Harness Your Internet Activity

Random Subdomain Attacks

Plaguing the Internet

Introduction

- DNS based DDoS attacks increasing
  - Late 2012 - DNS amplification remerges as a problem
  - January 2014 - new innovation with random subdomain attacks
- Major attack vector - open home gateways
- Severe stress on DNS worldwide
  - ISP resolvers – spikes of recursive requests
  - Authoritative servers – overwhelmed with NXD responses
  - Use of Response Rate Limiting in authorities is causing even more stress

Random Subdomain Attacks

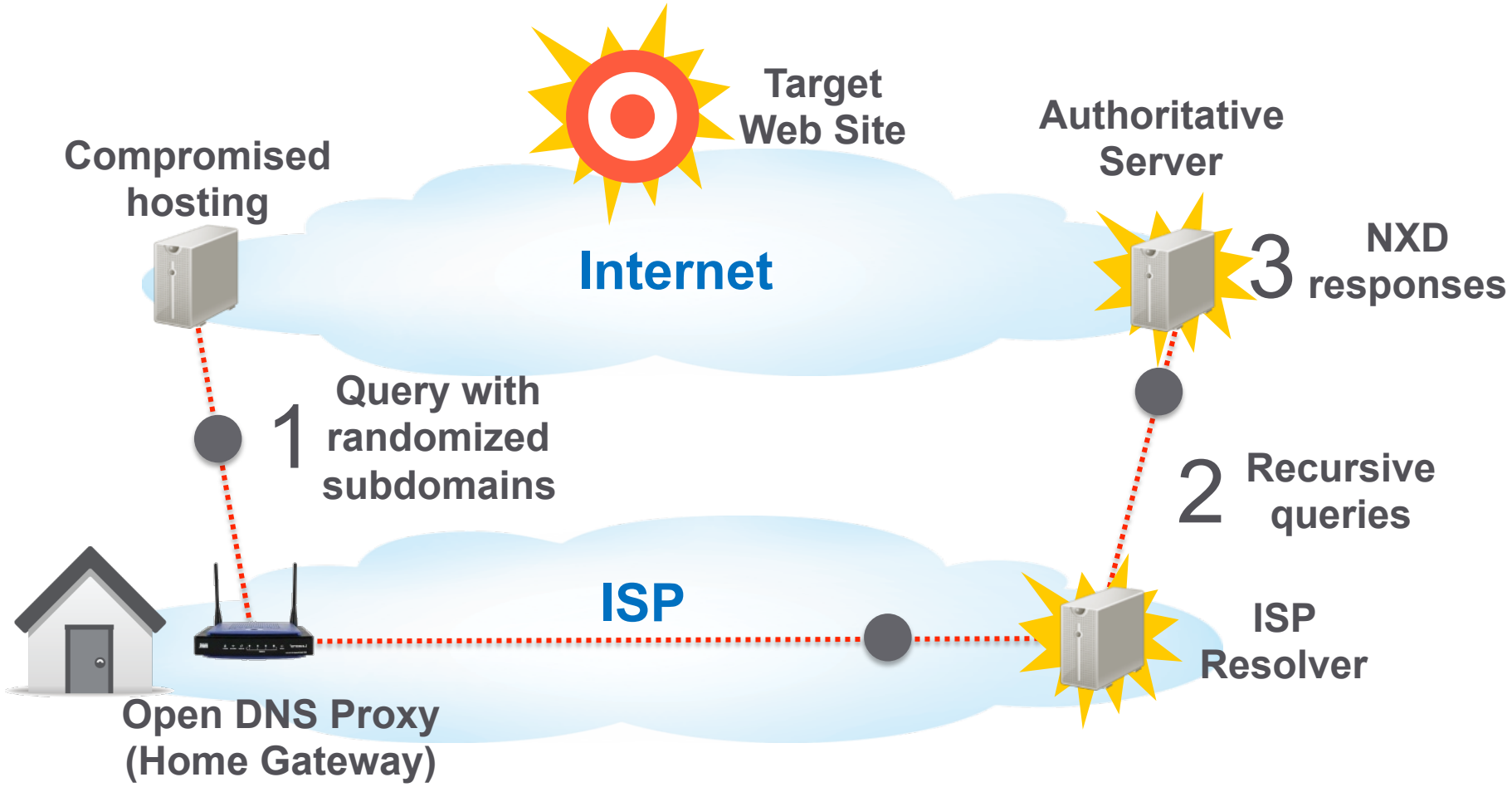
RANDOM **TARGET NAME**

wxctkzubkb. liebiao.800fy.com

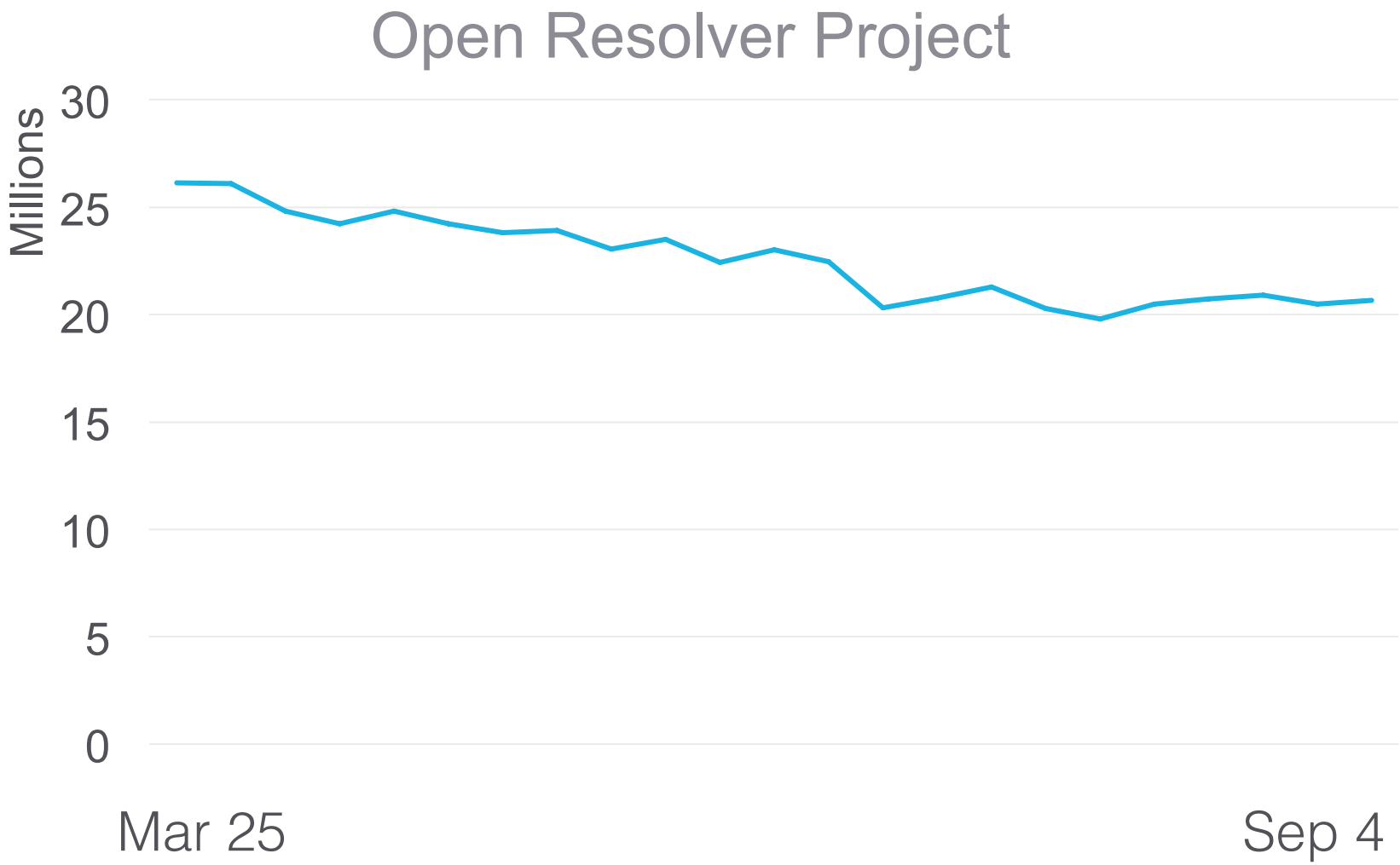
- Queries with random subdomains
  - Answer with “non-existent domain” (NXD)
- Creates lots of work for resolvers
  - Queries require recursion
- Creates lots of works for authoritative servers
  - Heavy volumes of NXD queries often cause failure

Random Subdomain Attacks

Open DNS Proxies are the Vector for Attacks



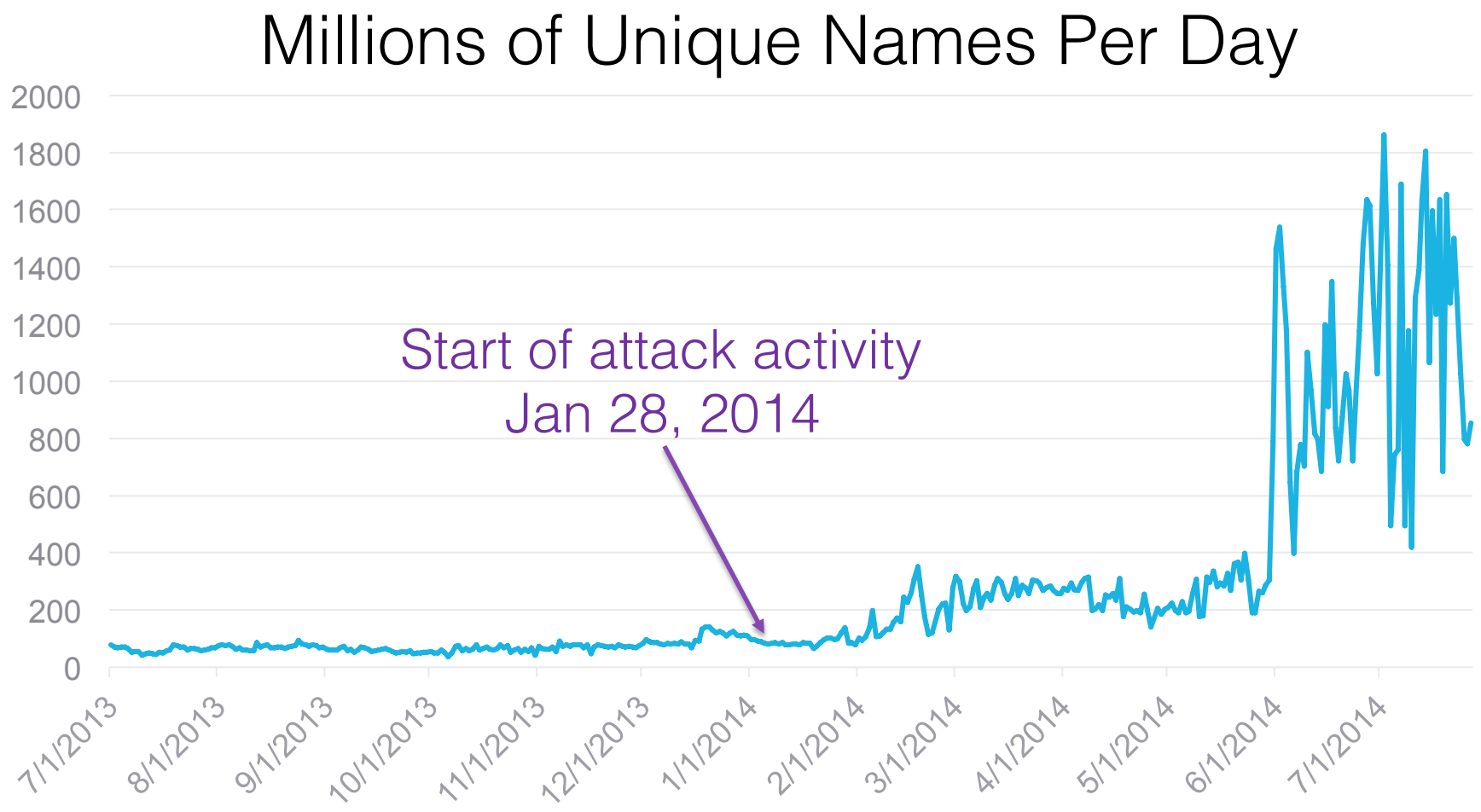
Open Resolvers Are Declining



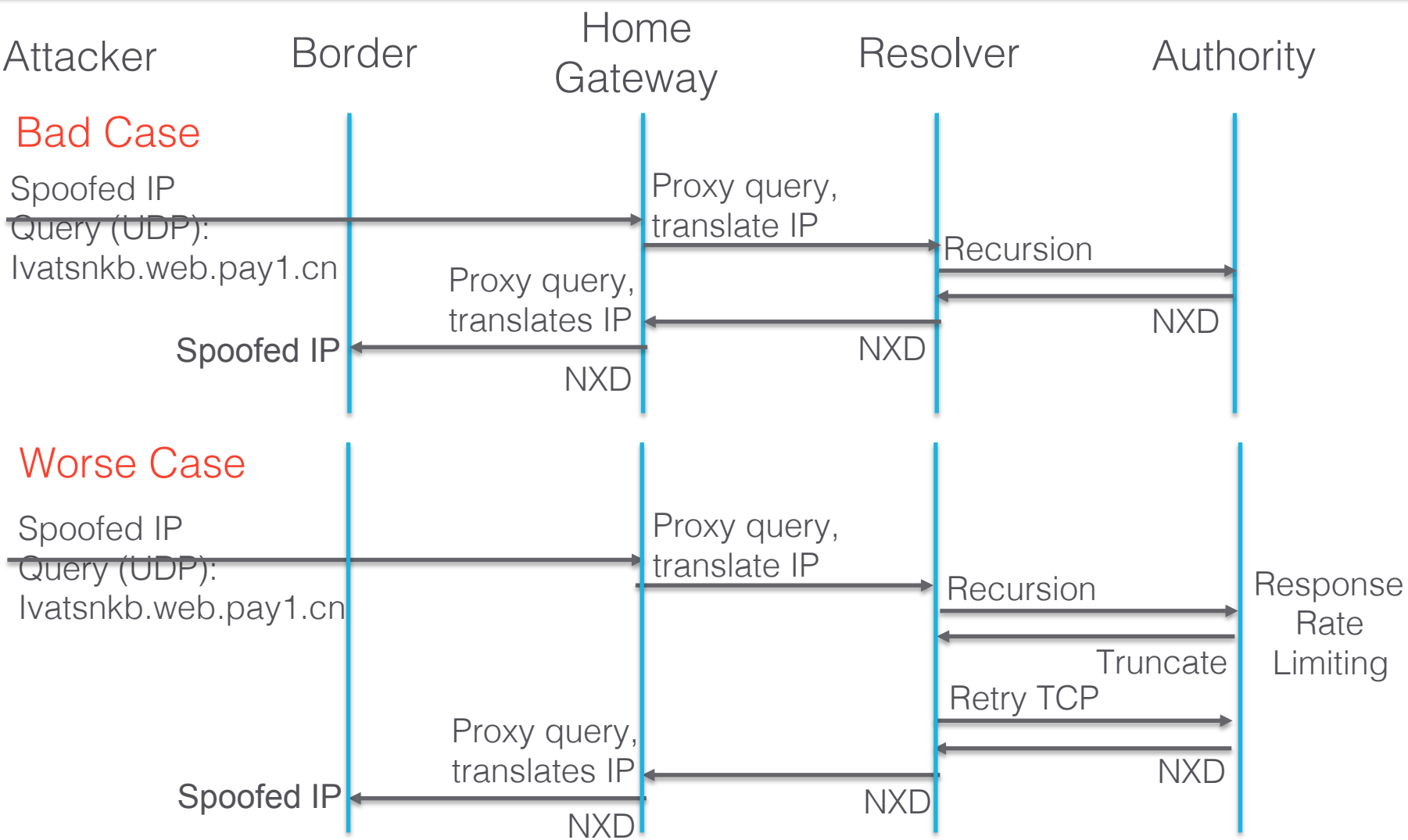
Open Resolvers By Country (Sep 4 2014)

AU	93835	GR	109503
BE	22093	HN	2264
DE	97558	IE	12450
DK	10572	IT	180377
ES	119116	LI	361
FR	113499	NL	76644
GB	194285	PT	20485

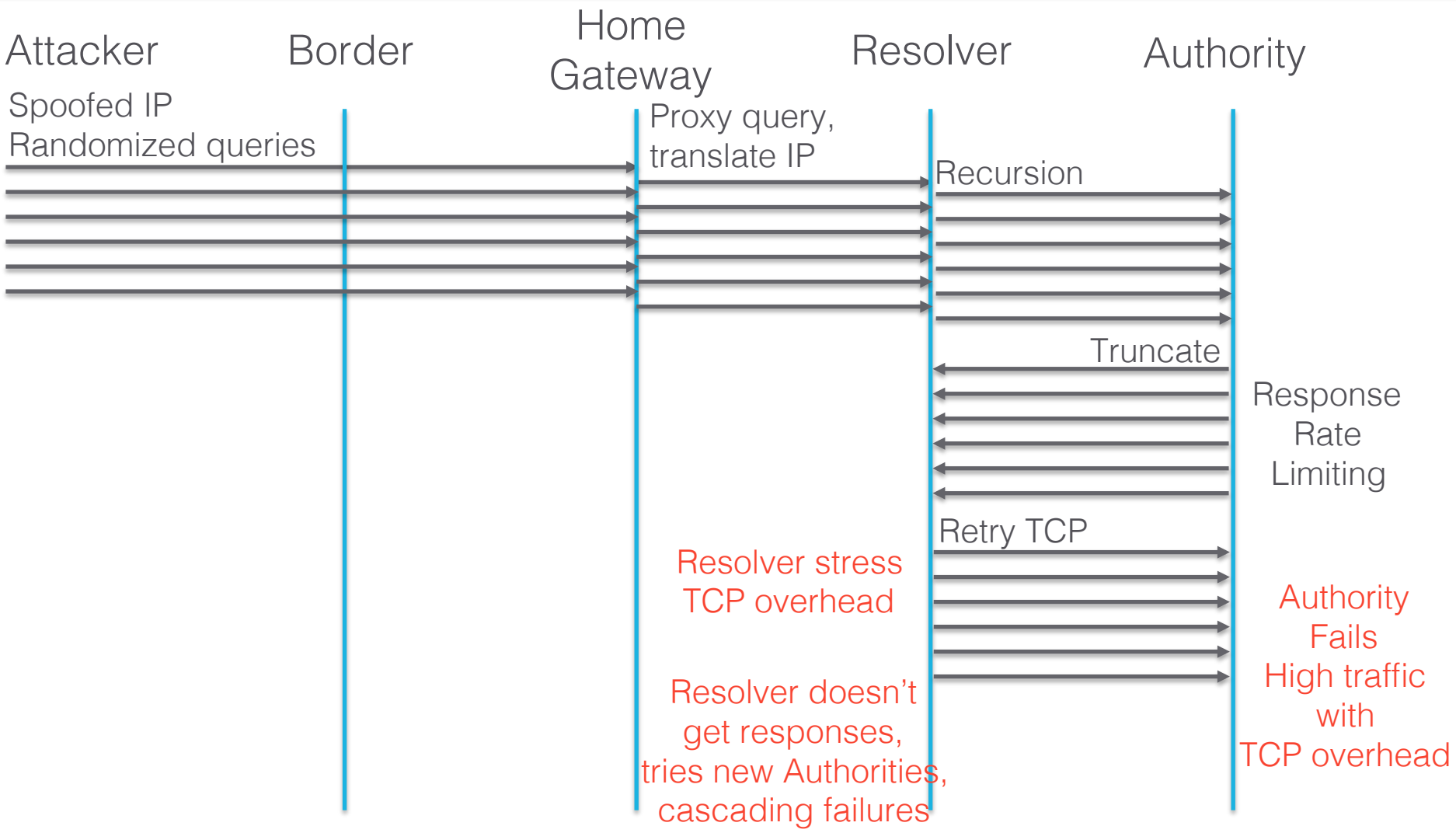
But Attack Traffic Went Up



Random Subdomain Attacks



Why These Attacks Hurt



Popular Names are Attacked

About 9% of names attacked are popular

Alexa 1000 Names

Name	Rank
baidu.com	5
blog.sina.com.cn	14
xlscq.blog.163.com	33
www.bet365.com	177
www.lady8844.com	379
cloudfront.net.	413
www.appledaily.com.tw	647

Other names you might recognize

Cloudflare

Akamai CDNs

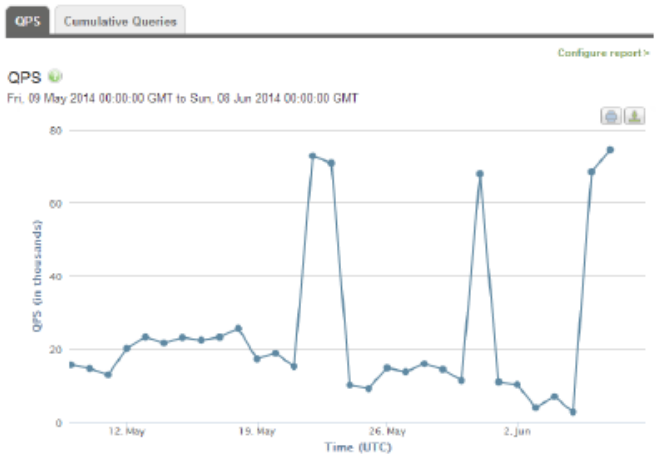
Attacks on popular names have to be handled carefully – Precision Policies, Whitelists

Example Attack Queries

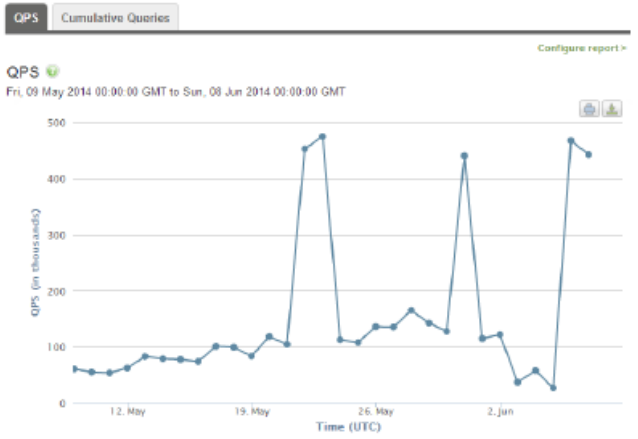
Hundreds of millions of randomized subdomains	~ 1,000 target names used thus far
krsfwzohwdghqx.	www.appledaily.com.tw.
wxctkzubkb.	liebiao.800fy.com.
avytafkjad.	www.23us.com.
gfqhuxenun.	wuyangairsoft.com.
uv.	vip.mia0pay.net.
lvatsnkb.	web.pay1.cn.
wfmlgzyrufaxid.	www.zhaobjl.com.
qzgziliv.	978sf1111.ewc668.com.
qxgtqfyv.	www.500sf.com.

Attacks Coordinated Worldwide

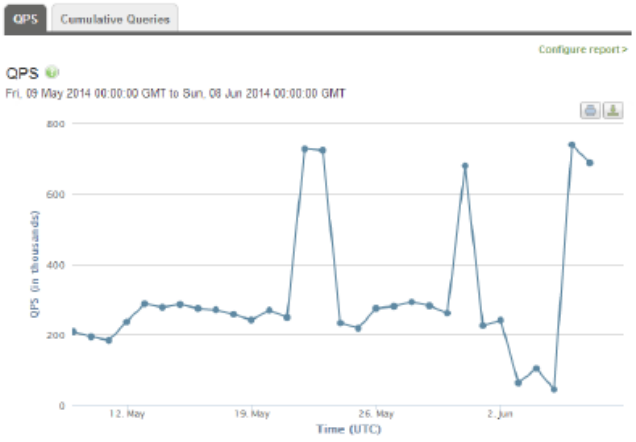
Large ISP EMEA



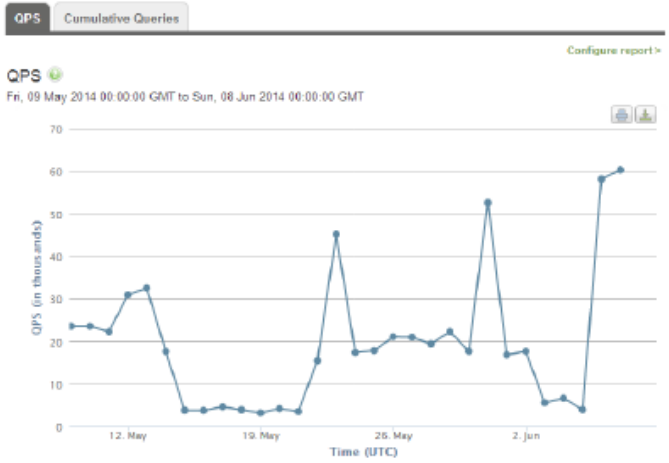
Large ISP LATAM



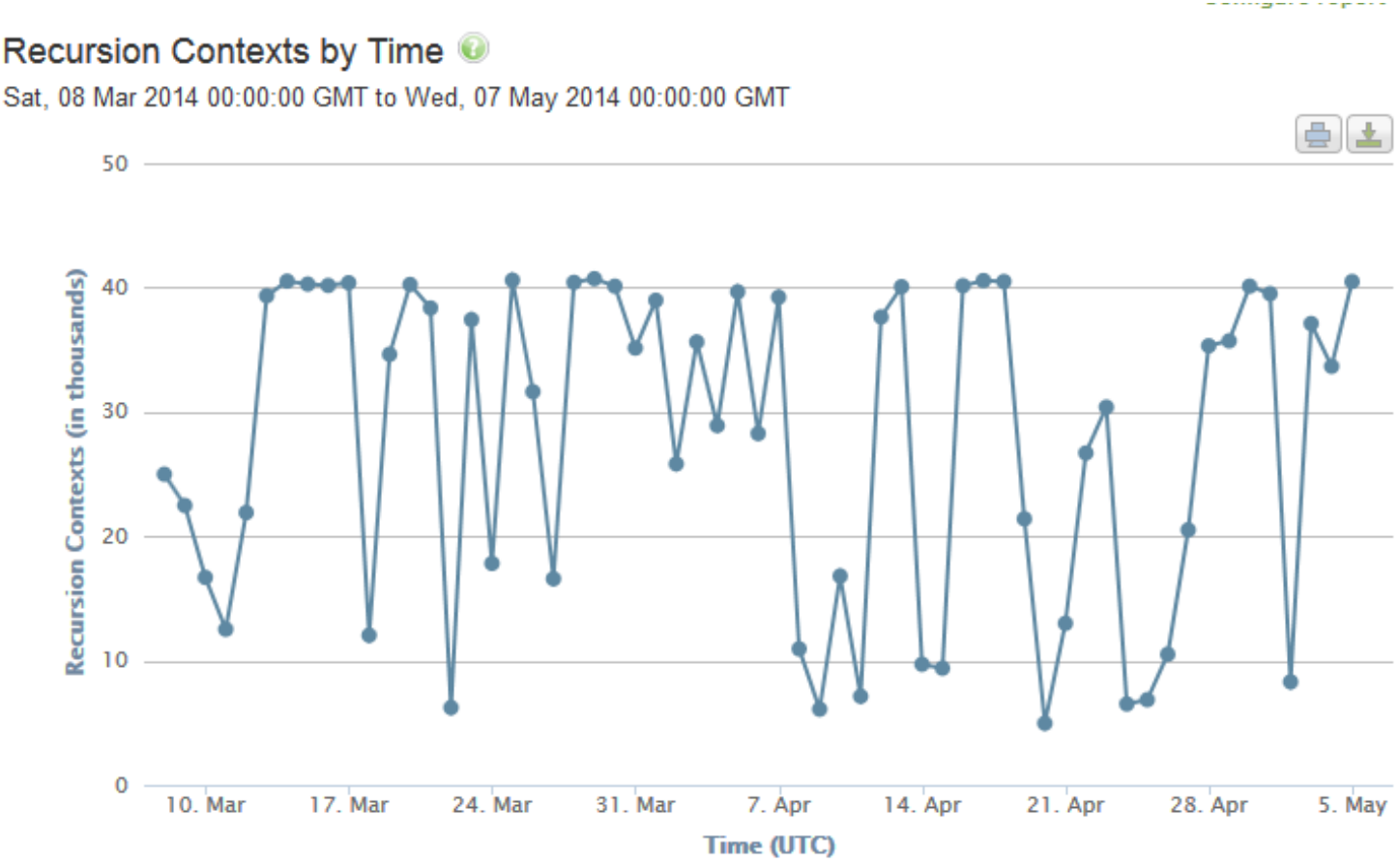
Large ISP North America



Large ISP APAC

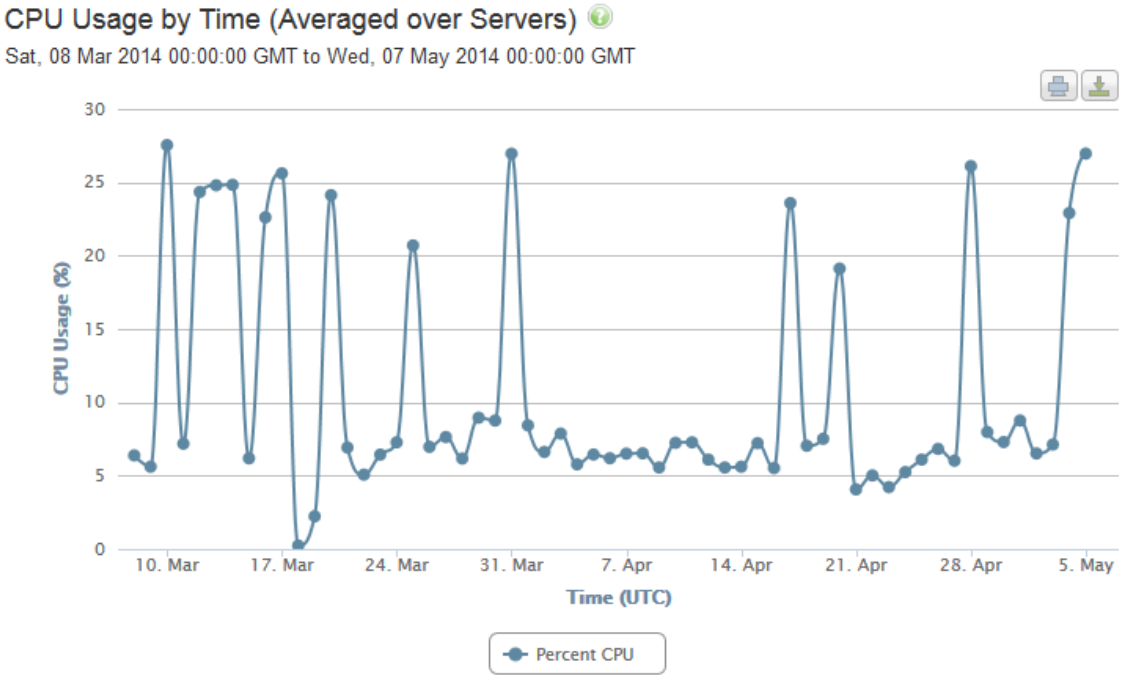


Resolver Impact



Resolver Impact

CPU spikes during attacks are caused by more expensive recursion



Removing useless random subdomain queries reduces processor load

Many Problems

- Home Gateways mask spoofed source IP
  - "Challenges", "DNS cookies" won't work
  - Blacklisting eliminates all queries from legitimate IPs
- RRL by authorities increases work for resolvers & authorities
  - It was designed for attacks directly on authoritative servers
  - Rate limiting resolvers is counter productive – "death spiral"
- Surrounding recursion with too much logic can be problematic
  - It does not address root cause – too much useless traffic
  - Collateral damage is observed:
    - Servers marked as non-responsive by recursor recovering but still not being used
    - Nameservers serving multiple domains taken out of service by traffic for one domain
- Tendency for cascading failures
  - Authorities successively fail, increasing stress on remaining authorities
  - This in turn increases stress on resolvers

Solution

- Filter traffic at ingress to the resolver
  - Near real time block lists
    - Randomized subdomains used for attacks
    - Purpose built DNS amplification domains
- Protect good traffic
  - Whitelist
- Fine grained policy
  - Tie the lists together:
    Block bad traffic
    Answer good traffic
  - Selectively filter other attack traffic on an ad hoc basis