
nominum™
Harness Your Internet Activity

DNS Trials and Tribulations
DENOG, Darmdtadt
October 2015

Ralf Weber

Intro Nominum

- Paul Mockapetris – founder and chairman
- Engineers architected and initally wrote BIND 9
- Deployed in over 40 countries
- Used by >400M subscribers daily
- Processes >1.8 trillion transactions daily

Nominum Customers

DNS is An Attractive Target

- Every network has it
- It's easy to find
- Carefully maintained
- Powerful servers
- High bandwidth
- Numerous ways to exploit

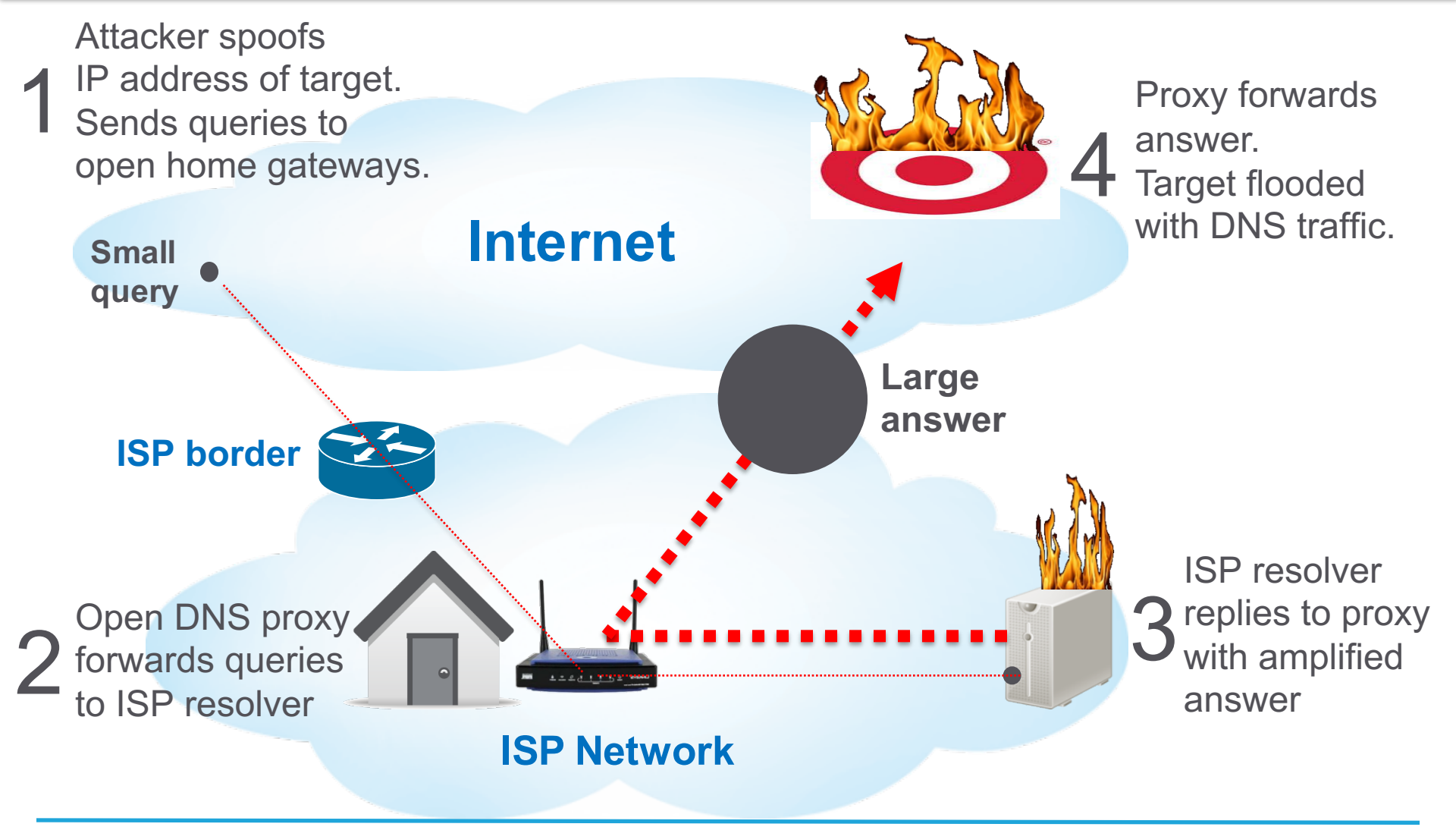
DNS Exploits

- Cache Poisoning
- DNS-based DDoS
- DNS Tunneling

Summer 2008:Internet Wake Up Call Kaminsky Vulnerability

- **Industry Response:**
  - Temporary measure - UDP SPR
- **Nominum Response:**
  - Layered defenses **STOP** Kaminsky'
  - 170 M households protected
- **Long Term Response:**
  - DNSSEC
- **Market Requirements:**
  - Secure the DNS
    - Strong protections for unsigned domains
    - Simple management for signed domains
  - Safe, secure and productive Internet experience

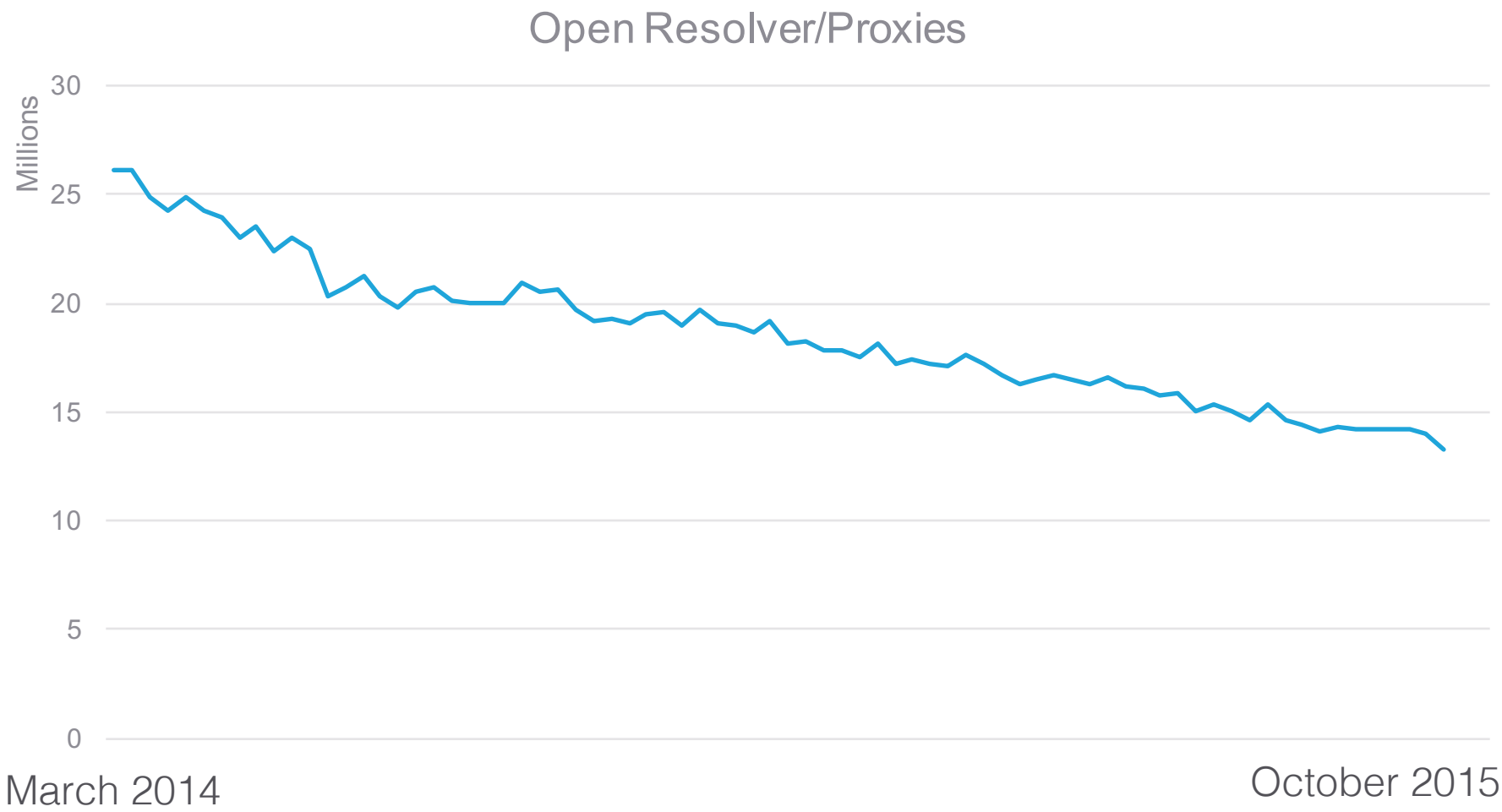
DNS DDoS: Amplification Attacks



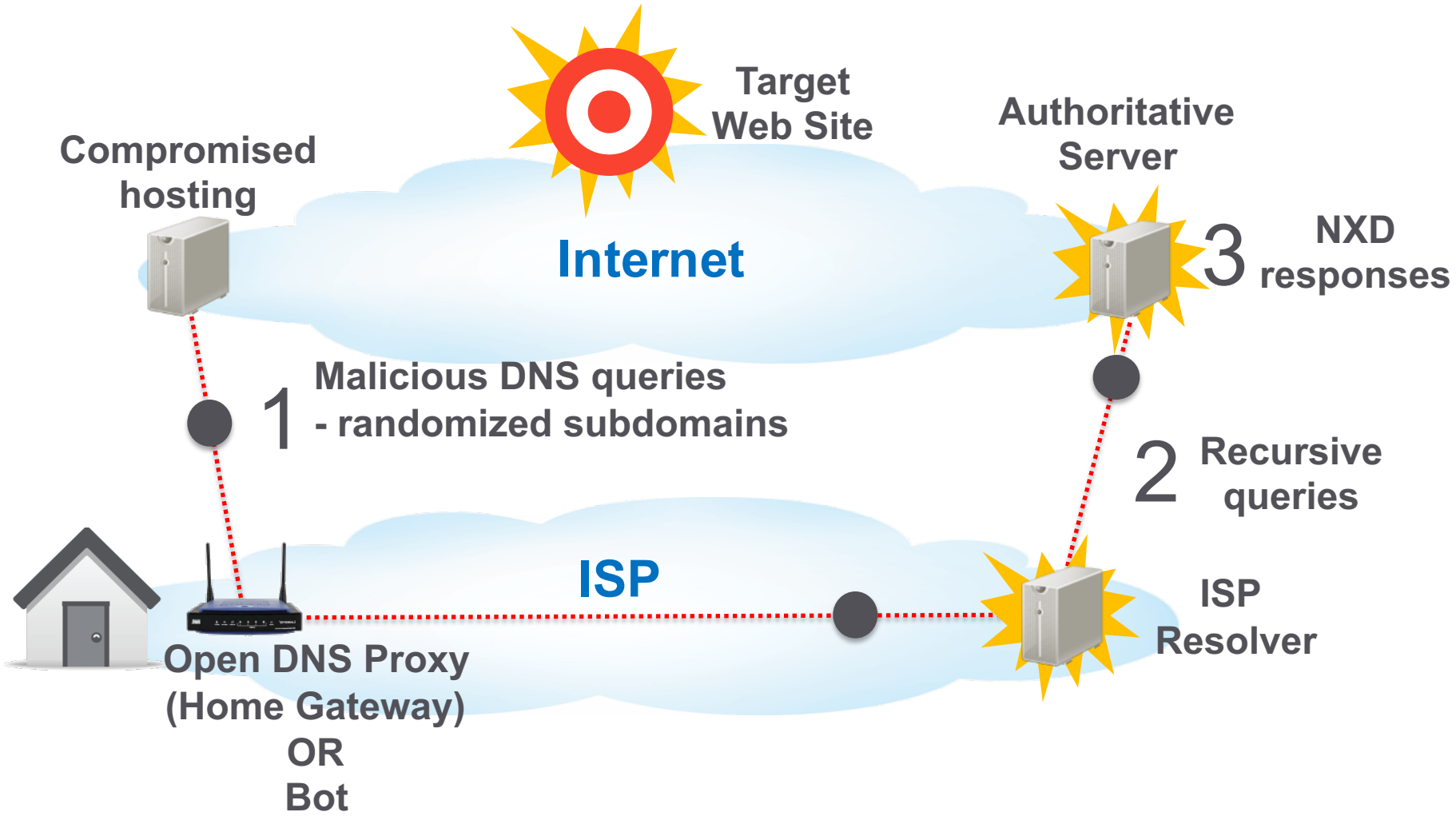
Amplification attacks

- **Industry Response:**
  - RRL
- **Nominum Response:**
  - RRL
  - Rate Limit ANY queries (maybe HINFO tomorrow ;)
  - Drop purpose build domain immediatley
  - Rate Limit legitimate domains that have huge answers

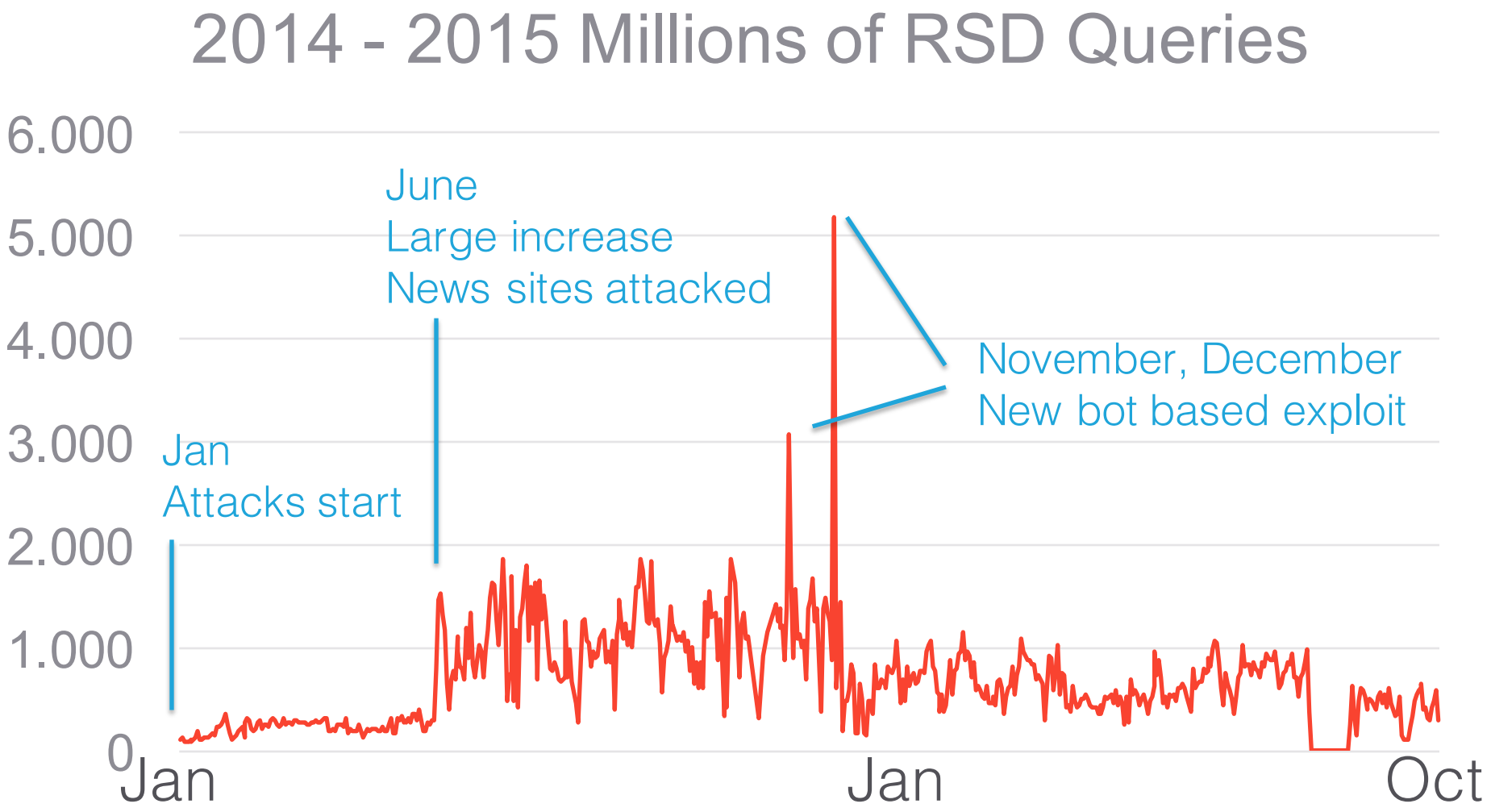
Open Resolver/Proxies are declining but,….



DNS DDoS: Random Subdomain Attacks



DNS DDoS Activity



Random Subdomain Attacks

RANDOM **TARGET NAME**

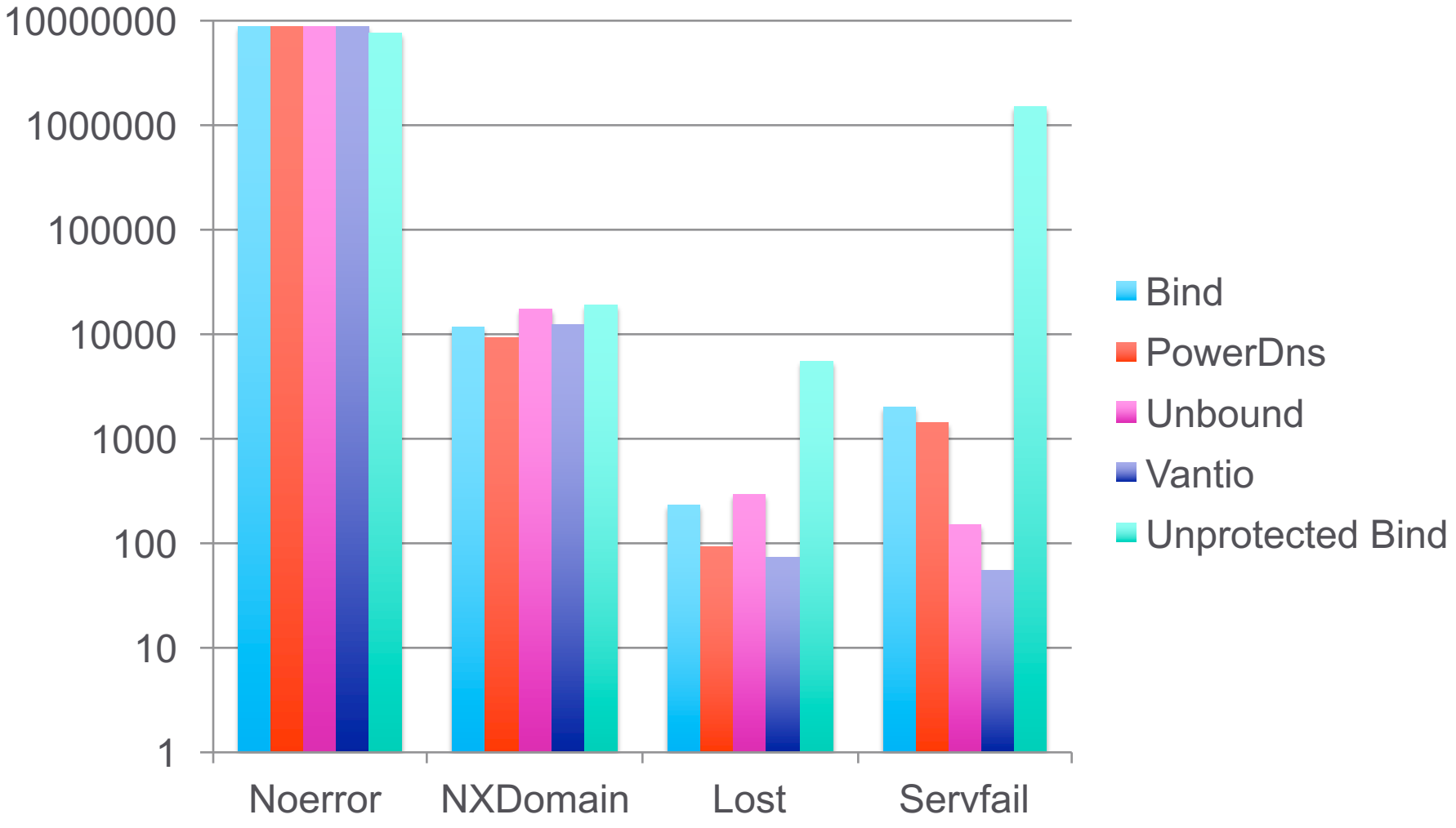
wxctkzubkb. liebiao.800fy.com

- Queries with random subdomains
  - Answer with “non-existent domain” (NXD)
- Creates lots of work for resolvers
  - Queries require recursion
- Creates lots of works for authoritative servers
  - Heavy volumes of NXD queries often cause failure

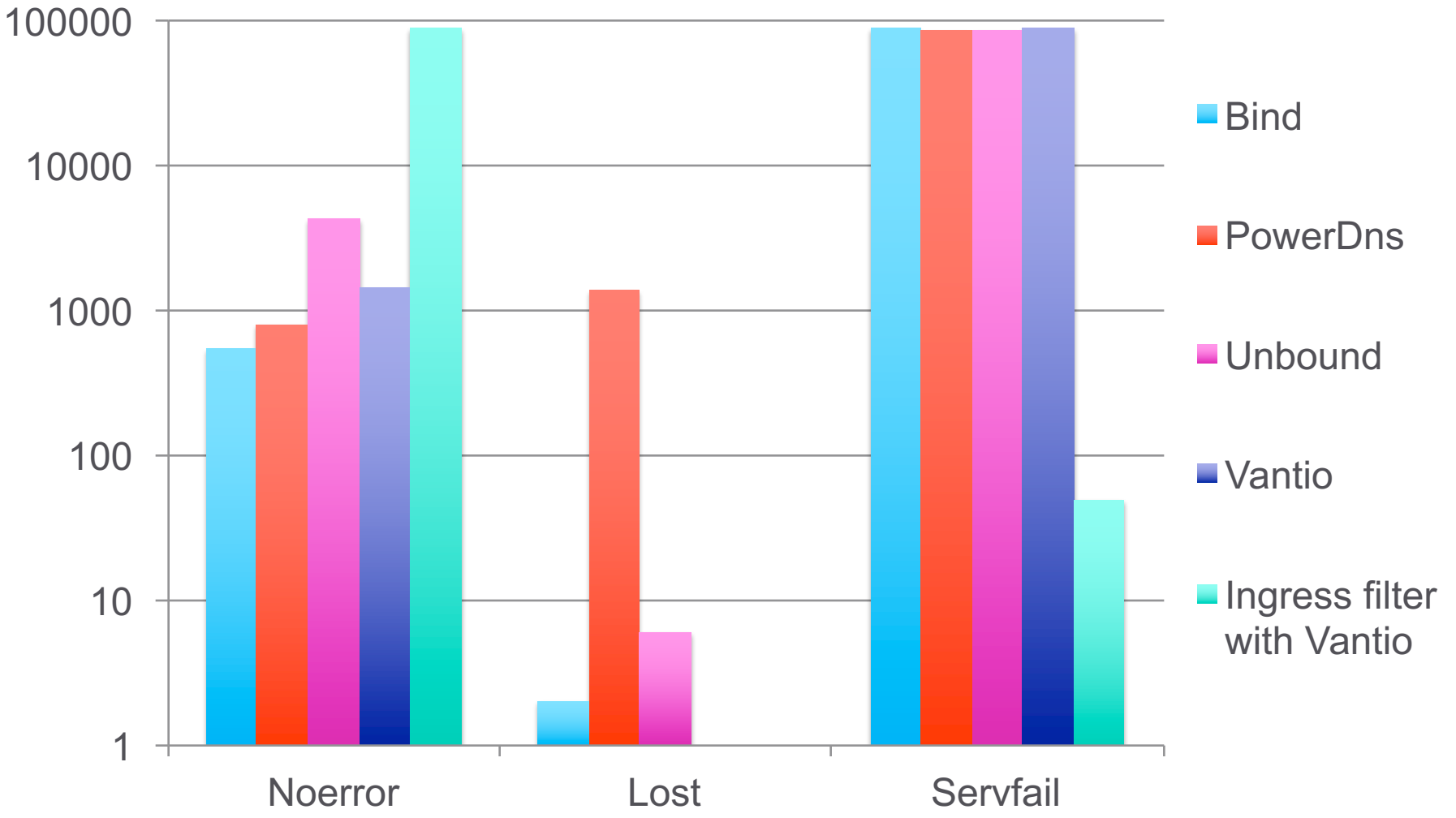
Random subdomain attacks

- **Industry Response:**
  - Outbound Rate Limiting
- **Nominum Response:**
  - Outbound Rate Limiting
  - Ingress filtering with white list to protect good traffic
    - Requires knowledge of historic traffic to know good domains
    - Is the only way to protect the attacked domain

Run attack traffic – Compare with normal



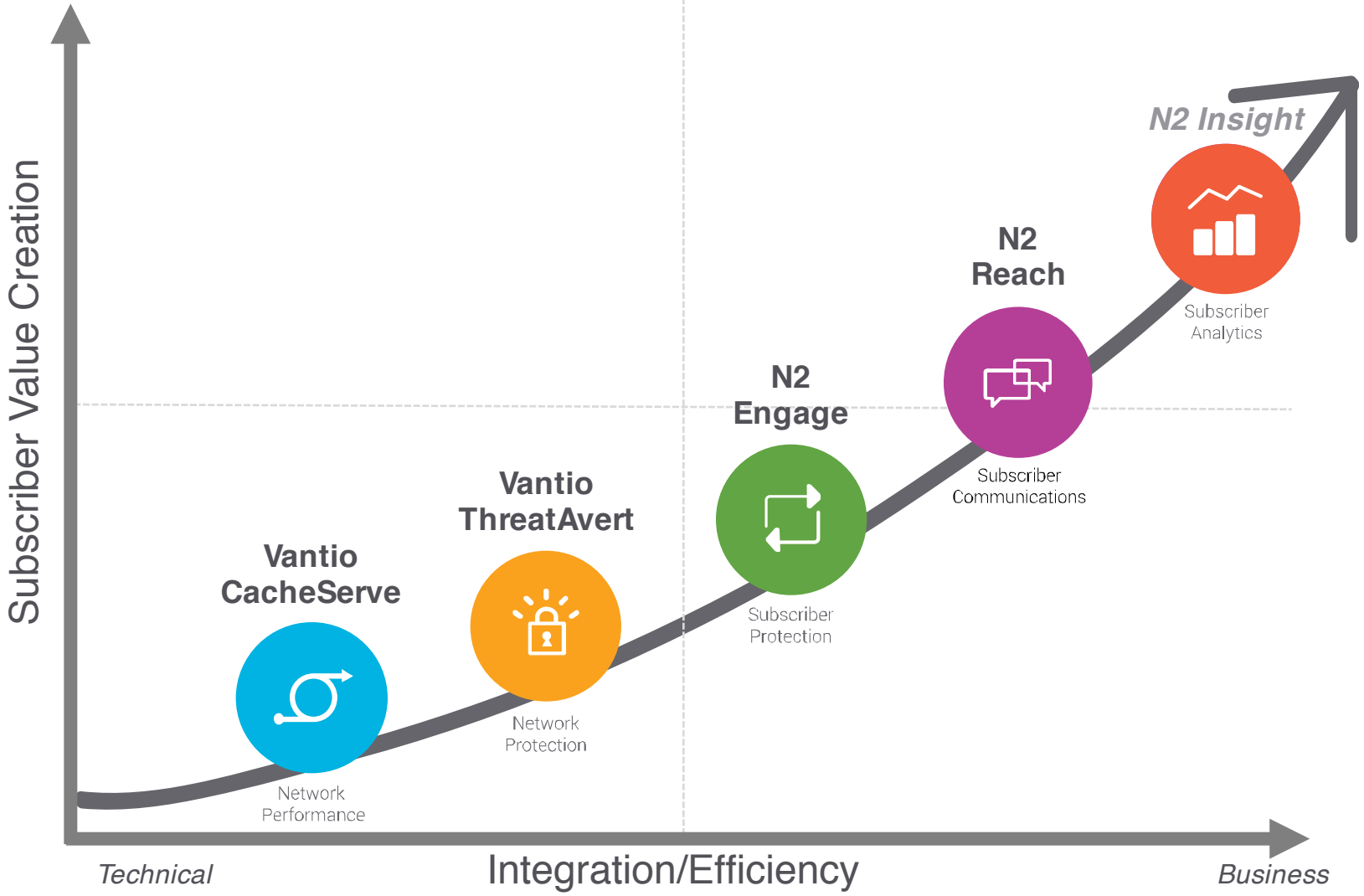
Run protected attack traffic: Test domains results



Global Intelligence eXchange (GIX) Overview

- Nominum's threat detection system
  - Worldwide data network, systems and people responsible for identifying and responding to global threats
- Successful 5+ year track record
  - Deployed in 21 countries
  - First automated detection of DNS amplification, random subdomain & DNS tunneling attacks
  - Exceptionally low false positive rate
- Dedicated research organization
  - Twelve (12) full time security researchers, data scientists & analysts
  - Experience in security, machine learning & DNS
  - Patented research methodology and algorithms
- Global sensor network
  - More than 4 TB of DNS data per day from the worlds largest networks
  - Over 300 sources of external data

Where the DNS is Going



Summary

DNS *Needs* Protection!
Defeat cache poisoning
Protect good traffic
Block bad traffic at *resolvers*

Better DNS,
Better Network,
Better Business