Random Subdomain Attacks

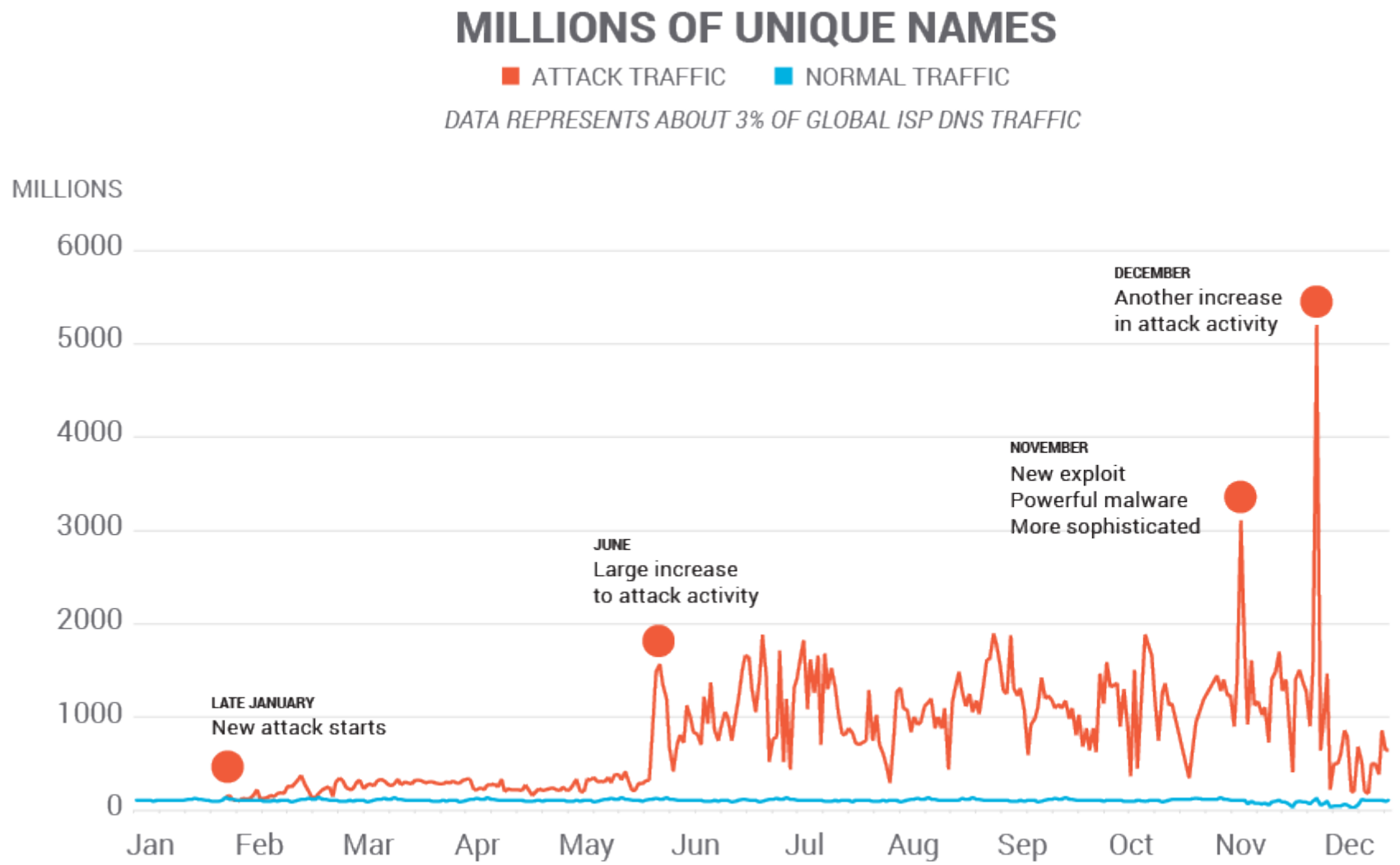
Netnod spring meeting 2015
Stockholm, Sweden

Mikael Kullberg

Nominum Research

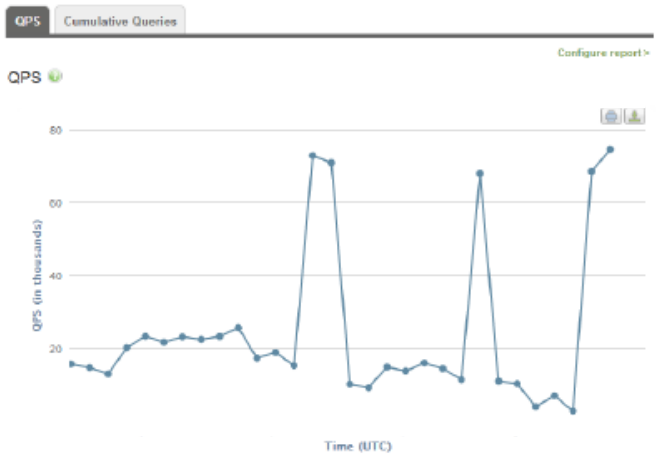
- Nearly 2 Terabytes of data analyzed per day
  - Anonymized from ISPs worldwide
  - Estimate about 5% of ISP DNS resolver traffic
- Team of data scientists
- Algorithms searching for:
  - DDoS
  - Bots
  - Malware
  - Machine generated traffic
  - Etc

DNS DDoS in Increasing: 2014 Data

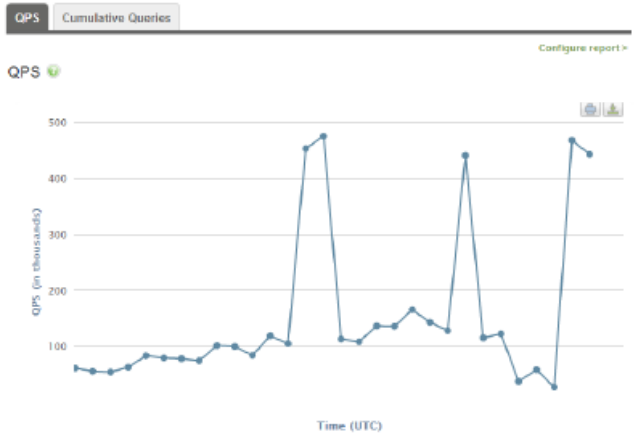


Attacks Coordinated Worldwide

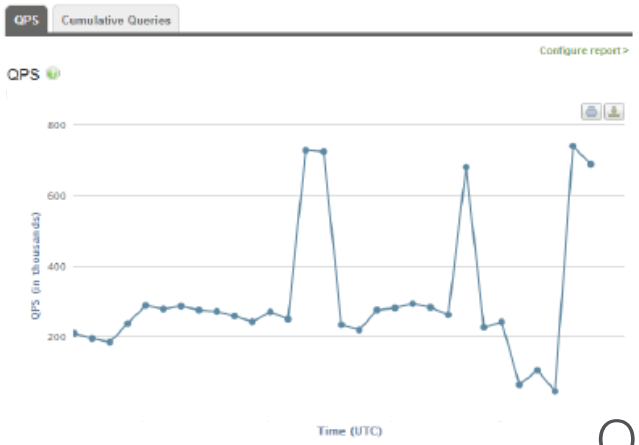
Large ISP EMEA



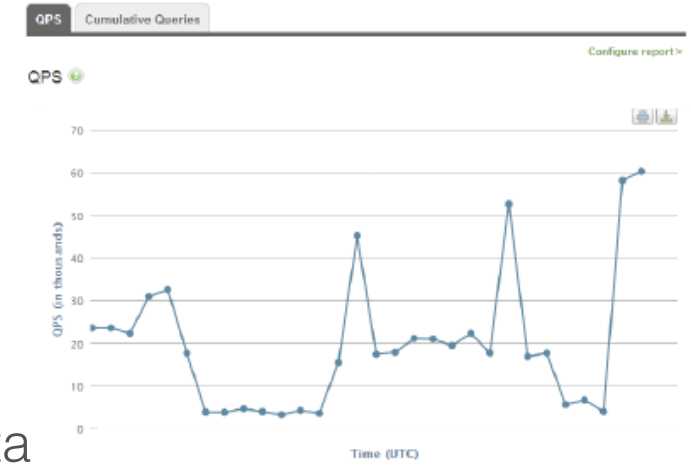
Large ISP LATAM



Large ISP North America



Large ISP APAC



One weeks data

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

Attacks have Evolved

- We have seen 4 distinct attacks:

2014 - Worldwide attacks using open DNS proxies

Nov 2014 – first attacks using bots

Dec 2014 – Spike in intensity per IP

Jan 2015 – Highly focused attacks

Different Kinds of “Random”

nbpdestuvjklz.pay.shop6996.com.

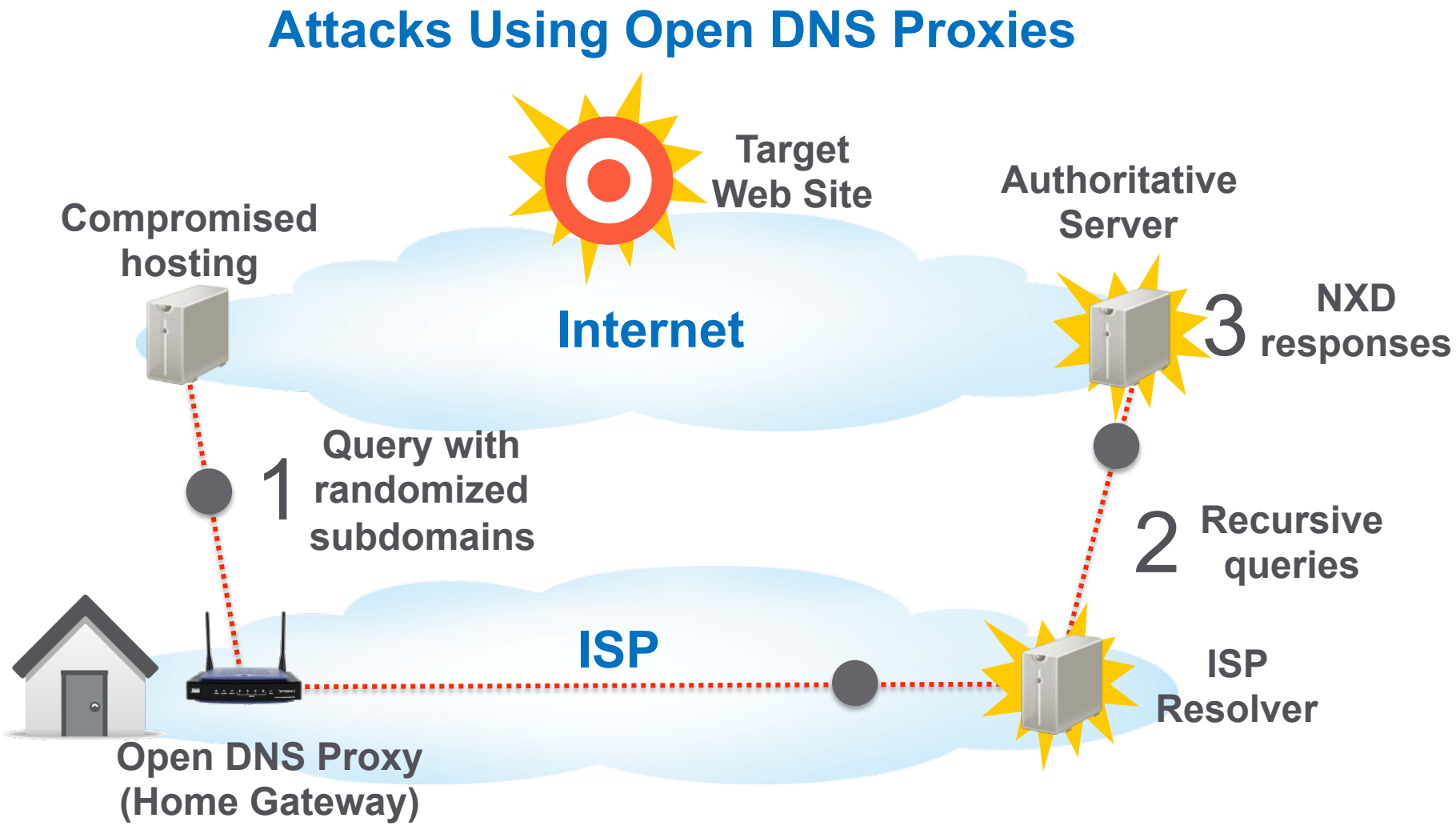
1lHecqrP.xboot.net.

hxdfmo.iyisa.com.

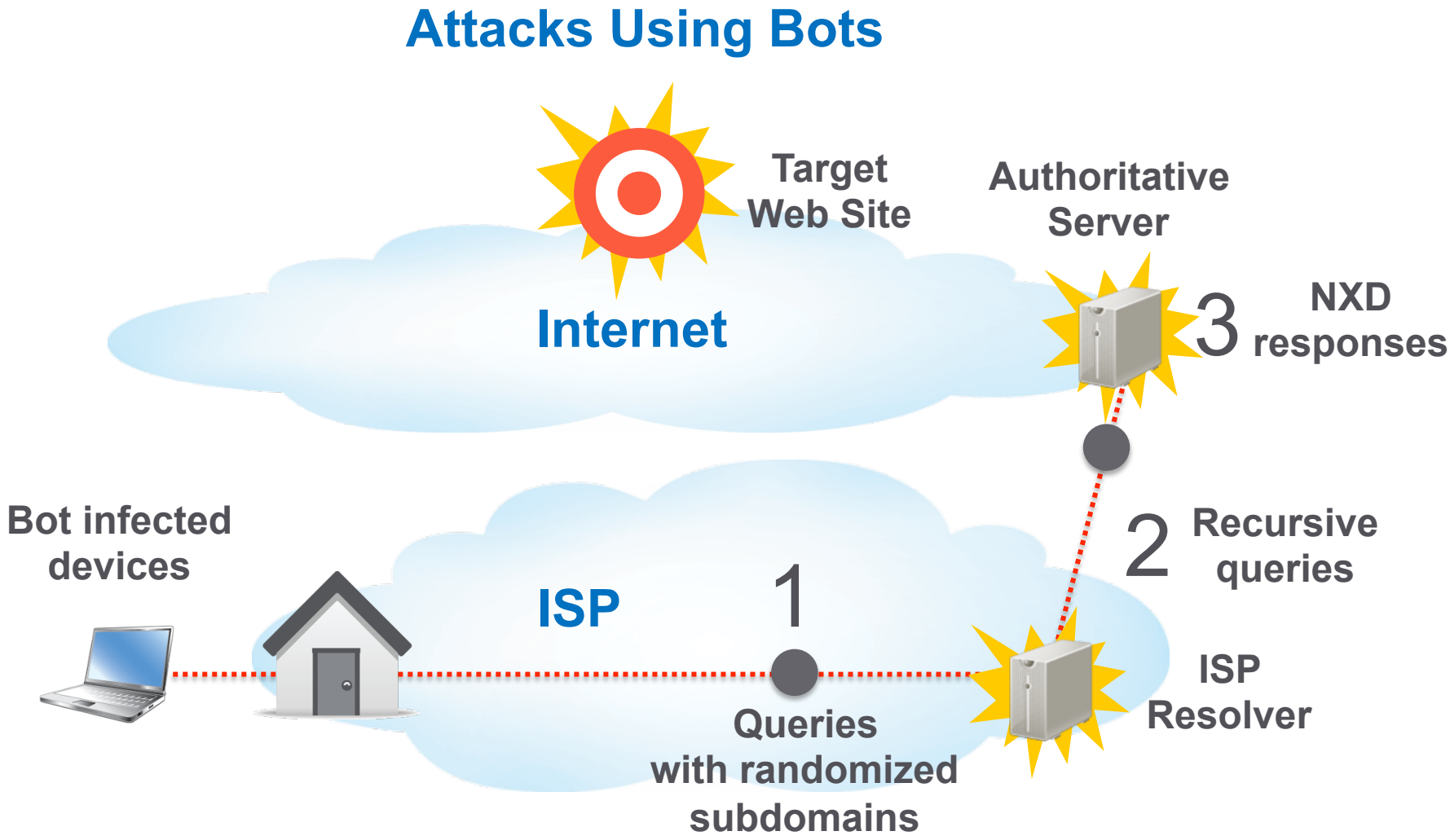
a6ca.cubecraft.net.

Different Patterns = Different Attacks

First Method of Attack



Second Method of Attack



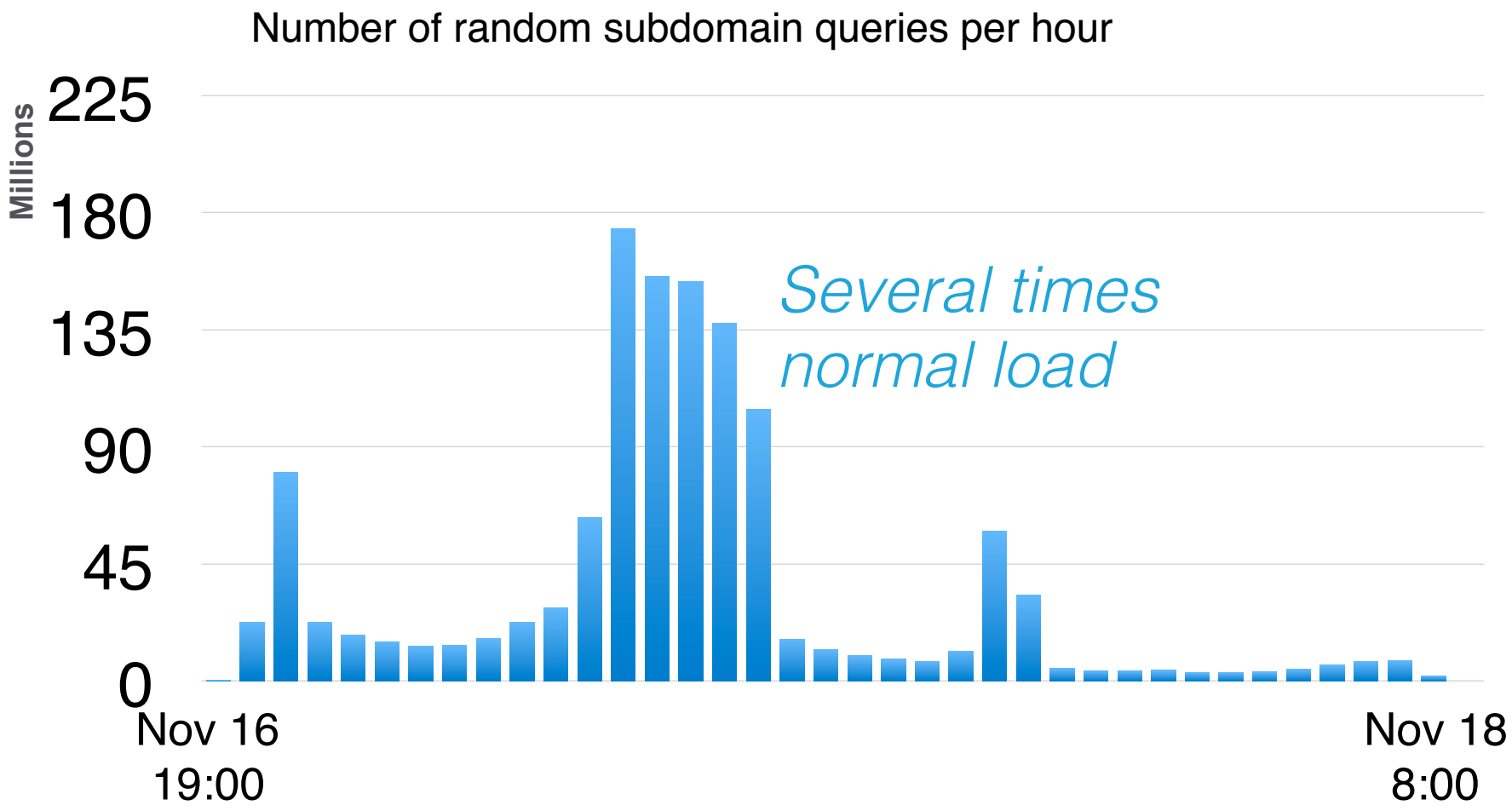
nominum

What's Happening?

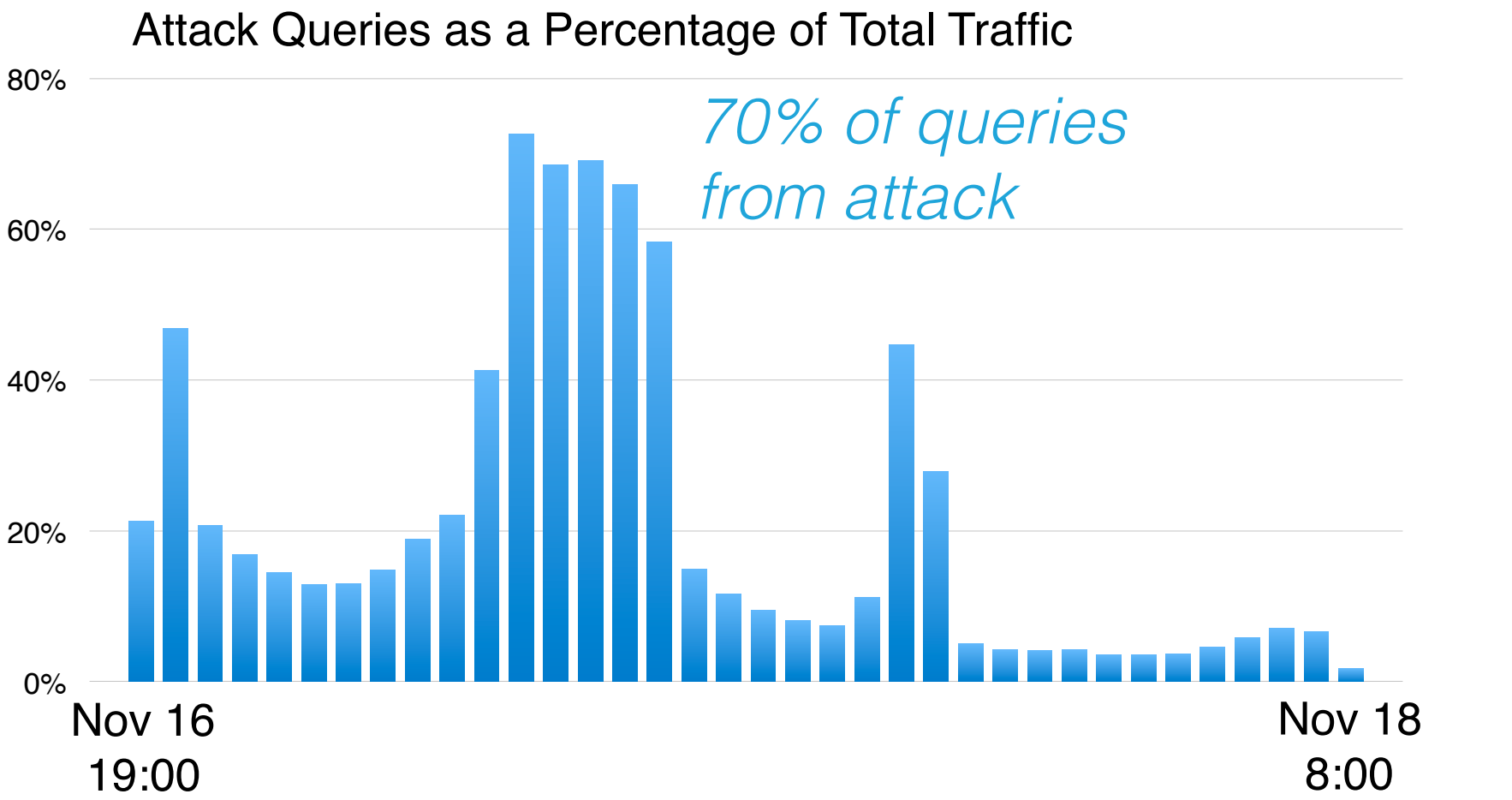
1. *Bots scan networks for home gateways or other vulnerable devices*
2. *Attempt to login with default passwords*
3. *Load malware on gateway*
4. *Malware sends huge volumes of specially crafted DNS queries*
5. *When DNS servers cannot handle requests websites become unreachable*

A single device sourced 1.5M queries in 3 mins (8000 QPS)!

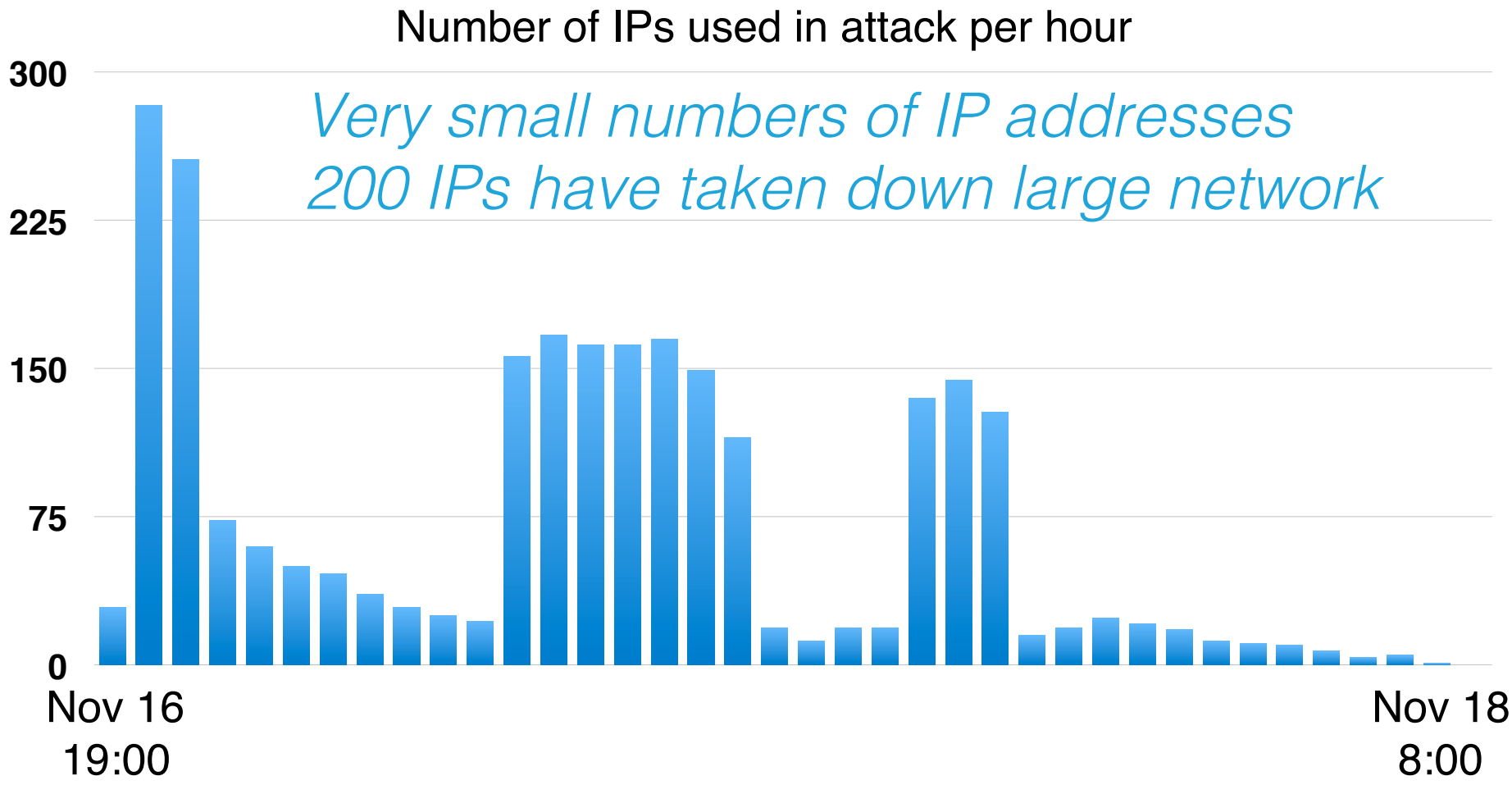
Example Attack: One DNS Server



Example Attack Data



Example Attack Data



Summary

- New generation of DNS Based DDoS
  - Stressing resolvers worldwide
  - Authority failures
  - Resources associated with target names taken offline
- Open Home Gateways remain a major problem
  - Limited options for remediation
- Filter DNS traffic at ingress to resolvers
  - Protect good queries – fine grained filters
  - Drop bad queries – protect authorities and targets