nominum™

Harness Your Internet Activity

Random Subdomain Attacks

Plaguing the Internet

Agenda

- Brief Intro
  - Covered at last OARC
  - Attack overview
- Latest data
  - Progress on open dns proxies in home gateways
  - Impact of Response Rate Limiting?
  - Chinese pornography sites
  - Hong Kong news site
- Testing resolvers
  - (Over) ambitious idea!
- What can we do?
  - Success filtering ingress traffic, some challenges
  - ???

Random Subdomain Attacks

RANDOM **TARGET NAME**

wxctkzubkb. liebiao.800fy.com

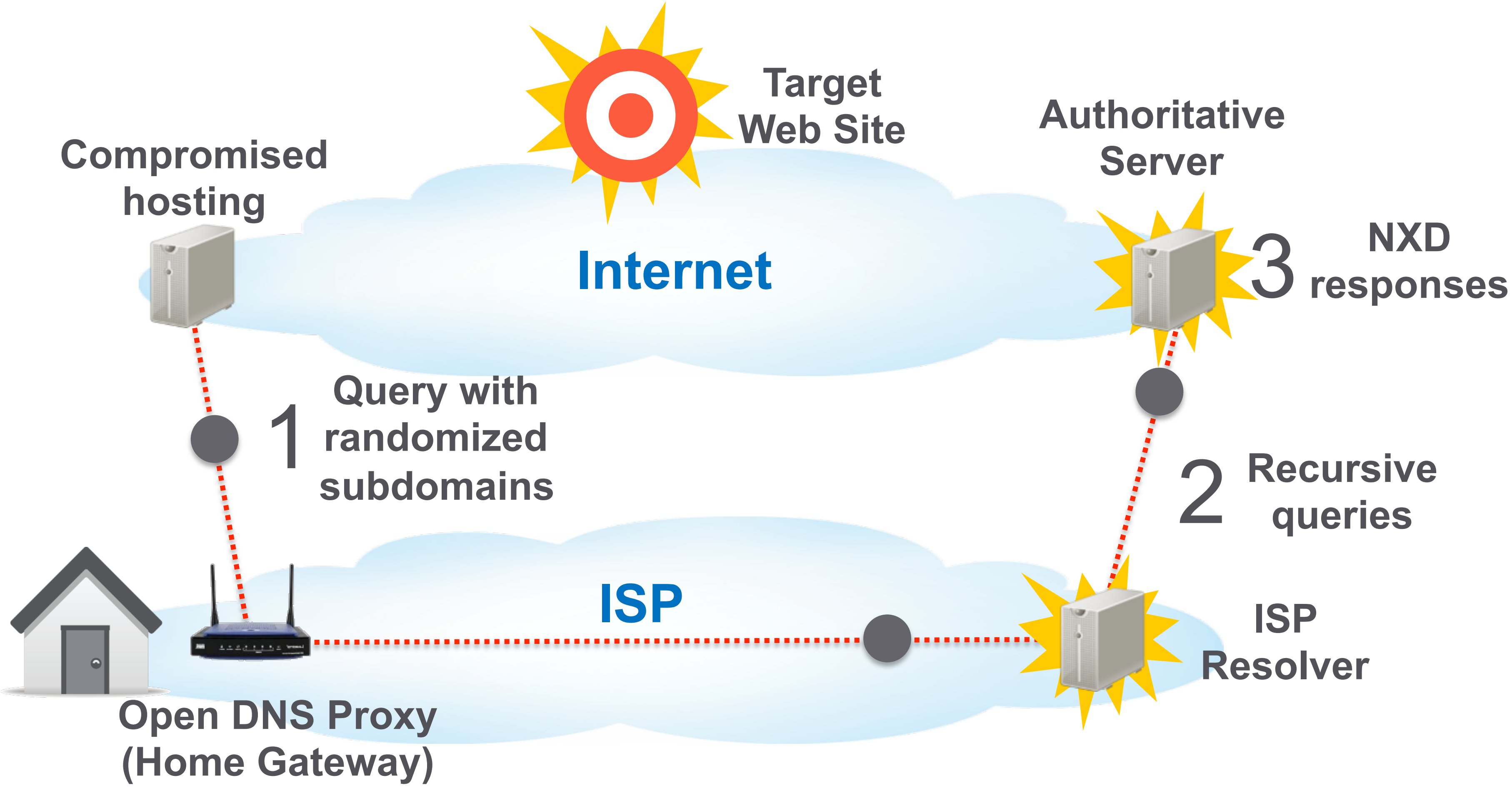
three labels

qzgziliv. 11hehe.com

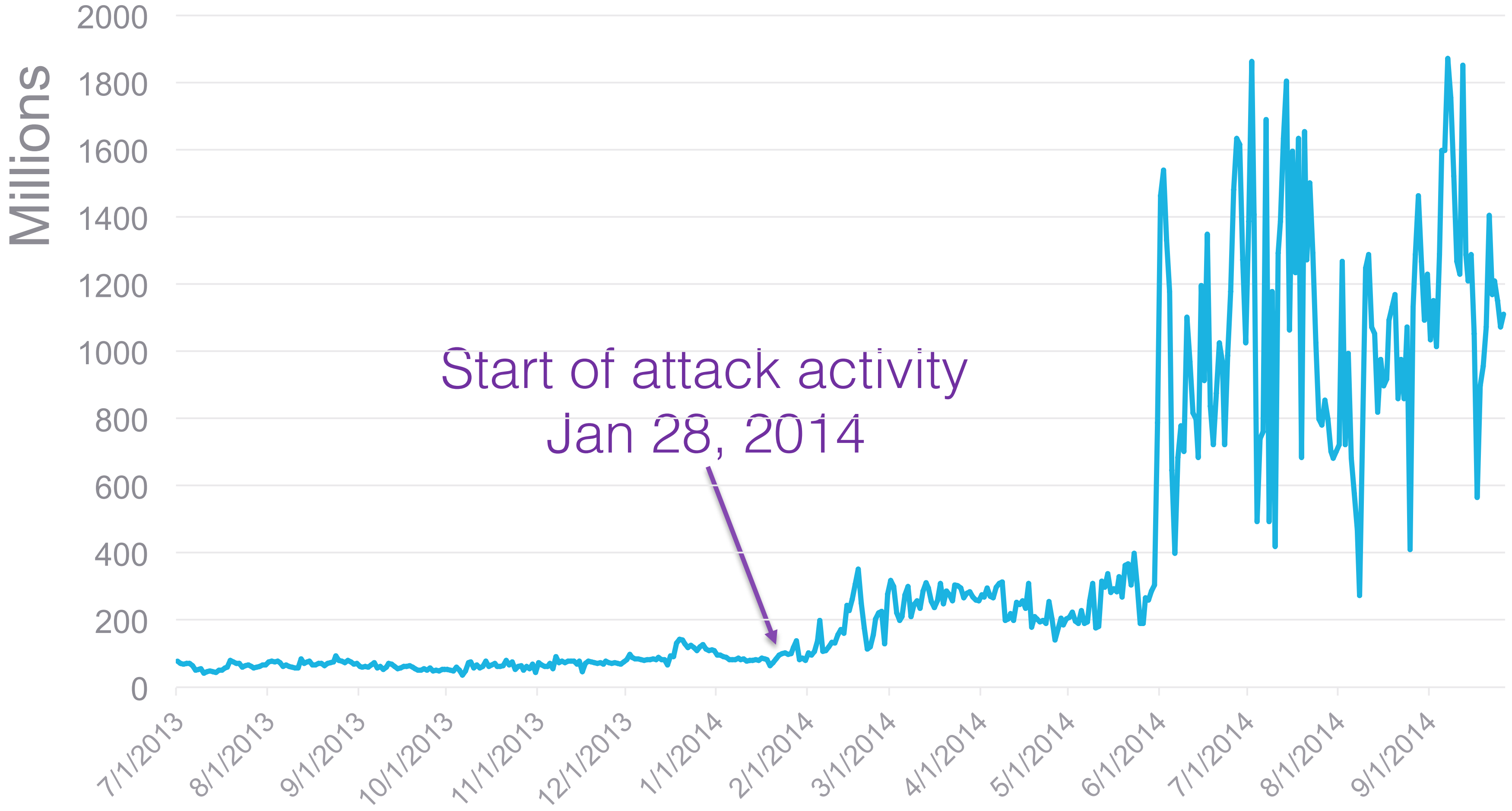
two labels

Random Subdomain Attacks

Open DNS Proxies are the Vector for Attacks

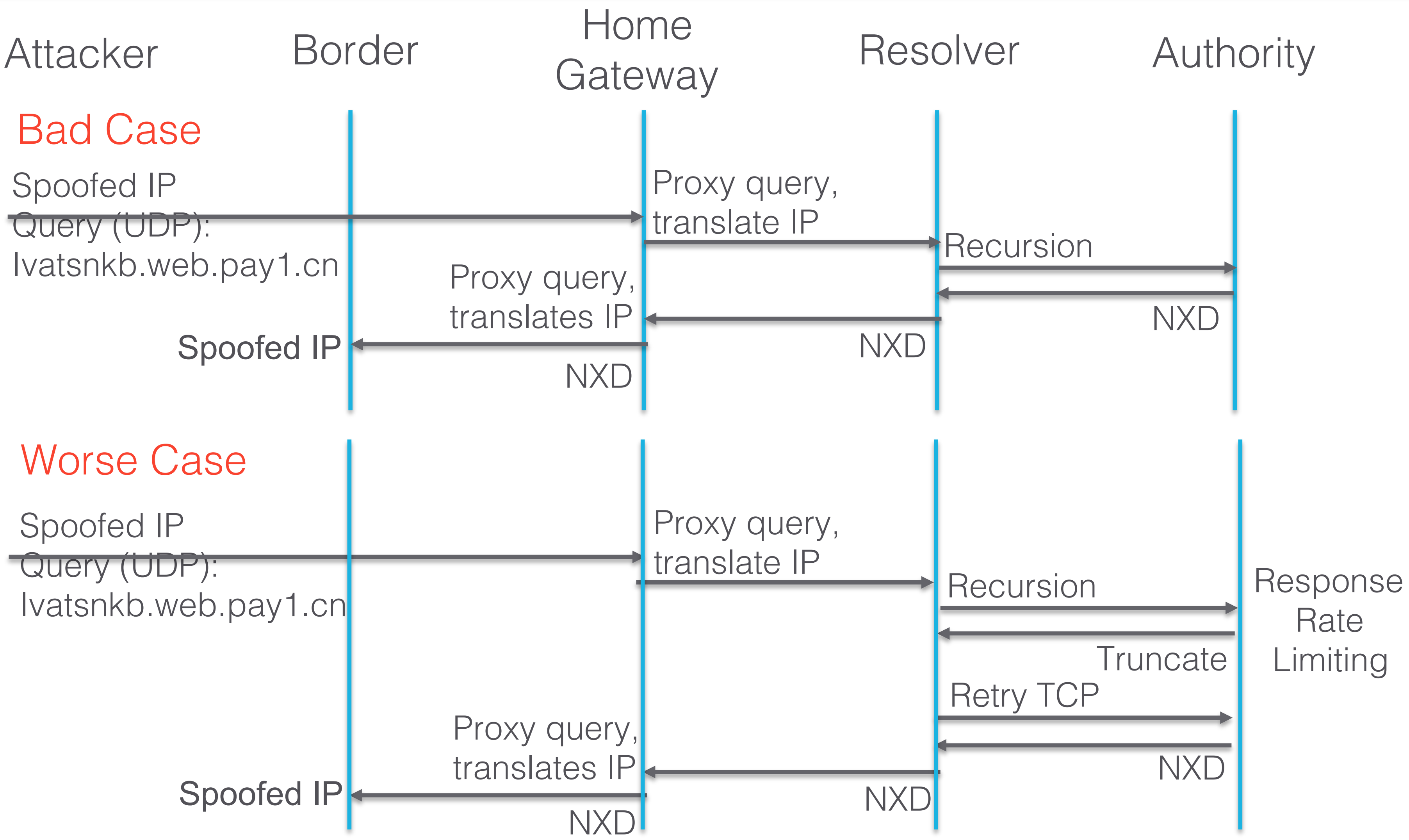


Latest Data: Unique Names



Start of attack activity
Jan 28, 2014

Impact of Response Rate Limiting



Attacker

Border

Home Gateway

Resolver

Authority

Bad Case

Spoofed IP Query (UDP): lvatsnkb.web.pay1.cn

Proxy query, translate IP

Recursion

NXD

NXD

Proxy query, translates IP

Spoofed IP

NXD

Worse Case

Spoofed IP Query (UDP): lvatsnkb.web.pay1.cn

Proxy query, translate IP

Recursion

Response Rate Limiting

Truncate

Retry TCP

NXD

Proxy query, translates IP

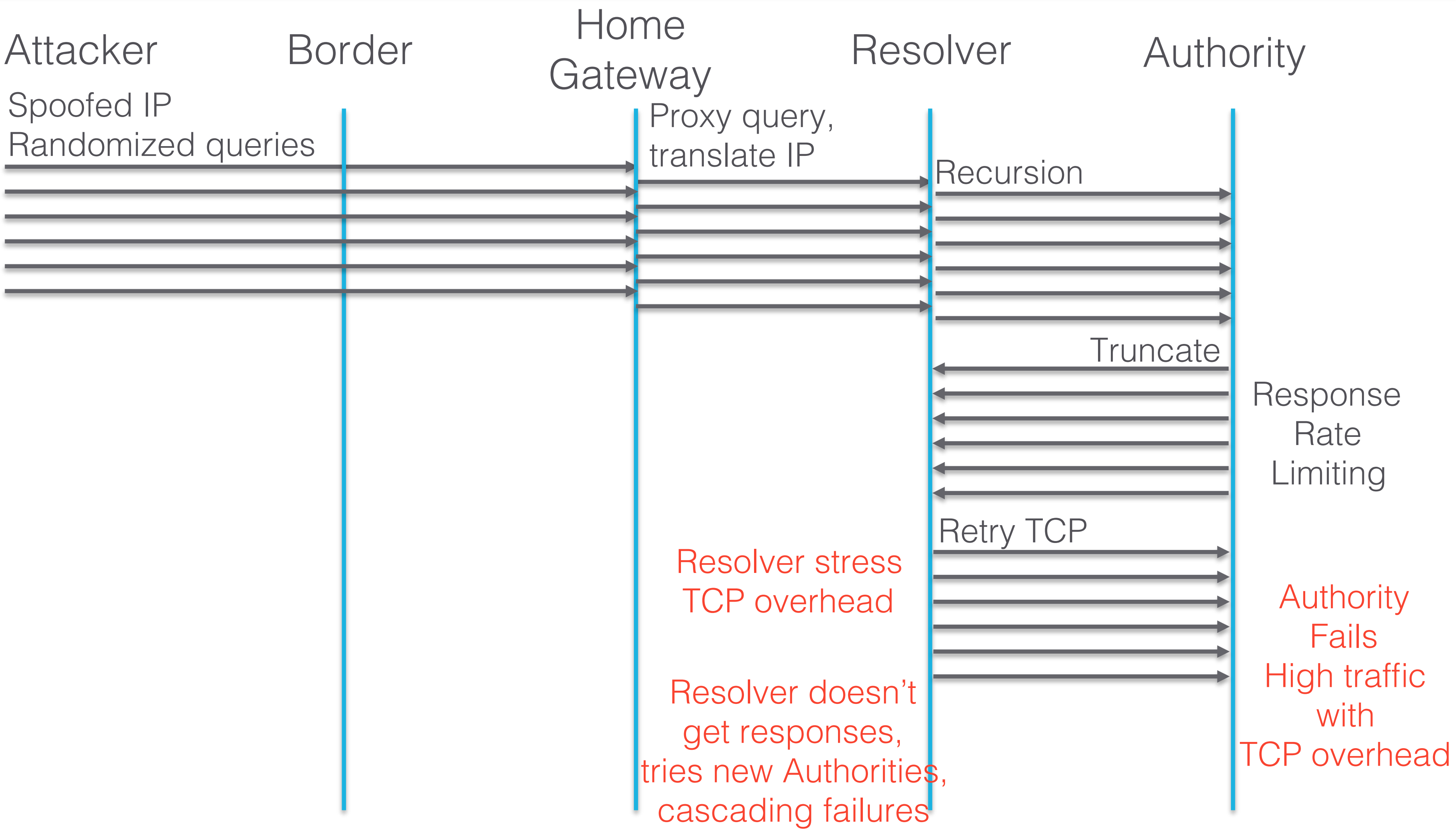
NXD

Spoofed IP

NXD

nominum

Attacks at Scale



Resolver stress
TCP overhead

Resolver doesn't
get responses,
tries new Authorities,
cascading failures

Authority
Fails
High traffic
with
TCP overhead

Hong Kong News Site

- Sept 28, 2014 UTC
- Height of Hong Kong democracy protests
- Distinct shift in tactics – 98% of attacks on one domain
  - Typical day 4-6 domains attacked, usually gaming sites
- Hong Kong online news Passion Times
- Website offline 13 hours

Chinese Pornography Sites

- Sept 25/26 2014 (UTC)
- Another shift in tactics 42 domains attacked simultaneously
- Attack lasted 6 hours
- Most web sites went down

- Motive for most attacks remains unclear
  - Monetization is likely very modest
  - Collateral damage across the Internet far exceeds revenue from DDoS for hire

Sept 25/26 Attacks

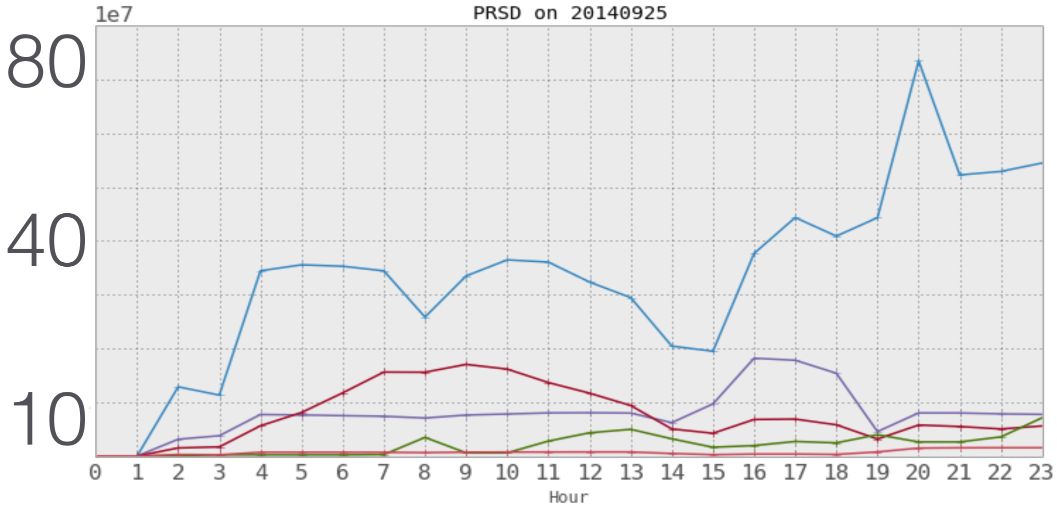
Data from 5 providers

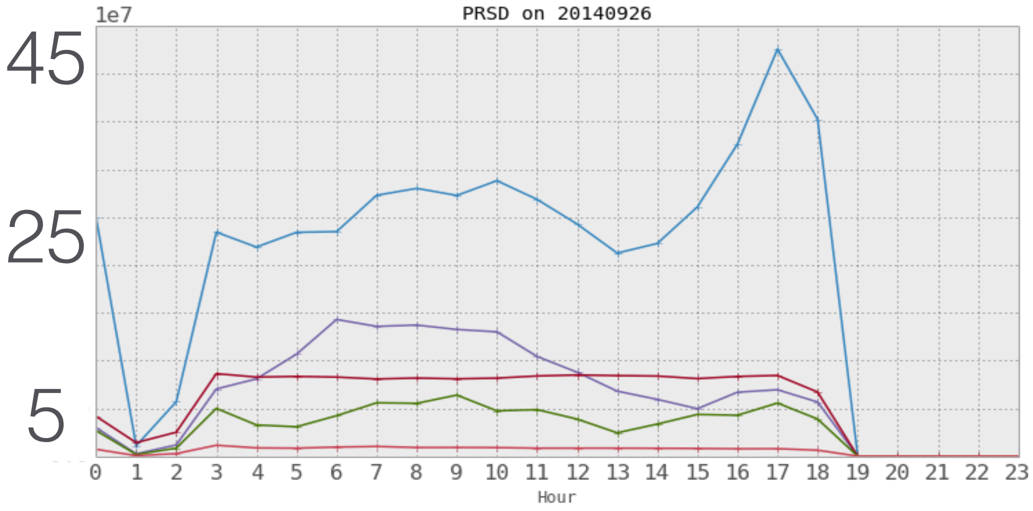
Volume of attack queries

In Millions

Small fraction of overall attack activity

Nominum est << 5%

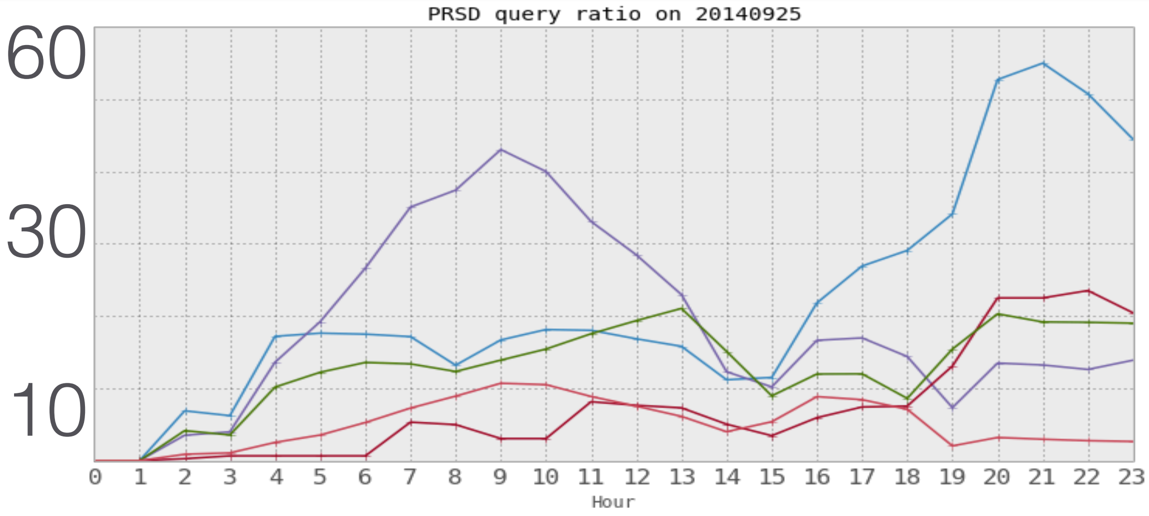


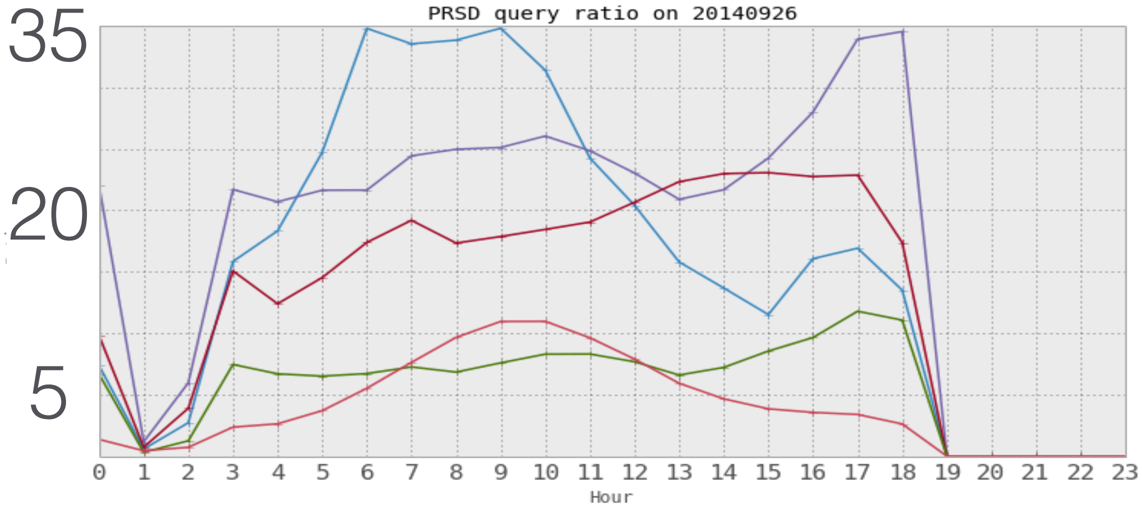


Sept 25/26 Attacks

Data from 5 providers

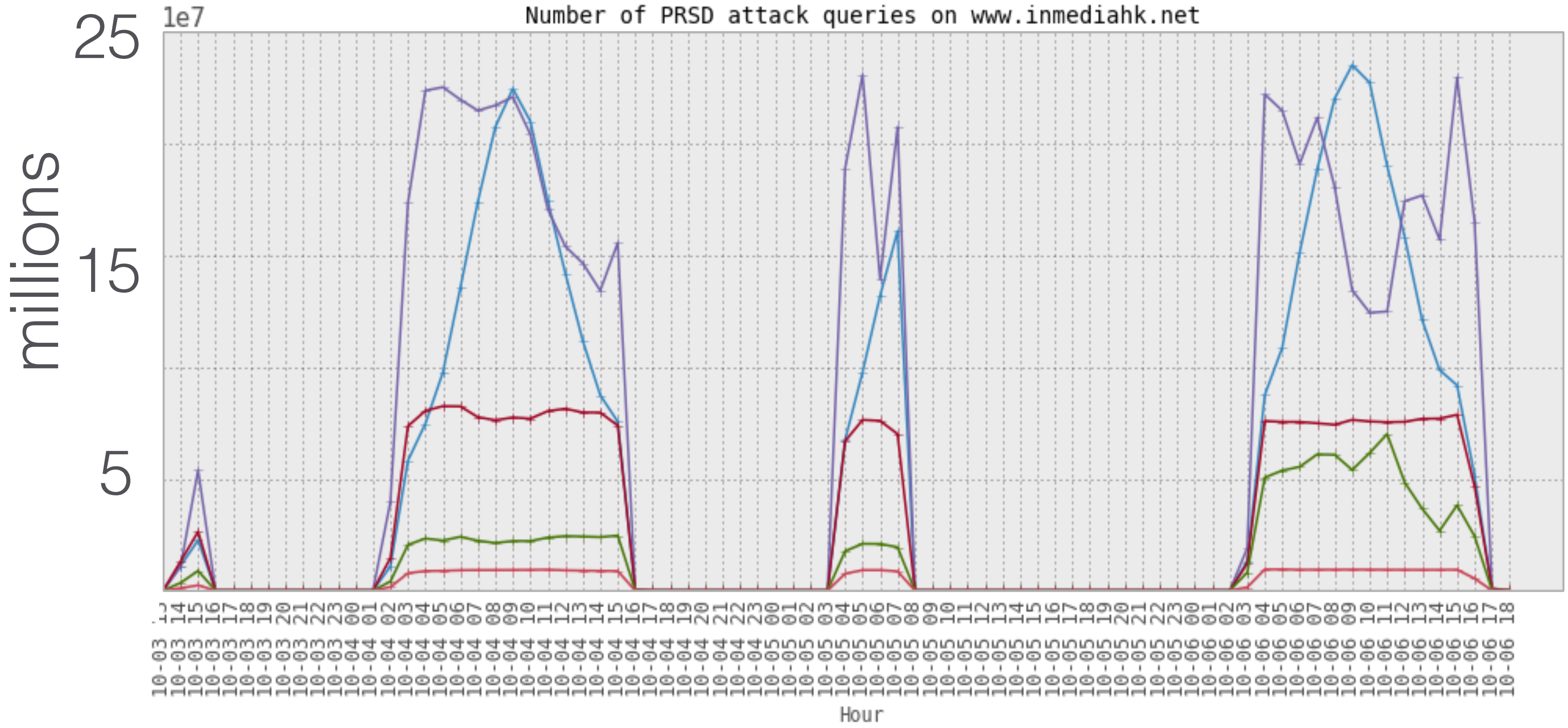
% attack queries





Oct 3- 6 Attacks

In-media is an Independent Hong Kong news site



Many Problems to Address

- Home Gateways mask the spoofed source IP
  - “Challenges”, “DNS cookies” won’t work at either resolvers OR authorities
  - Queries are from legitimate IPs – blacklisting eliminates all traffic for those IPs
- Response Rate Limiting by authorities increases the workload for *both* resolvers and authorities
  - It was designed for attacks directly on authoritative servers
  - Rate limiting resolvers is counter productive
- Surrounding recursion with too much logic can be problematic
  - D*oesn’t* address root cause
  - 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

Solutions

- Filter traffic at ingress to the resolver
  - Near real time block lists
    - Randomized subdomains used for attacks
- Protect good traffic
  - Whitelist
- Fine grained policy
  - Tie the lists together:
    Block bad traffic
    Answer good traffic

IDEAS?

Testing Resolvers

- Goal: Understand impact of PRSD on resolvers
  - BIND
  - PowerDNS
  - Undound
  - Vantio
- Method: Simulate DNS E-E behavior

– Attack behavior	Easy
– Resolvers	Easy
– Authorities	Hard
– Variability of Internet	Very hard

- Whoops!

Current Test Plan

- Authoritative server answers up to threshold, then randomly drops
- Authoritative server switches to TCP at threshold, then restricts tcp connection slots
- Authoritative server drops traffic for attack domains, answers other domains
- Authoritative server doesn't answer, other servers for domain successively fail, vary latency response latency

IDEAS?