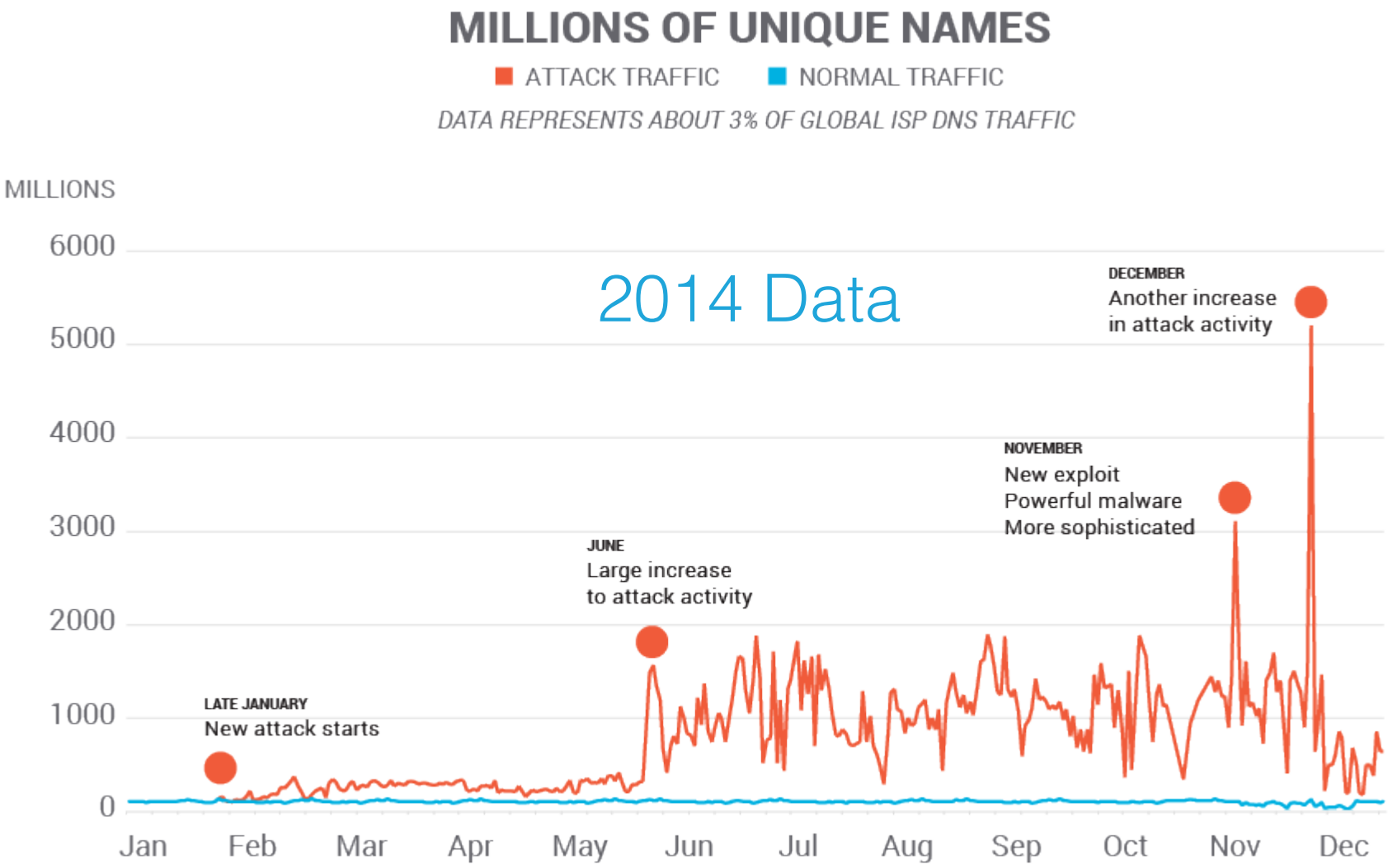
DNS-Based DDoS
Evolving Threat

RIPE May 2015
Amsterdam

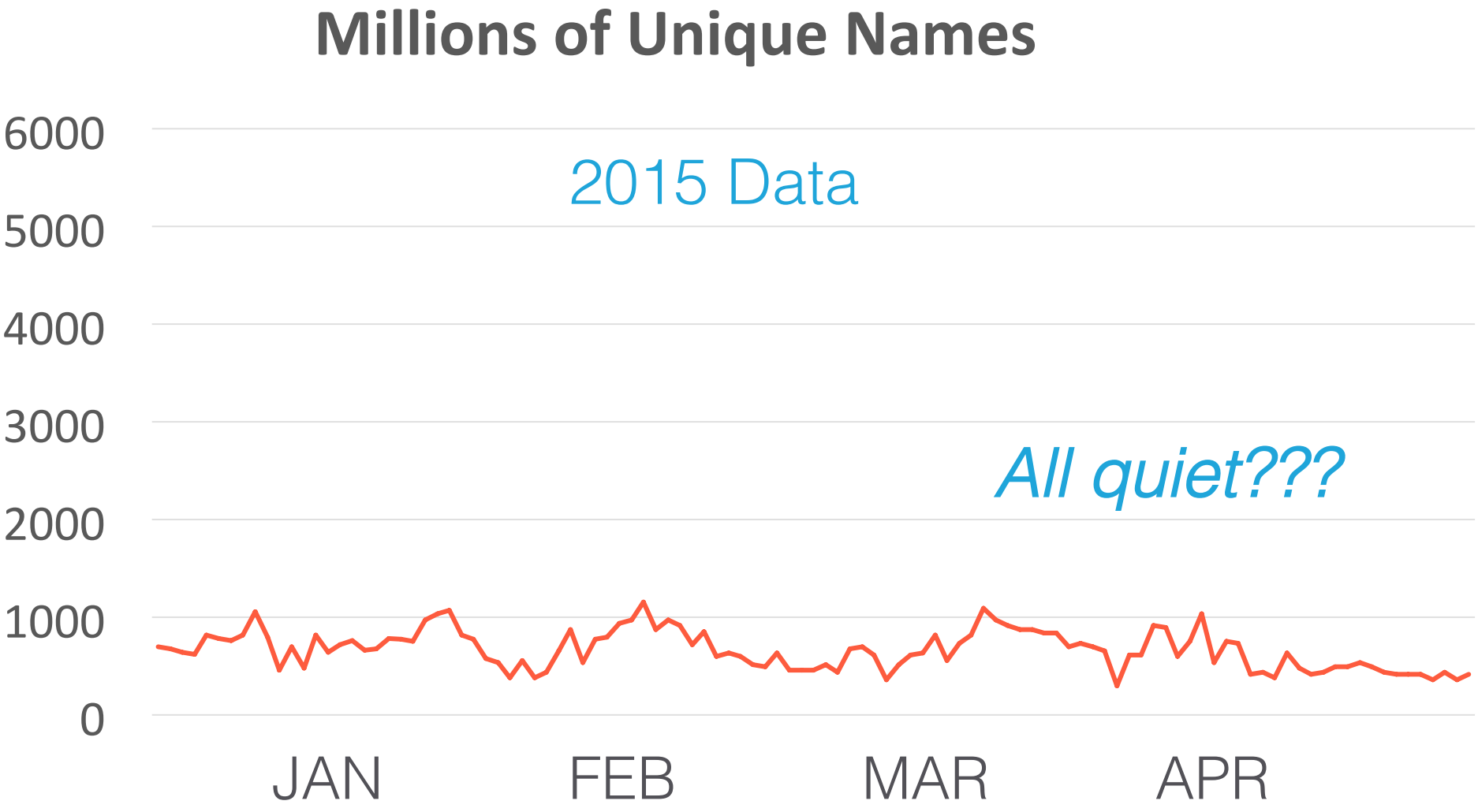
Ralf Weber

Bruce Van Nice

2014 Random Subdomain Attacks



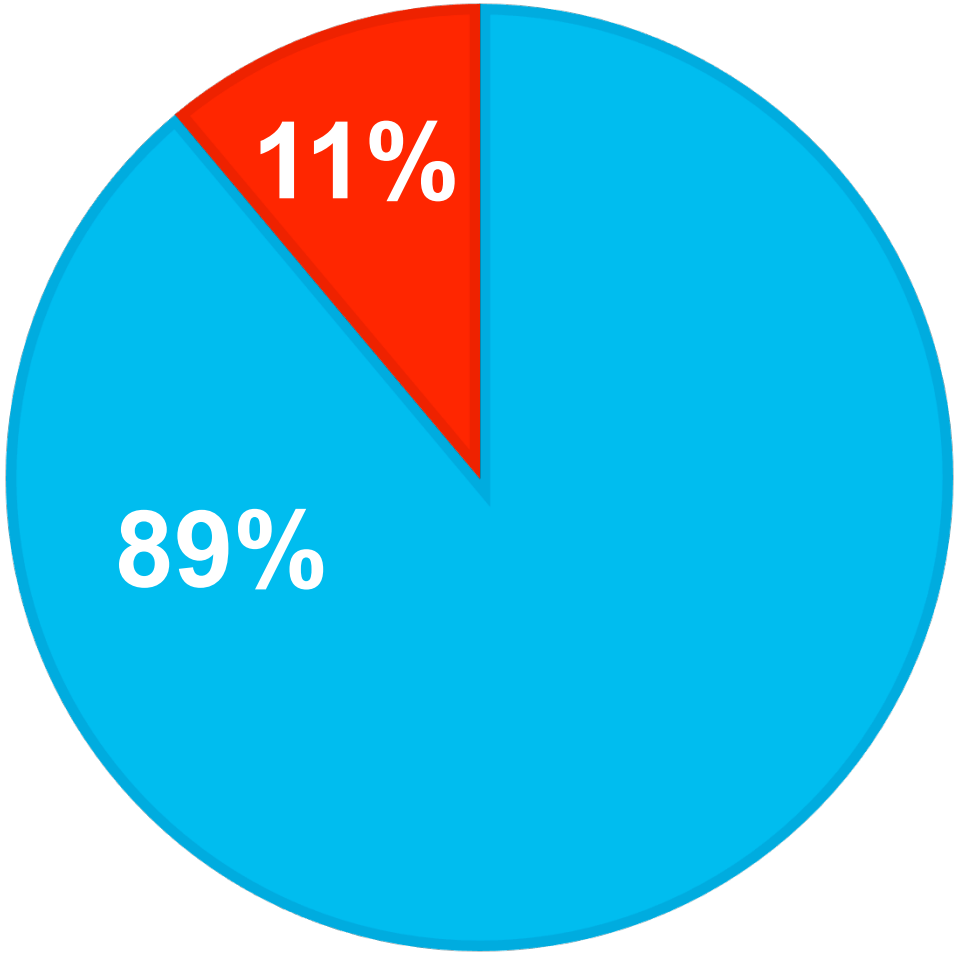
2015 – Quieter in Some Ways



Typical “Day in the Life”
DNS Queries Seen at Resolvers

DDoS

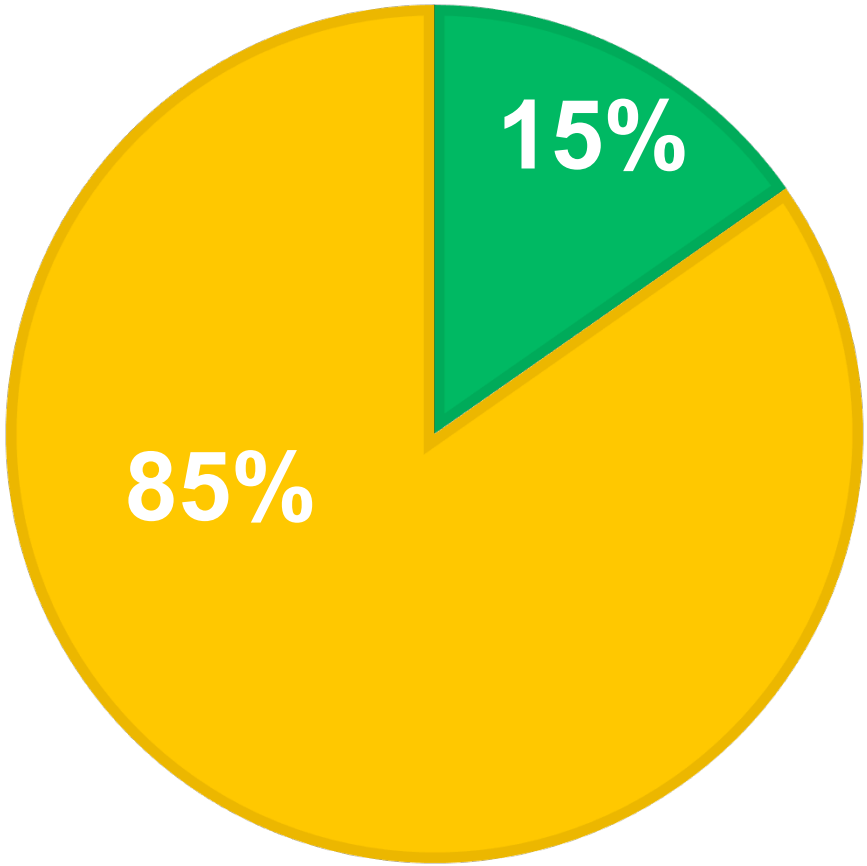
Other



Typical Day in The Life
DDoS Queries Seen at a Resolver

Amplification

Random Subdomain



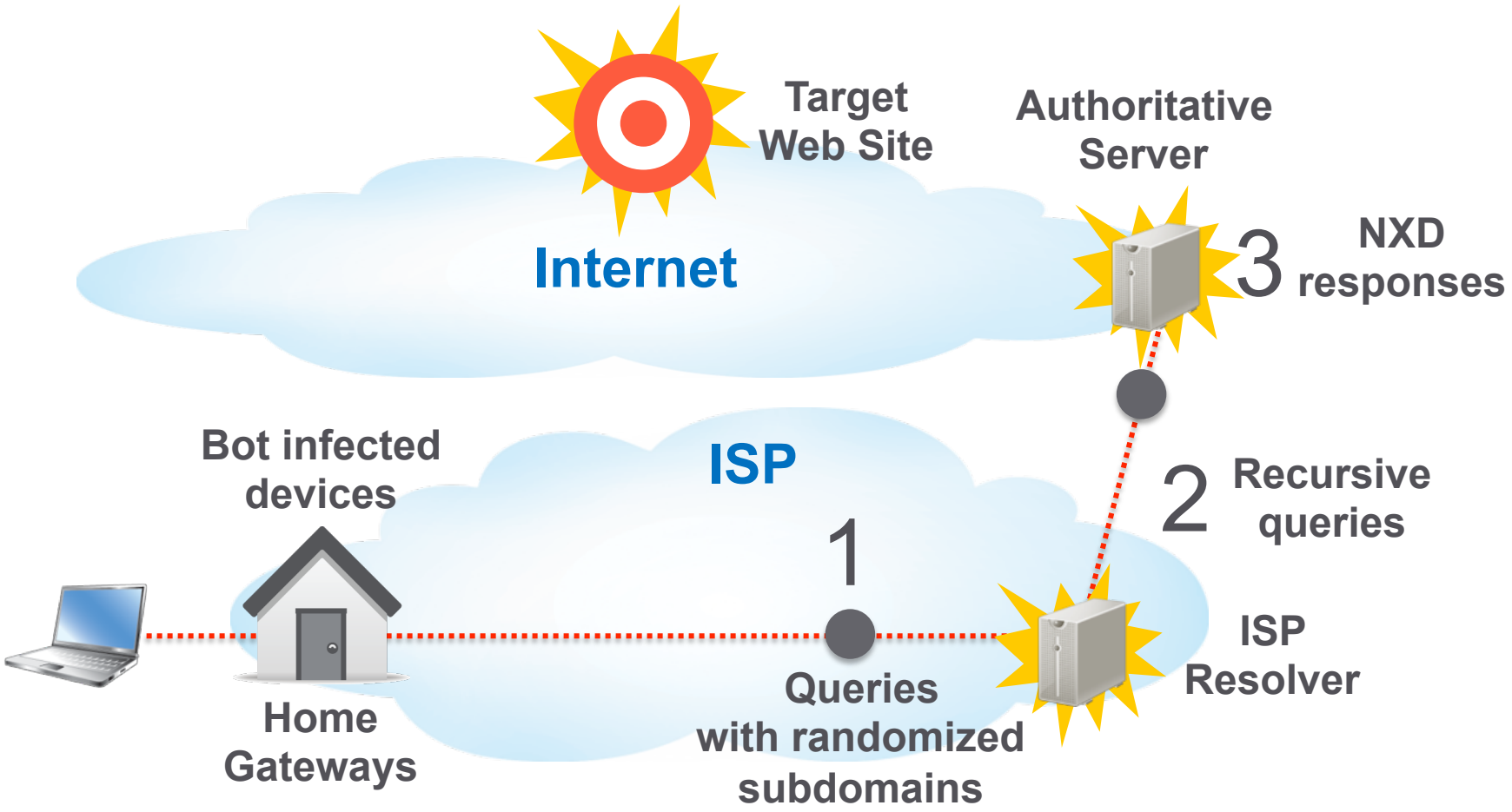
Observations

- Use of open resolvers/proxies still predominates
  - Installed base around 17 M
  - Trend toward more stealthy attacks - Send enough traffic to bring down authorities
  - Highly distributed attacks – 1,000s of open resolvers per attack
  - Often low intensity per IP
  - Interesting recent example: www.appledaily.com

Observations

- Bot based attacks
  - Tend to be few IPs - tens to hundreds
  - High to very high intensity per IP
    - Up to 1000s of QPS/IP
    - Long tail with lower QPS
  - Recent interesting example: rutgers.edu

Attacks Using Bots



What's Happening?

Network scans for vulnerable devices:
Home gateways or other "Things"

Attempts login with default passwords

Many utilities at the attackers disposal
Load and run malware

Other vectors possible: Bots with loaders, Rompager

The Problem

- Considerable stress on DNS infrastructure:

  Resolvers

  Queries require recursion (computationally expensive)

  Working around failed or slow authorities

  Stress concentrates as authorities fail

  Authorities

  Unexpected query spikes exceed provisioned limits

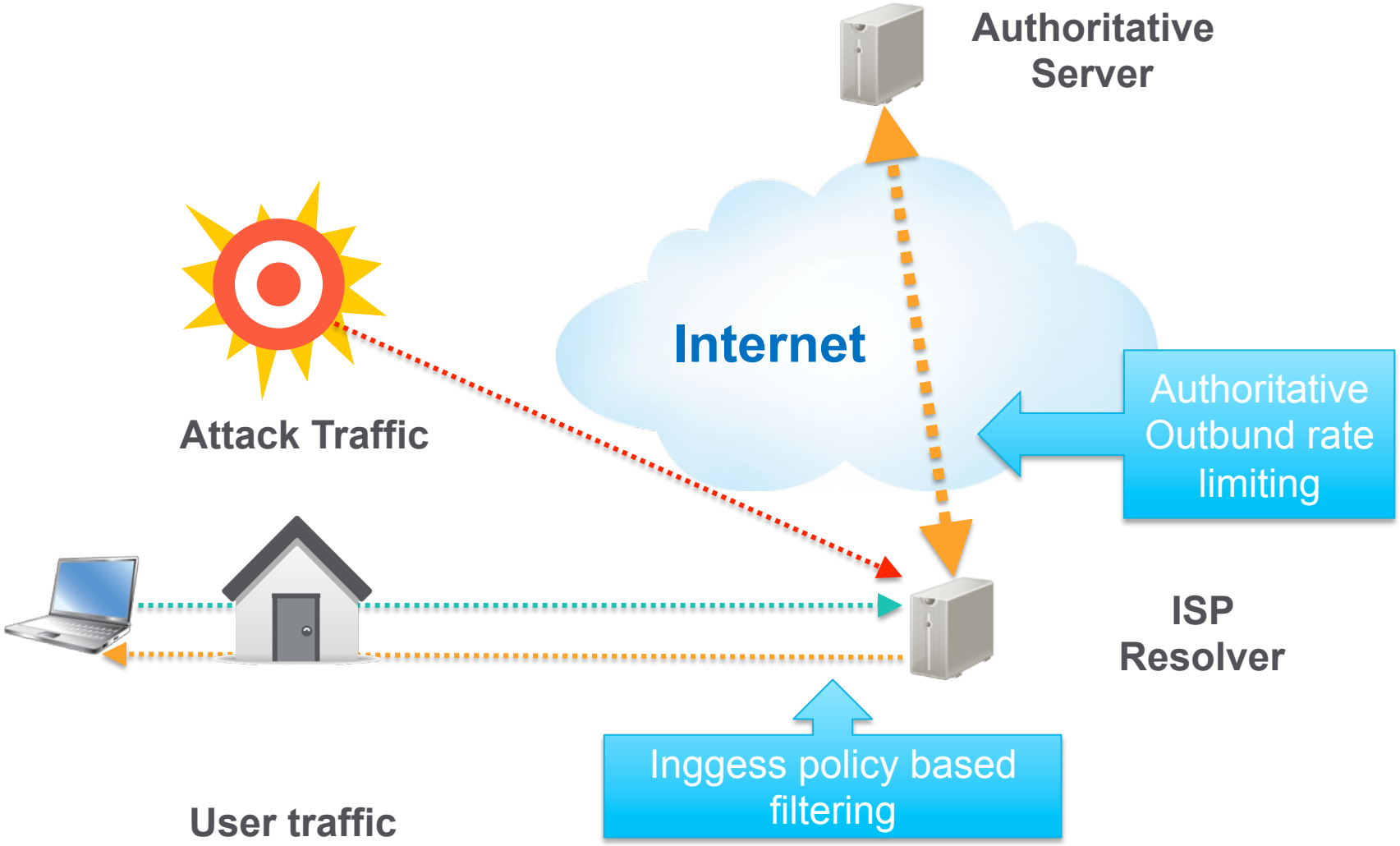
Goals for Remediation

- Minimize work for resolvers
- Eliminate bad traffic to authoritative servers
- Answer legitimate queries
- Answer legitimate queries for attacked domains
  - don't drop, don't SERVFAIL

- Two approaches being used:
  - Rate limit traffic to authorities
  - Ingress filtering

How do they behave in practice?

Testing Efficiency of Rate Limiting



Test Diagram

Redwood City, CA

good traffic
10kqps background
100qps for test domains

Regensberg
, Germany

2 domains
being attacked

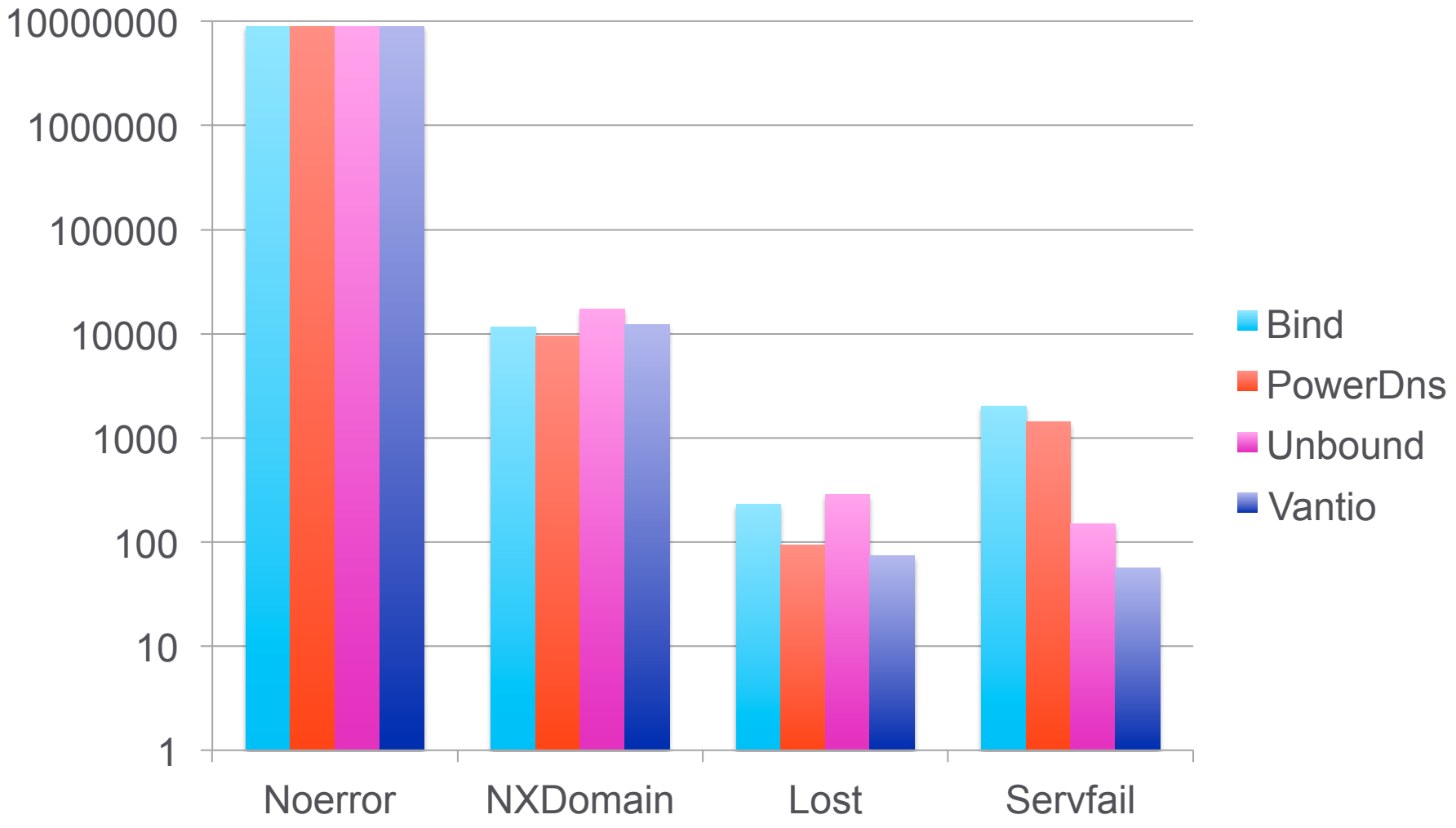
attack traffic
2 * 5000 qps for
two domains

other
resolutions

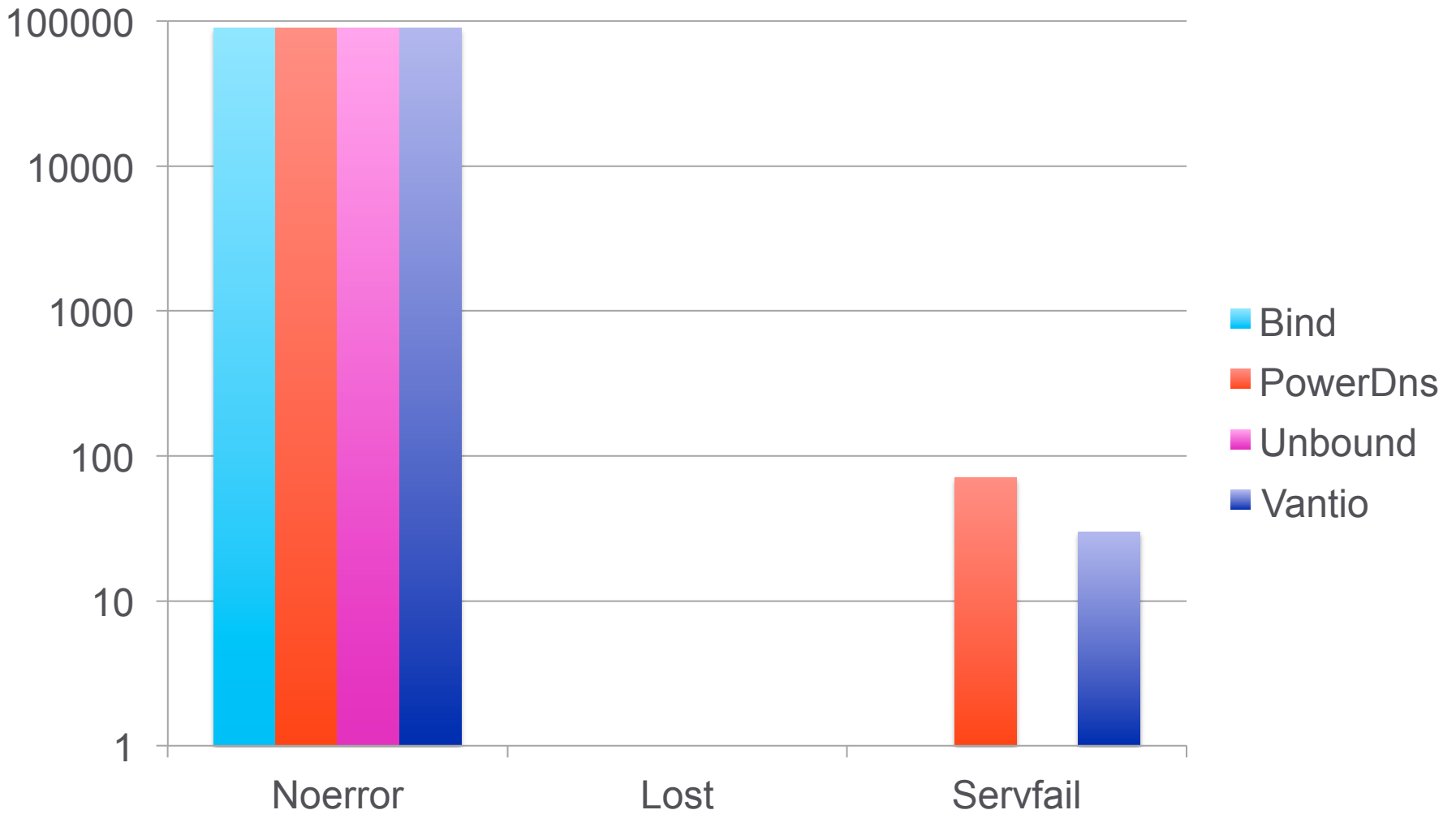
100qps
1qps

Rate limits should not be hit for normal traffic
Resolver and authoritative servers record traffic

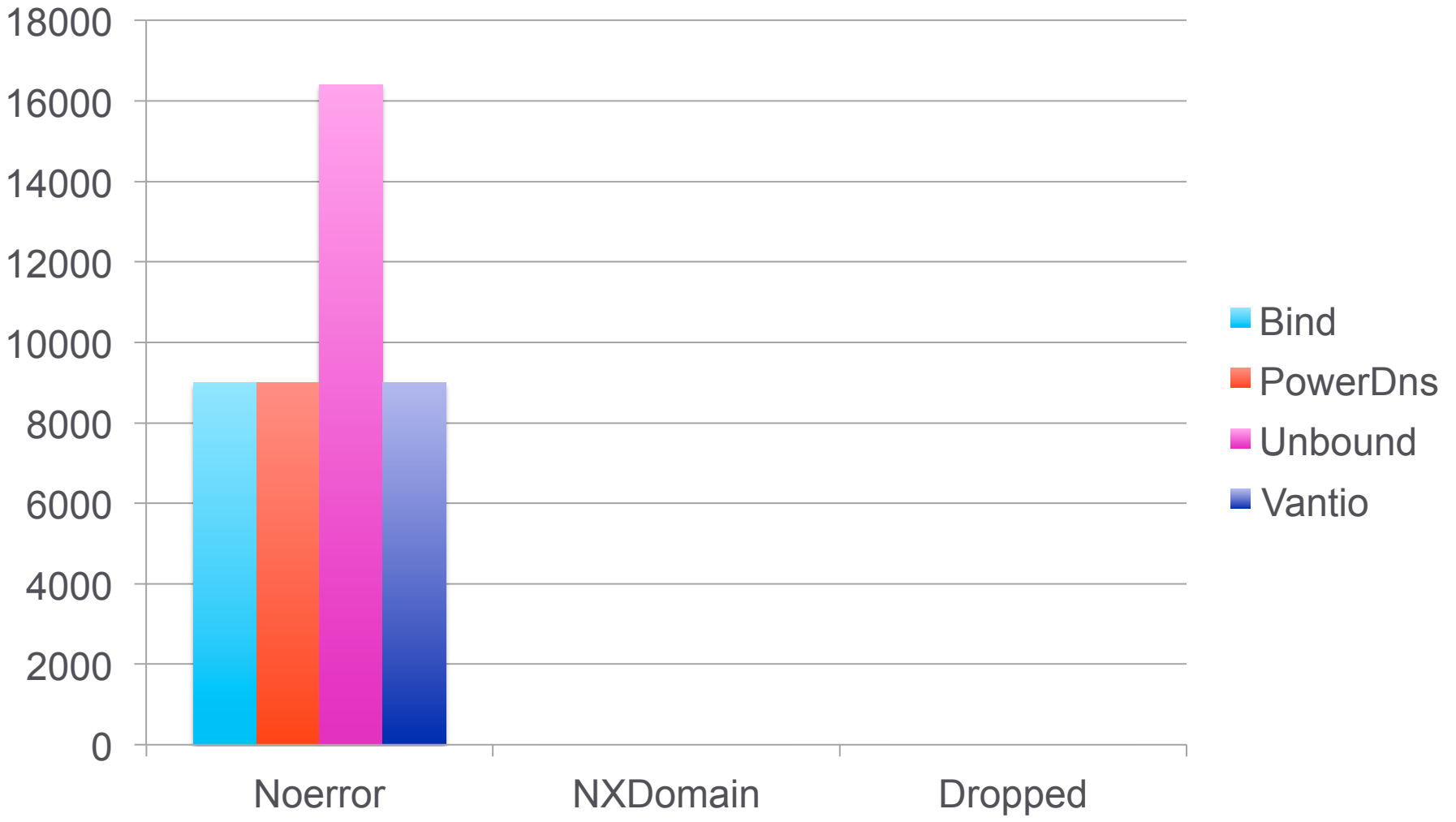
Run good traffic: User results



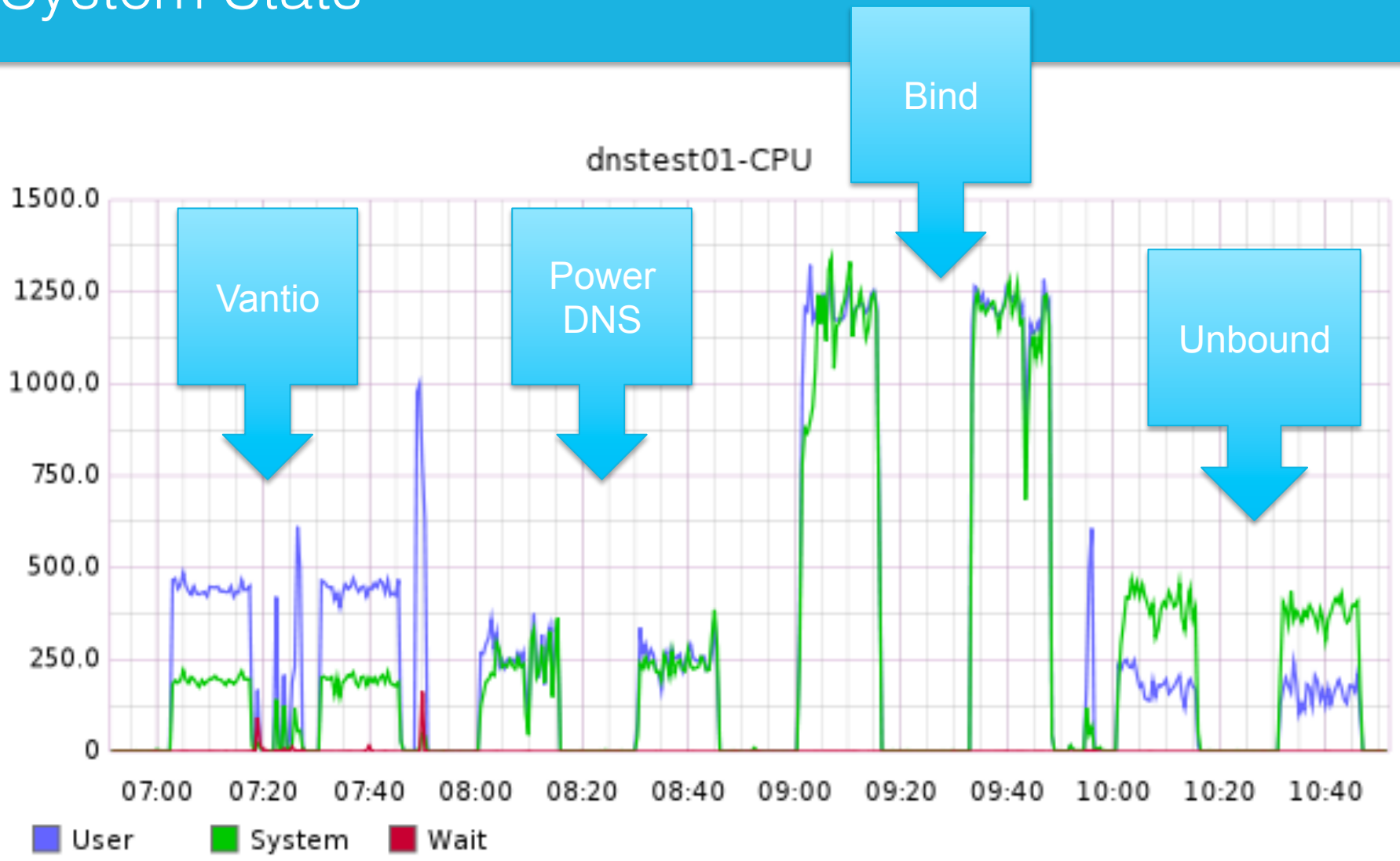
Run good traffic: Test domains results



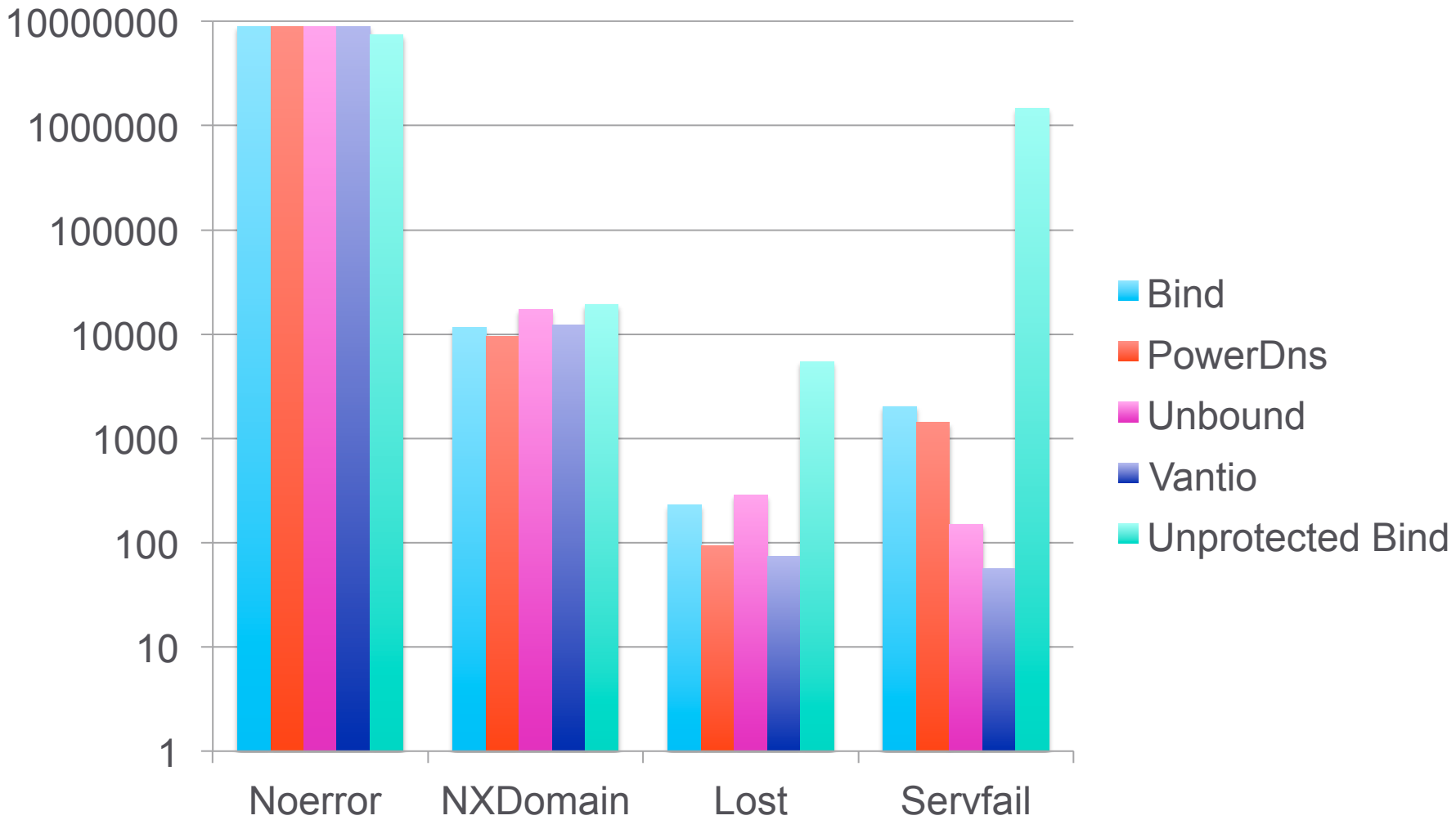
Run good traffic: Authoritative Server Results



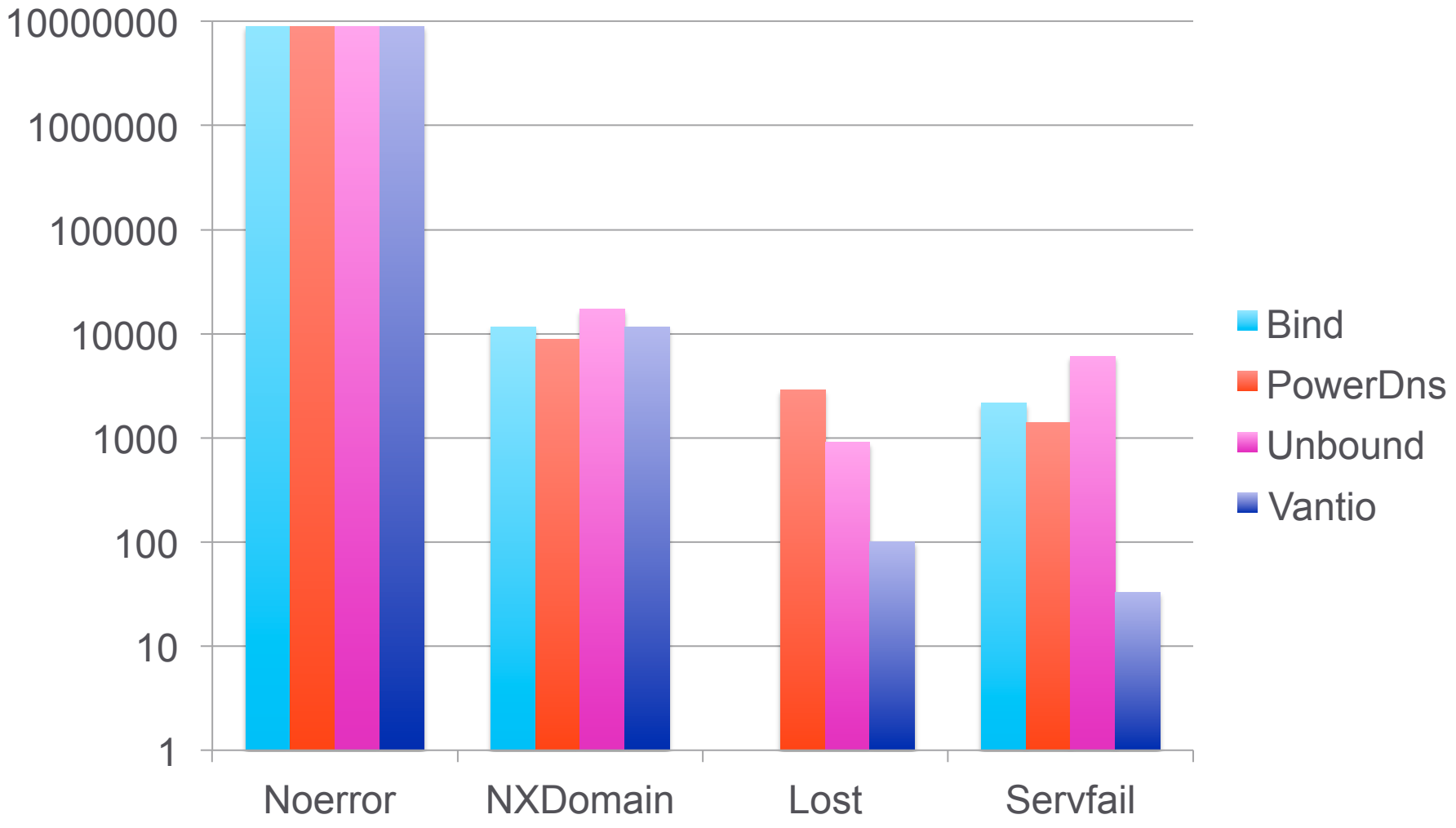
System Stats



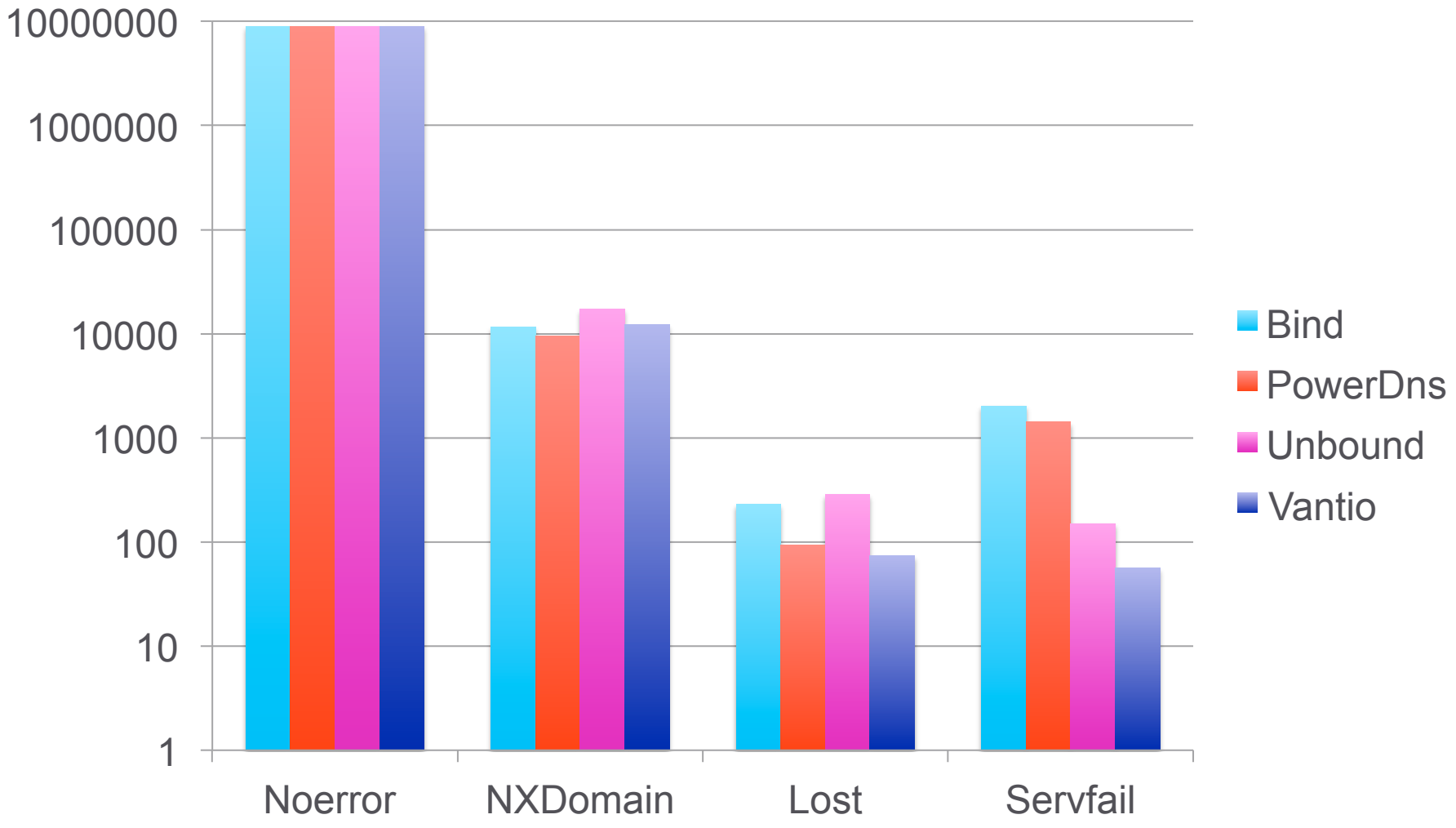
Run attack traffic – Compare with normal



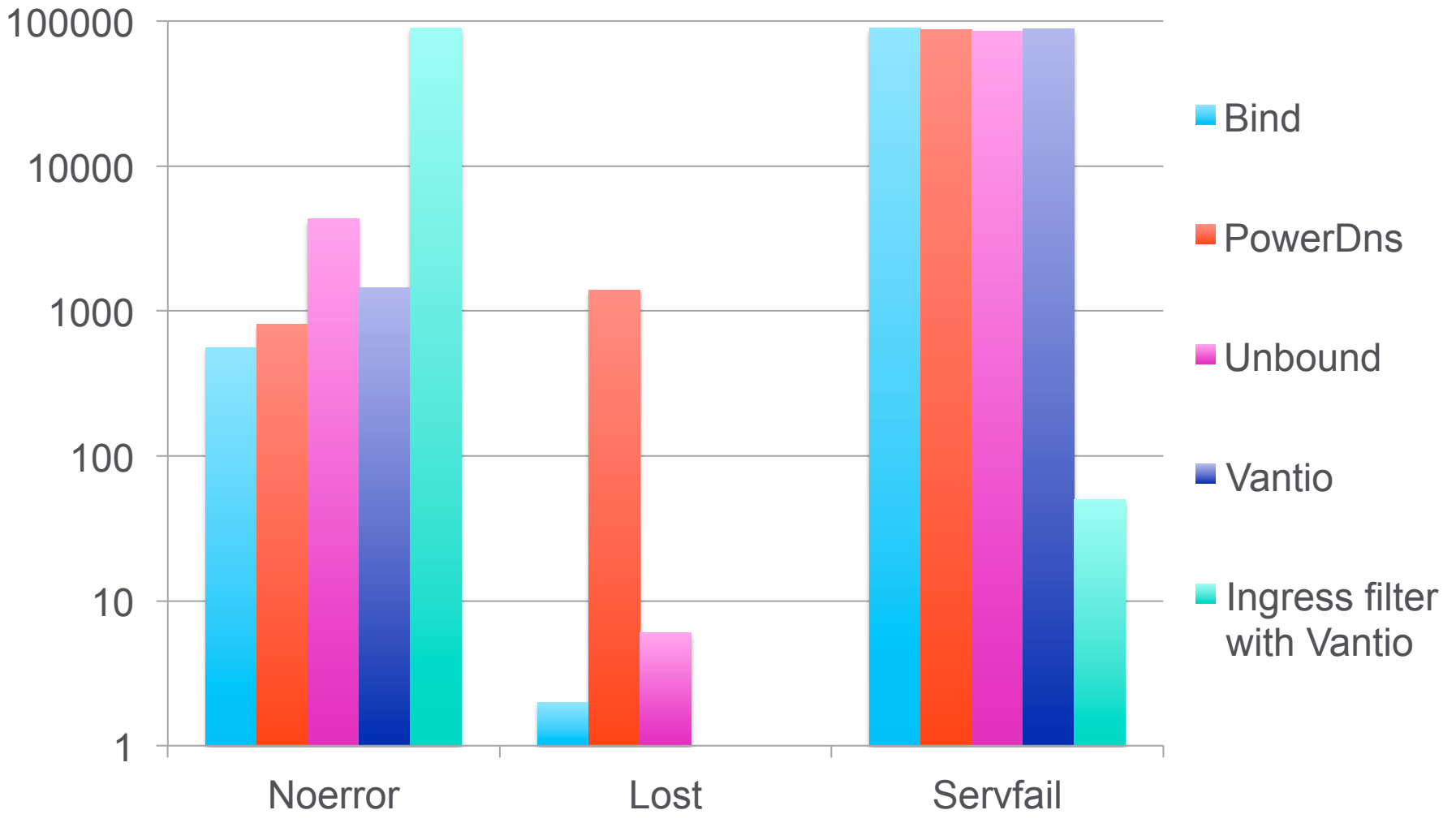
Run protected attack traffic: User results



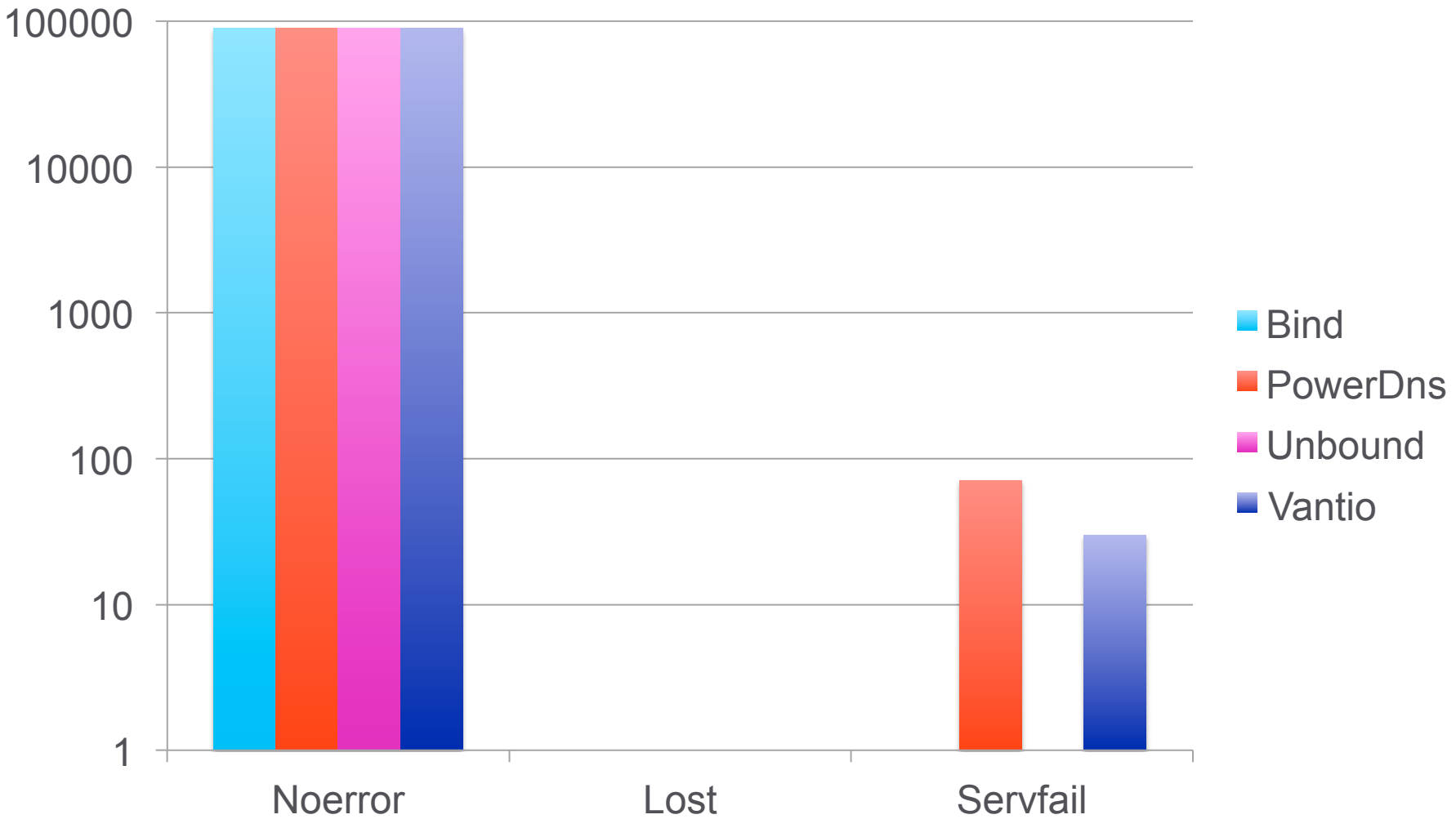
Run good traffic: User results



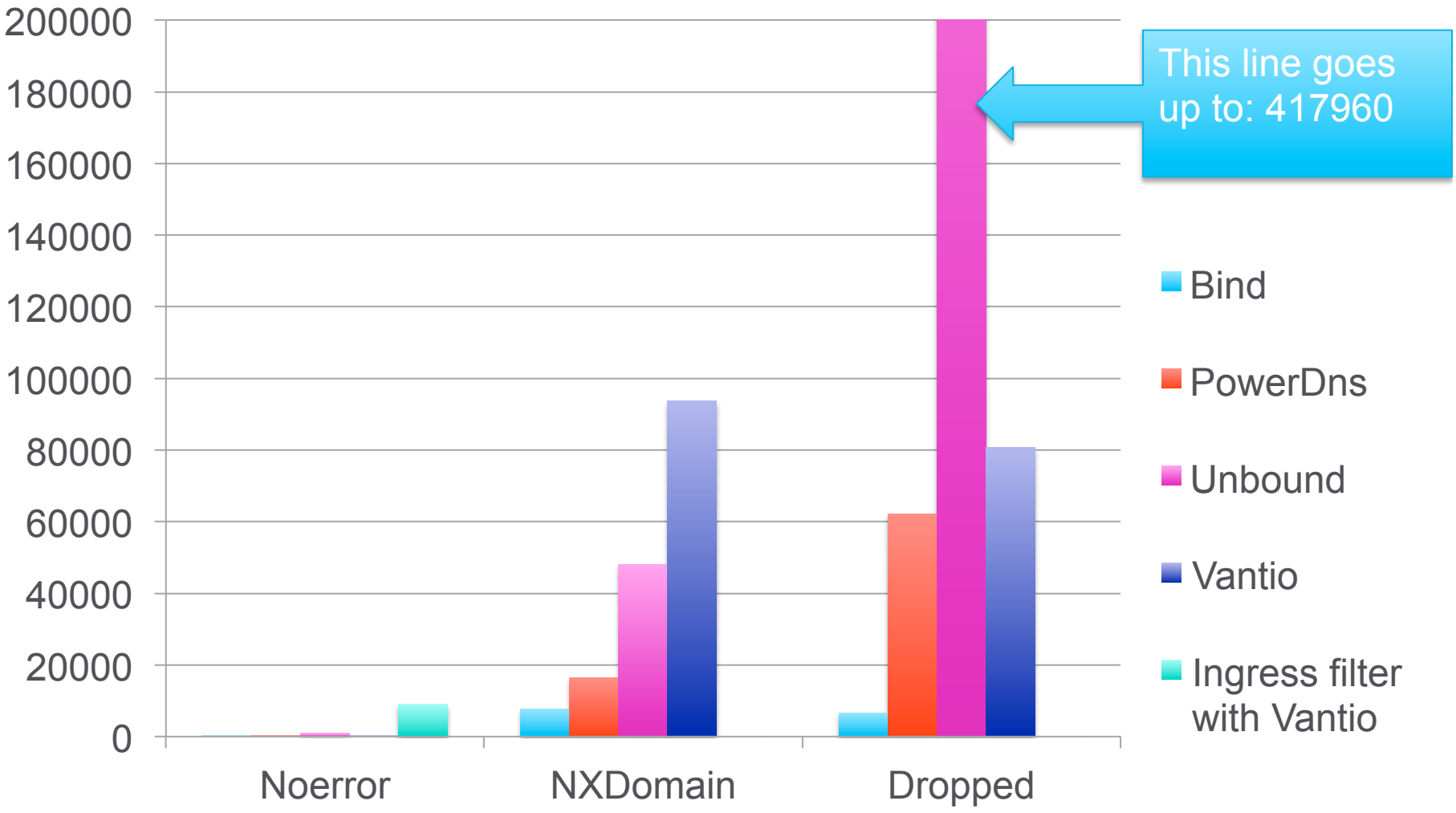
Run protected attack traffic: Test domains results



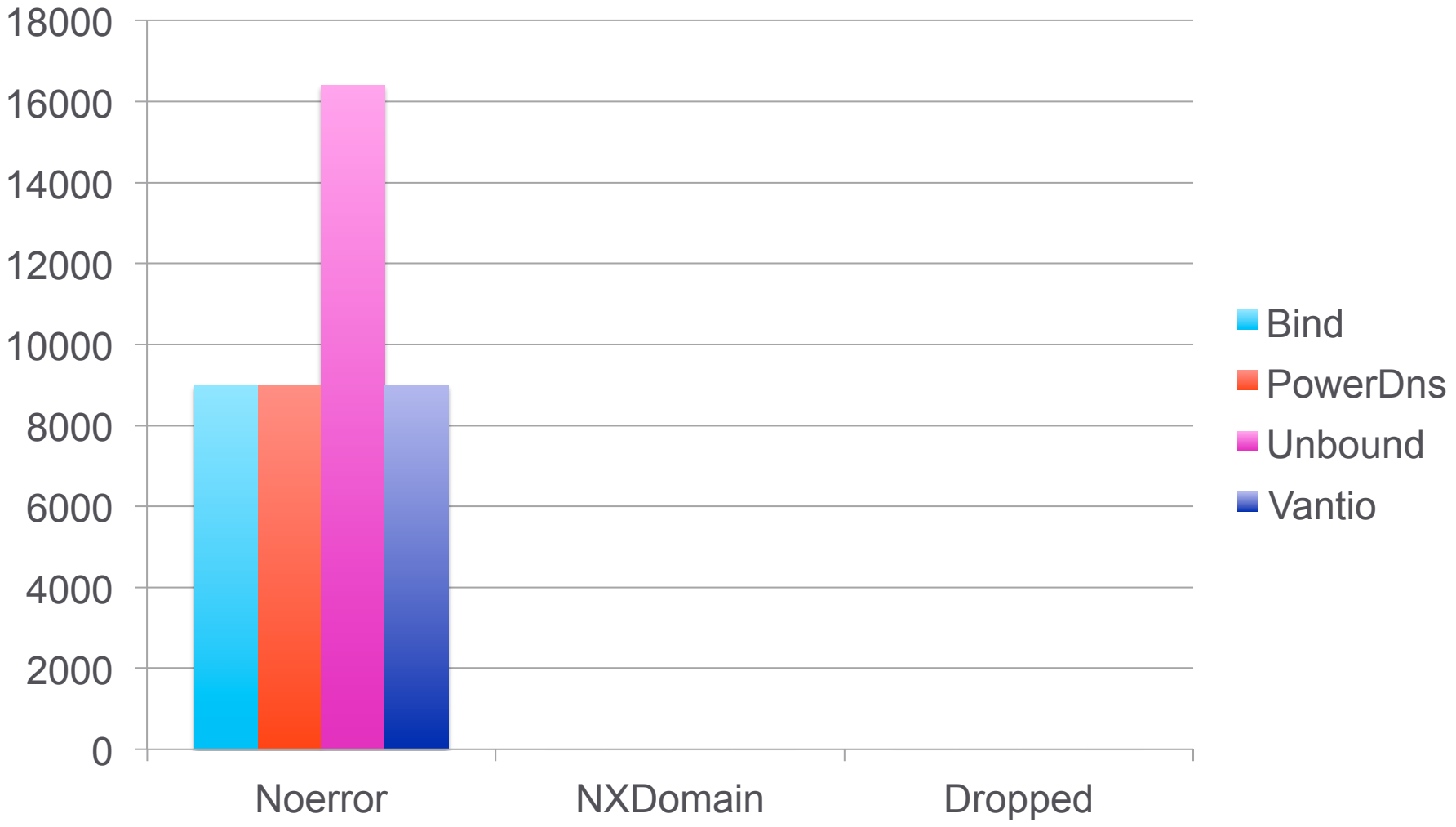
Run good traffic: Test domains results



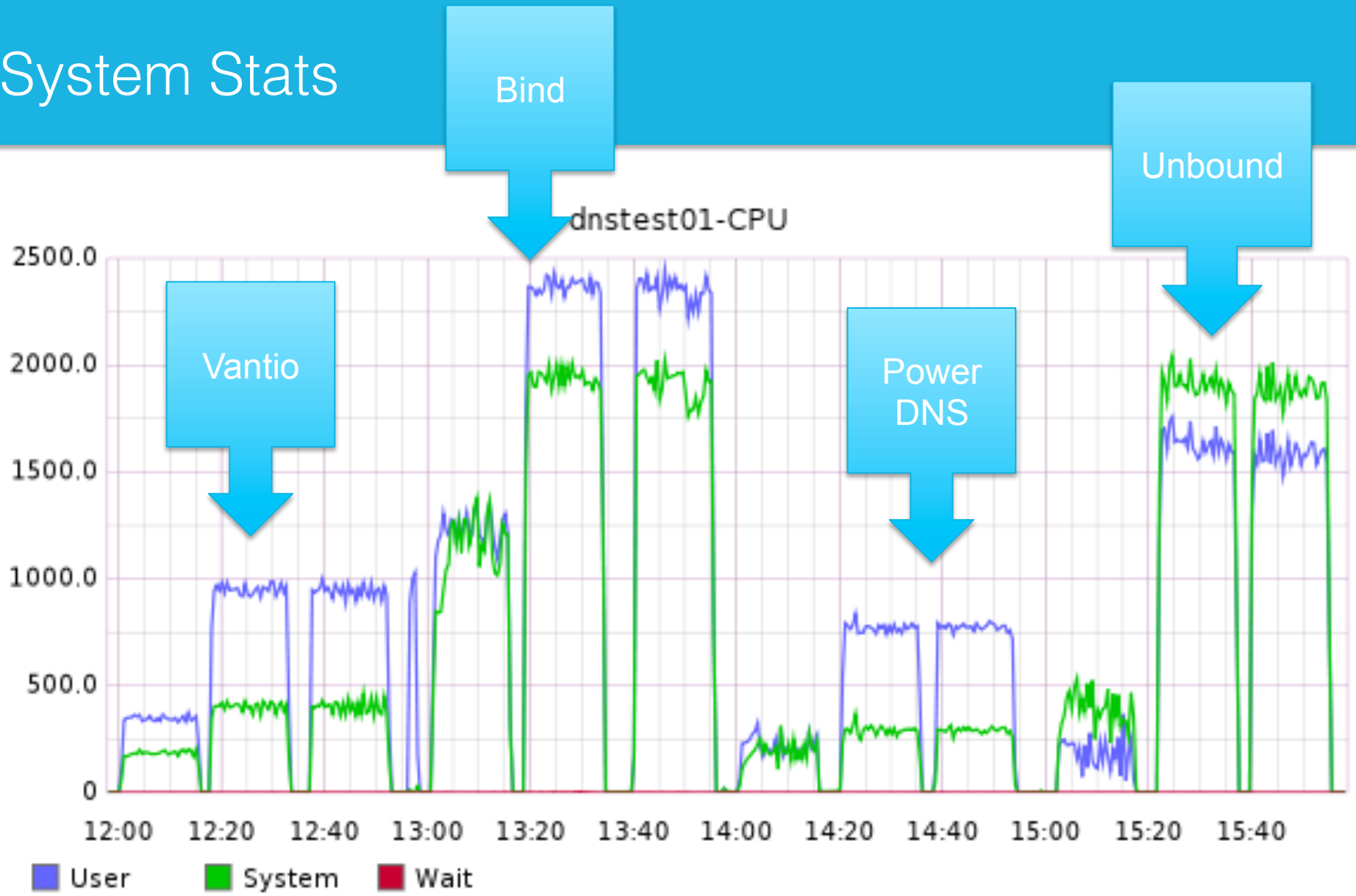
Run protected attack traffic: Authoritiative Server Results



Run good traffic: Authoritative Server Results



System Stats



Results: Resolver Traffic 9,000,000 queries

Resolver	Test run	Type	No Error	NXDomain	Lost	Servfail
Vantio	3	Good	8987622	12248	74	56
	5	Attack	8988291	11576	100	33
ingress filter	7	Attack	8978049	20668	1142	141
PDNS	3	Good	8989007	9477	94	1422
	5	Attack	8986967	8767	2868	1398
Bind	3	Good	8986205	11537	231	2027
	5	Attack	8985913	11571	371	2145
unprotect	7	Attack	7497150	19291	5436	1478123
Unbound	8	Good	8982254	17309	287	150
	9	Attack	8975942	17114	901	6043

Results: Attack domains

Software	Test Run	Type	No Error	Lost	Servfail	Auth Noerror	Auth NXDomain	Auth Dropped
CS7	3	Good	89970	0	30	8997	0	0
	5	Attack	1450	0	88550	145	93684	80790
ingress filter	7	Attack	899950	0	50	8998	0	0
PDNS	3	Good	89929	0	71	8995	0	0
	5	Attack	807	1395	87798	99	16317	62131
Bind	3	Good	90000	0	0	9000	0	0
	5	Attack	560	2	89438	56	7683	6670
unprotect	7	Attack	3310	160	86530	332	94315	2538256
Unbound	8	Good	90000	0	0	16401	0	0
	9	Attack	4311	6	85584	910	48110	417843

Test Results Summary

	Ingress Filtering	Rate Limit Authorities
Eliminate bad traffic to authoritative servers	**YES**	**SOME**
Correctly answer legitimate queries (don't drop, don't SERVFAIL)	**YES**	**YES**
Correctly answer legitimate queries for attacked domains	**YES**	**NO**

Summary

- Constant DNS Based DDoS evolution
- Open Home Gateways remain a problem
- Malware-based exploits create broad exposure

- Not clear where attacks are headed
- Evidence attackers refining techniques
- Remediation needs to be undertaken with care