Vulnerable Internet “Things” Fuel DNS-based DDoS

HKNOG Sept 2015

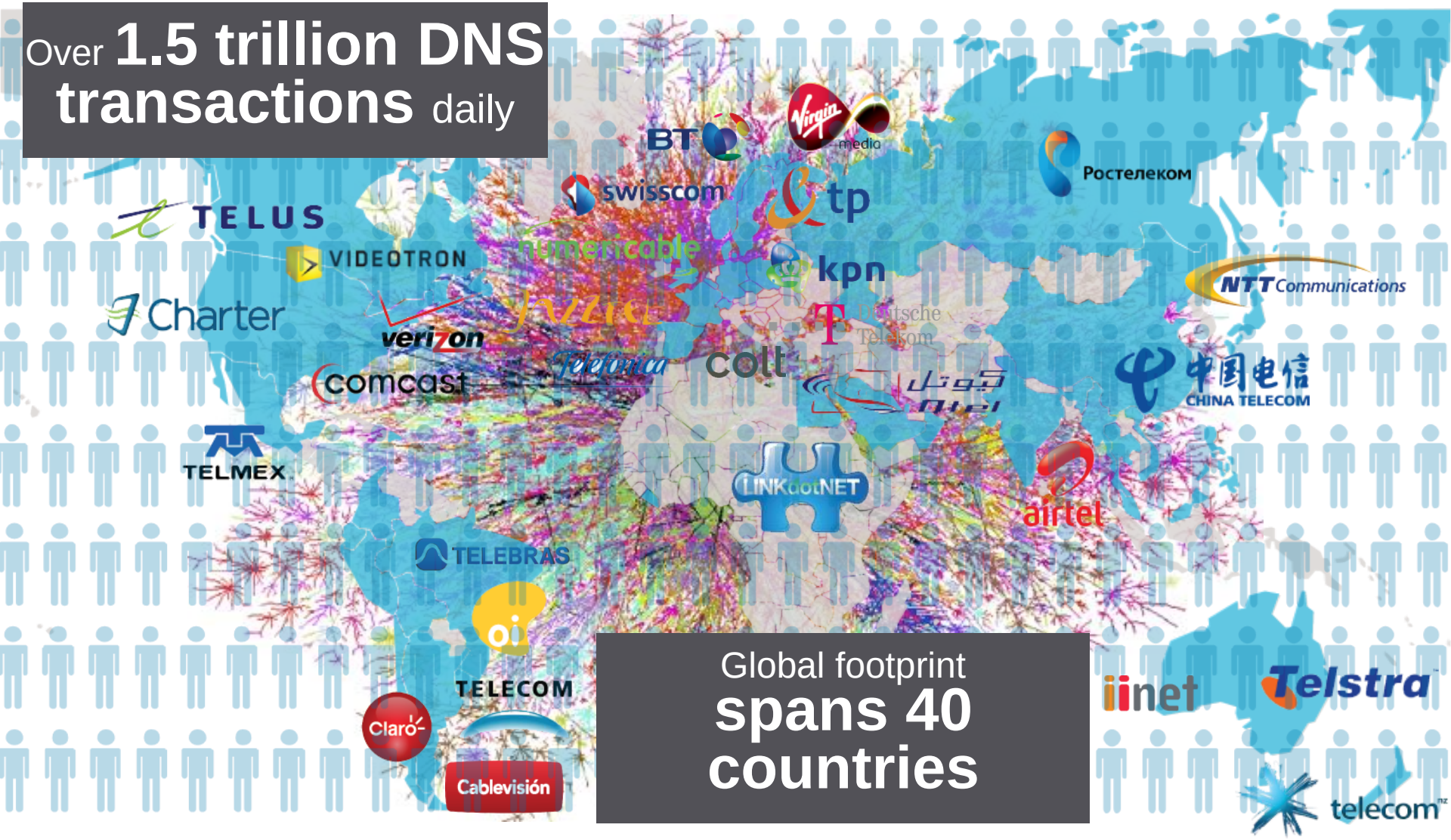
Bruce Van Nice

Agenda

- Introducing Nominum
- Why DNS Security Matters
- DNS Data Science
- Better DNS Security

Trusted Partner to the Globe's Leading Service Providers

Over **1.5 trillion DNS transactions** daily



Global footprint **spans 40 countries**

Why DNS Security Matters

DNS Security Exposure

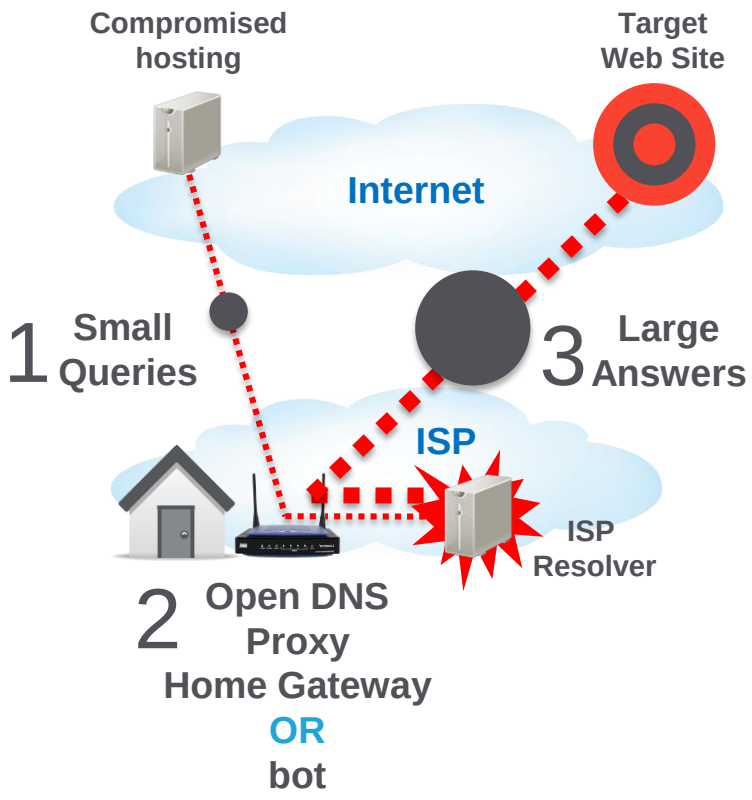
- DNS-based DDoS attacks increasing
  - DNS Amplification
  - Random subdomain attacks – focus of this presentation
- Attack vectors
  - Open home gateways
  - NEW - Bot malware
- Stress on DNS worldwide
- Other DNS and network exposure
  - Bots
  - Cache poisoning

Why DNS Security Matters

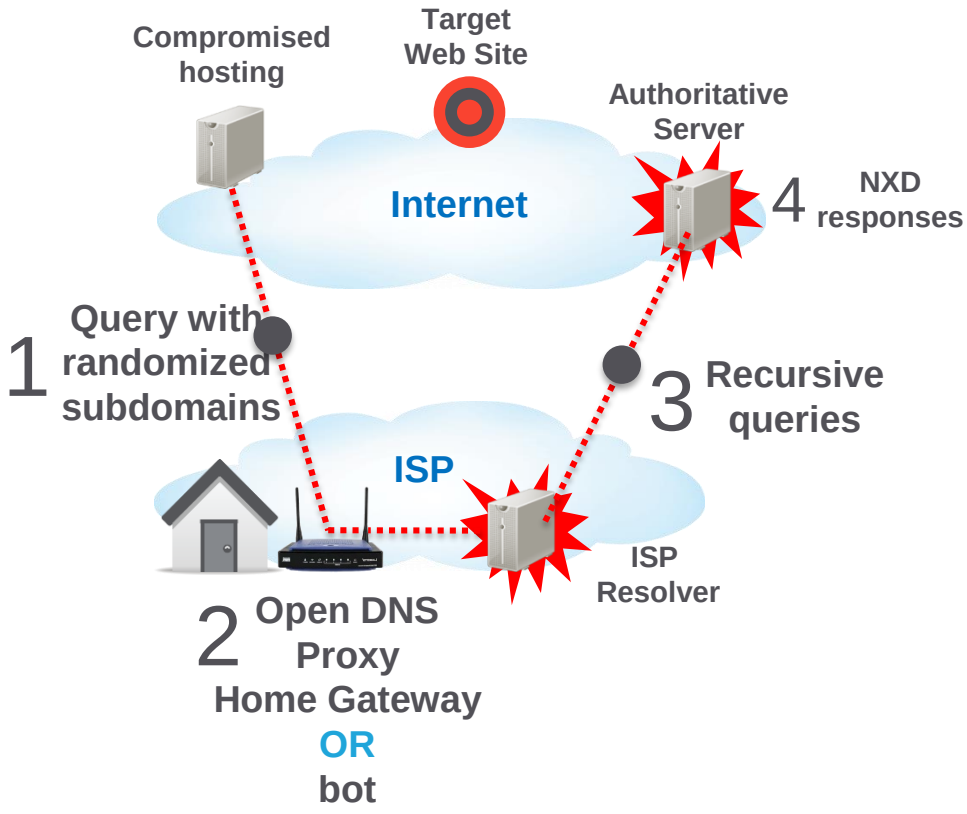
- Customer satisfaction
  - DNS availability and a safe experience promote customer satisfaction
- Operational efficiency
  - Clean networks perform reliably and predictably – no fire drills
- Economics
  - Incremental savings - infrastructure, bandwidth, support
- Network Integrity
  - Confidence infrastructure isn't, or can’t easily be compromised
- Peer reputation
  - Contractual obligations, negotiating leverage, industry stature

DNS DDoS: Two Kinds of Attacks

DNS Amplification Attacks

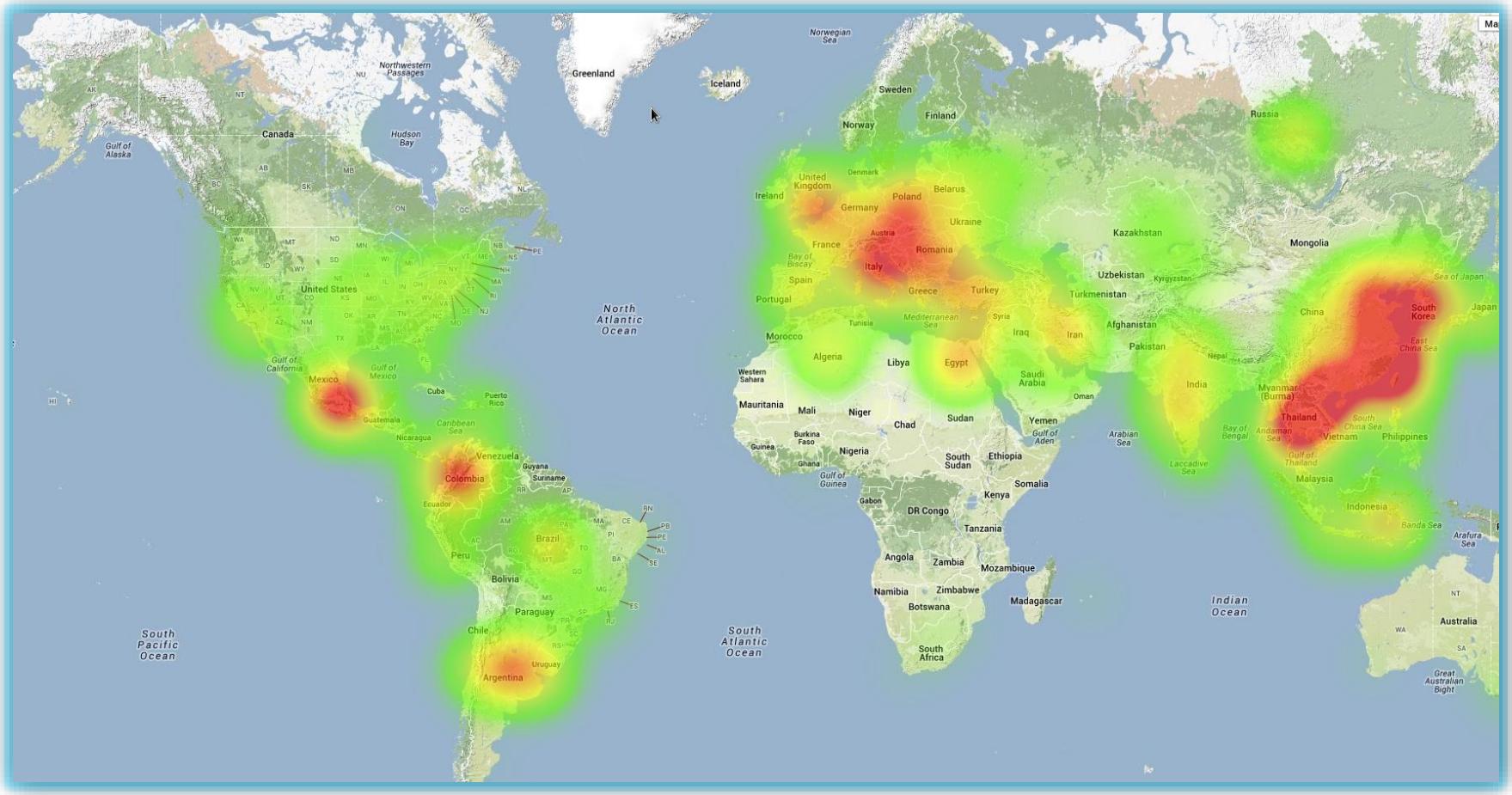


Random Subdomain Attacks



Two vectors: open home gateways or bots

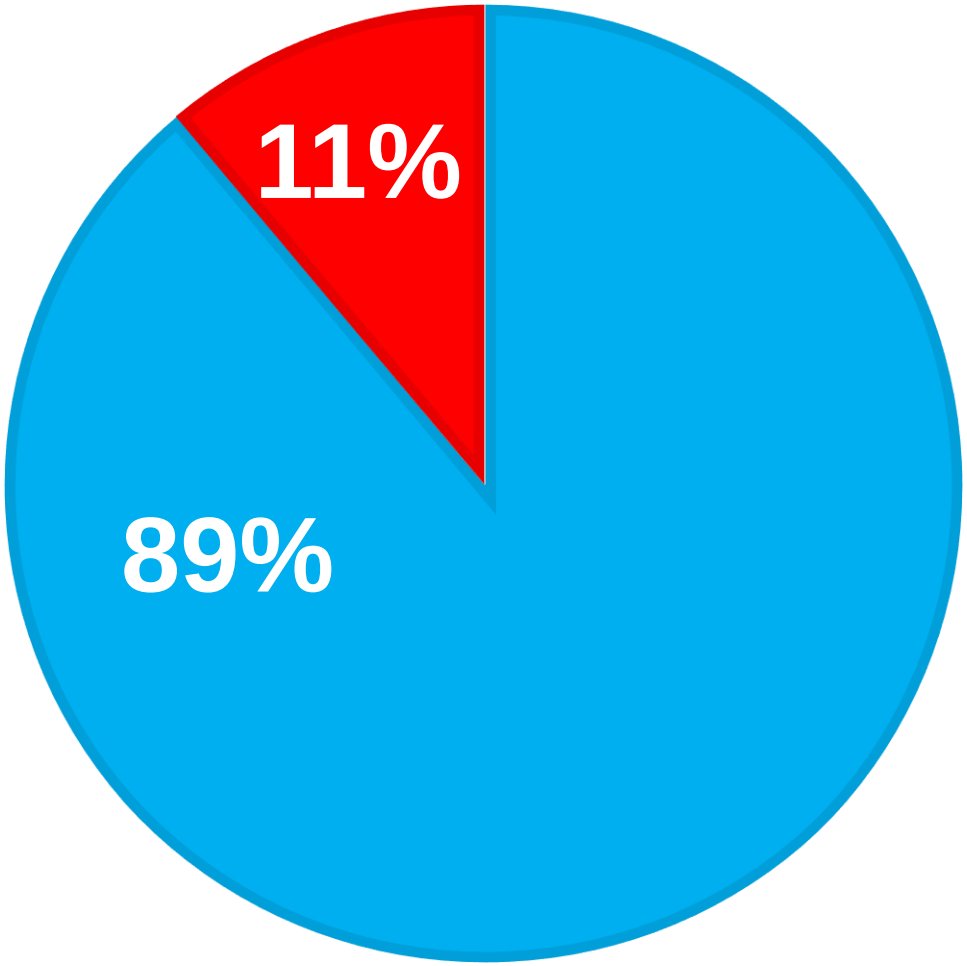
Open Resolvers WorldWide



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

DDoS

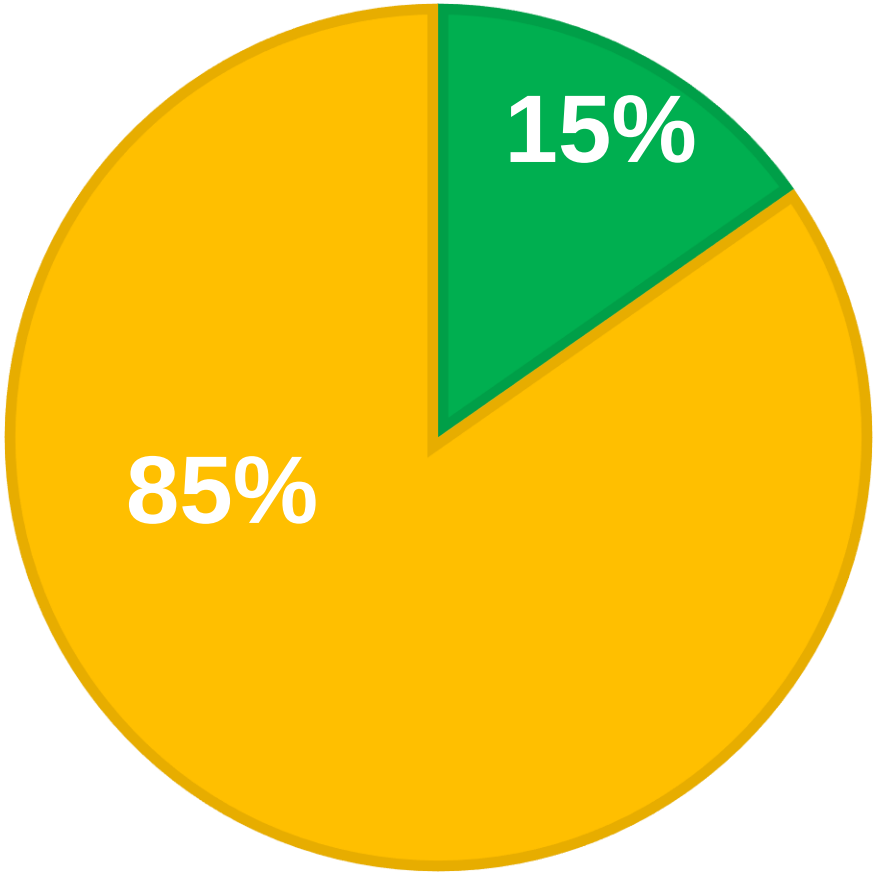
Other



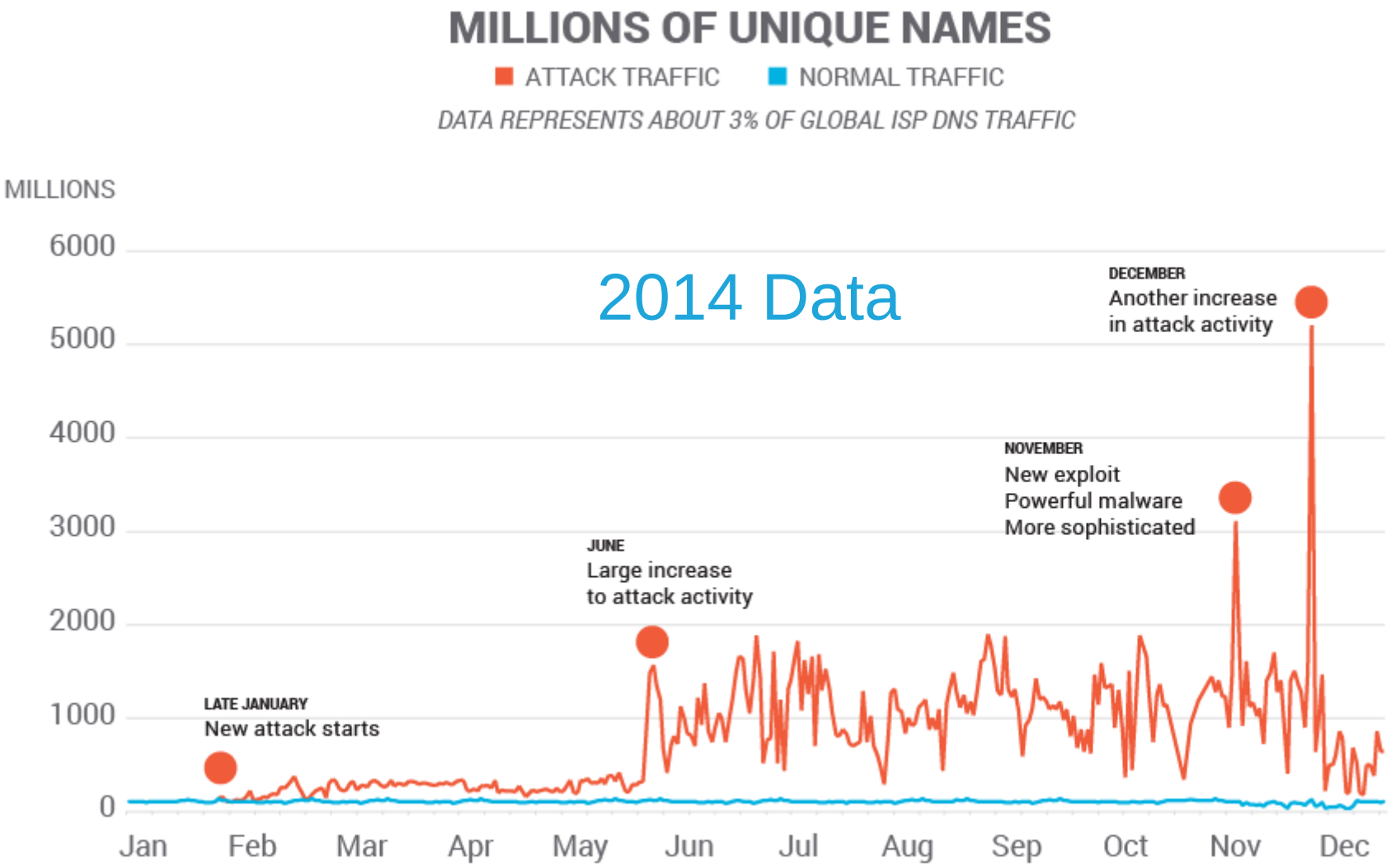
Typical “Day in The Life”
DDoS Queries Seen at a Resolver

Amplification

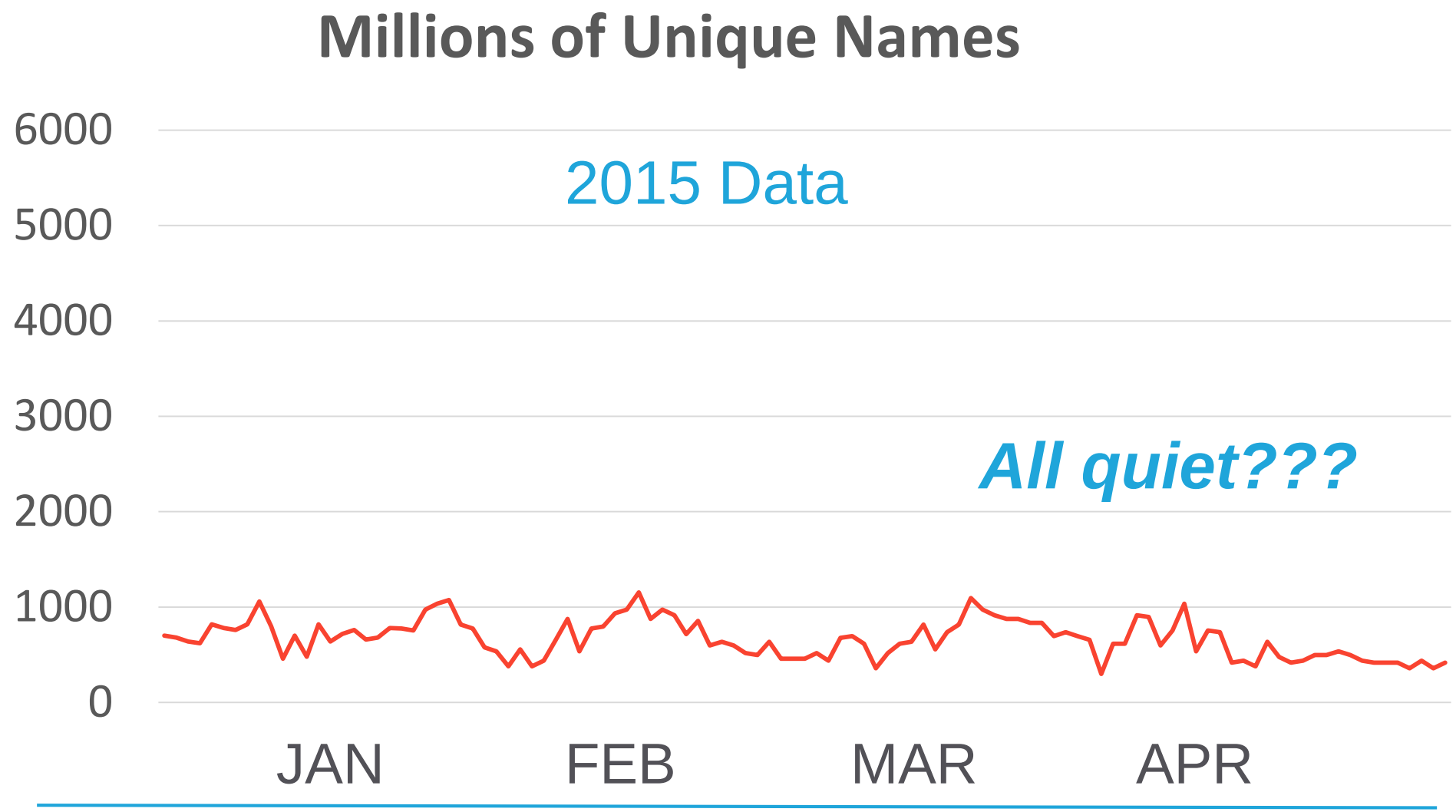
Random Subdomain



Random Subdomain Attack Trends



2015 – Quieter in Some Ways



Attacks Cause *Many* Problems

- Every query requires recursion
  - Far more work for resolvers – estimate 5x or more
  - More work for authorities responding with NXD
- Attacks on popular domains complicate filtering
- Home Gateways mask spoofed source IP
- Bots operate wholly within provider networks
  - Filtering DNS at borders won't work
- Observed tendency for cascading failures
  - Authorities and resolvers

Categorizing Attacks

- Attacks distinguished by:
  - Randomization algorithms
  - Use of open DNS proxies or bots
  - Traffic patterns – intensity, duration, ToD
  - Domains attacked
- LOTS of other attack activity out in the long tail

Observations

- Use of open resolvers/proxies still predominates
  - Installed base around 17 M mostly home gateways
  - 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
  - Example: www.appledaily.com commonly attacked

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
  - Example: rutgers.edu

Different Kinds of “Random”

nbpdestuvjklz.pay.shop6996.com.

1lHecqrP.xboot.net.

hxdfmo.iyisa.com.

a6ca.cubecraft.net.

Different Random Label Patterns = Different Attacks

Popular Names are Attacked

About 9% of names attacked are popular

Alexa 1000 Names	Rank
baidu.com.	5
blog.sina.com.cn.	13
xlscq.blog.163.com.	56
amazon.co.uk.	65
www.bet365.com.	265
www.lady8844.com.	389
d3n9cbih5qfgv5.cloudfront.net.	458
www.appledaily.com.tw.	565
asus.com.	702

Attacks on popular names must be handled carefully: Fine Grained Policy, Whitelists

Summary Data 2015
Random Subdomain Attacks

mean	24.6 names attacked/day
median	20 names attacked/day
mode	11 names attacked/day
range	3-105 (min-max) names attacked/day
stdev	16.8

Known Compromised Devices

- Home gateways
- Surveillance cameras
- Set top boxes

- Bots scan networks for home gateways or other vulnerable devices
- Attempt to login with default passwords
- Load malware on gateway
- Malware sends huge volumes of specially crafted DNS queries
- Other vectors are possible:
  - Bots with loaders
  - Rompager
  - Others

Great Post: “The Internet of Stupid Things”

CircleID
INTERNET INFRASTRUCTURE

Home | Topics | Blogs | News | Community | Industry

Home / Blogs

The Internet of Stupid Things

Apr 30, 2015 9:37 AM PDT | Comments: 2 | Views: 10,756

By Geoff Huston

Comment | Print

In those circles where Internet prognostications abound and policy makers flock to hear grand visions of the future, we often hear about the boundless future represented by "The Internet of Things". This phrase encompasses some decades of the computing industry's transition from computers as esoteric piece of engineering affordable only by nations, to mainframes, desktops, laptops, handhelds, and now wrist computers. Where next? In the vision of the *Internet of Things*, we are going to expand the Internet beyond people, and press on with connecting up our world using billions of these chattering devices in every aspect of our world.

Another Great Post: "Smartness is a Zero Sum Game"

Credit:
Nicolas Carr
Rough Type Blog
Sept 8, 2015

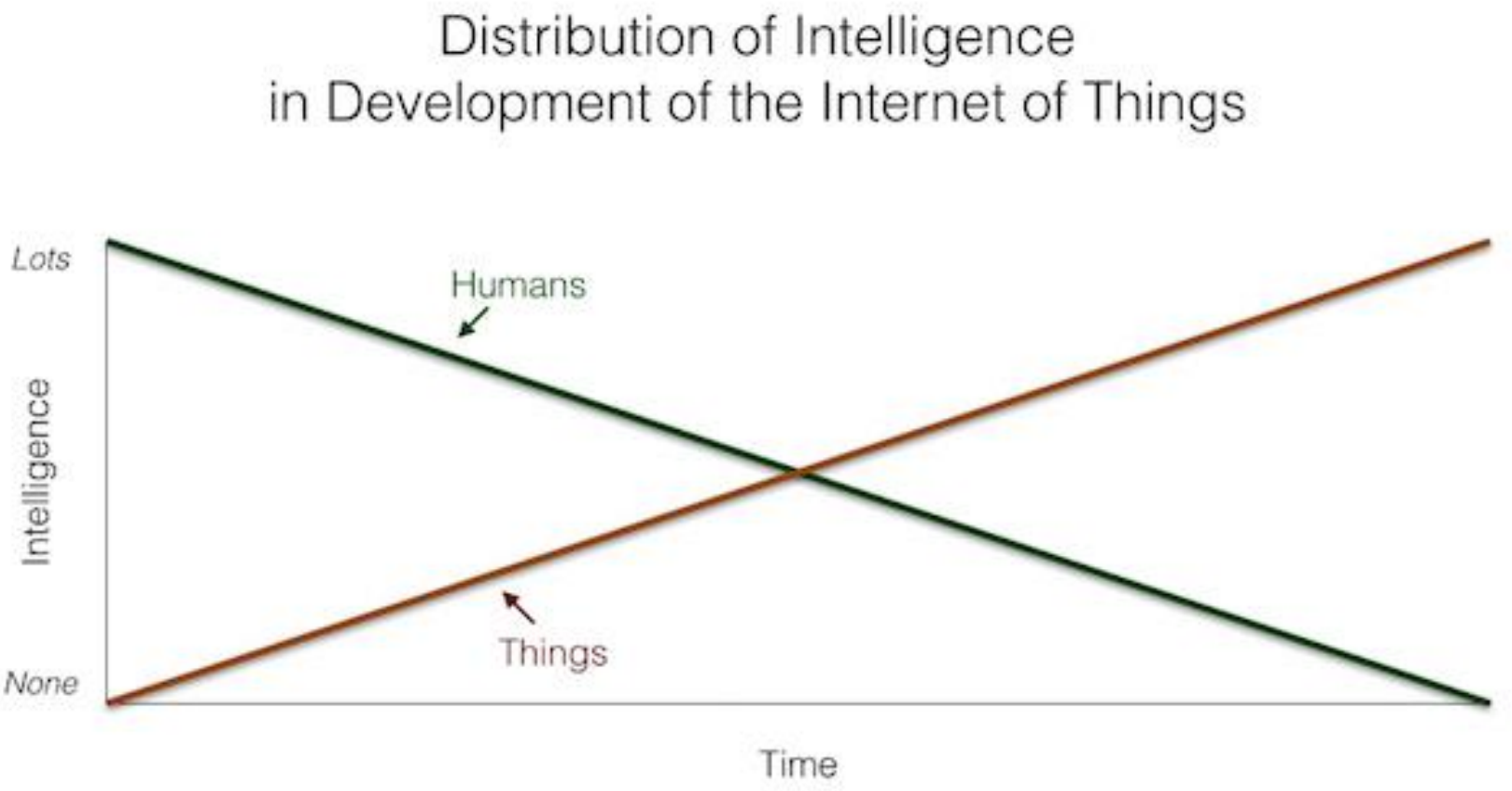
ROUGH TYPE

Menu

Smartness is a zero-sum game

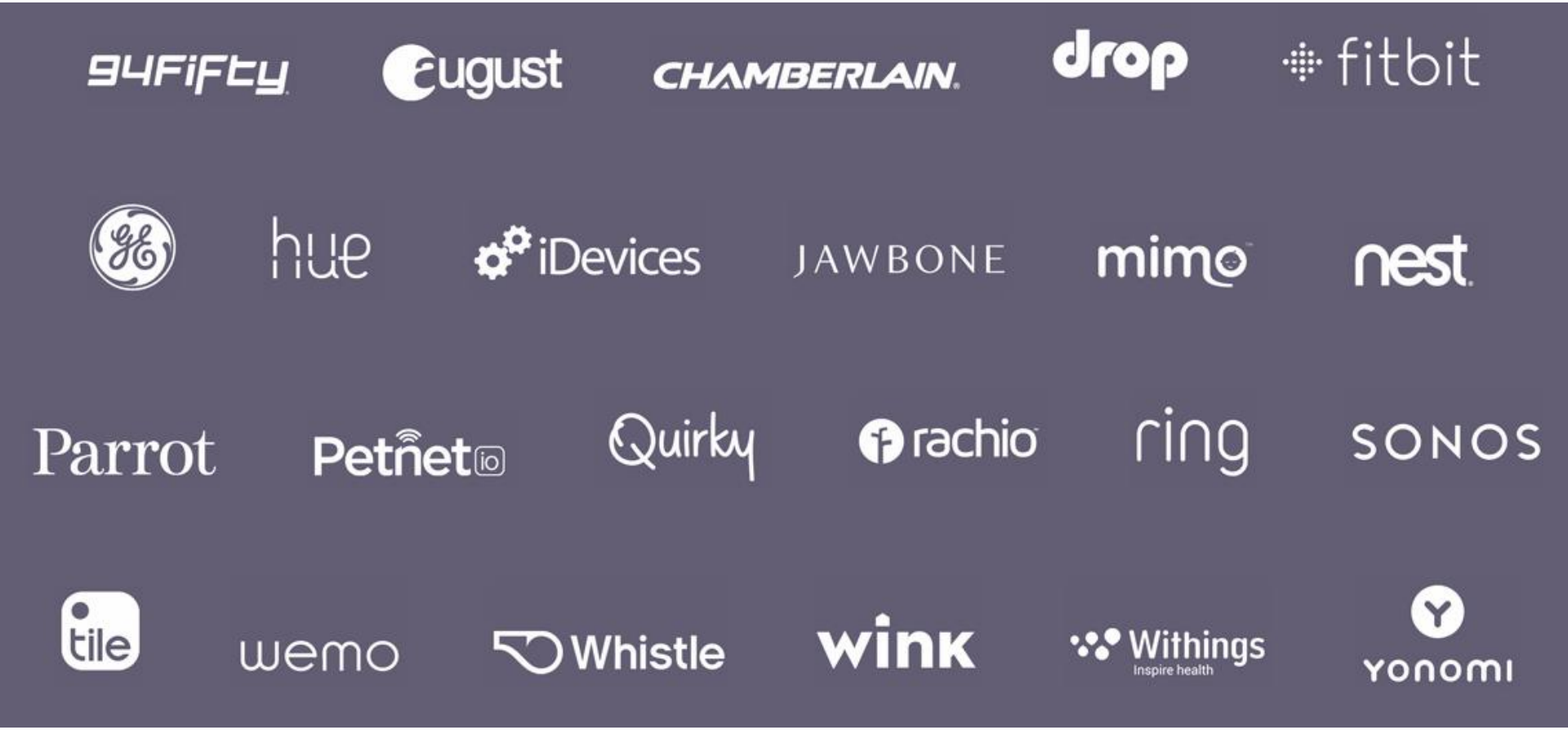
In her article "The Internet of Way Too Many Things," Allison Arleff reviews some of the exciting new products on display at Target's trendy Open House store in San Francisco. There's Leeo, a night light "that 'listens' for your smoke detector to go off and then calls your smartphone to let you know your house

What's In Store



Lots of Consumer “Things” on the Way!

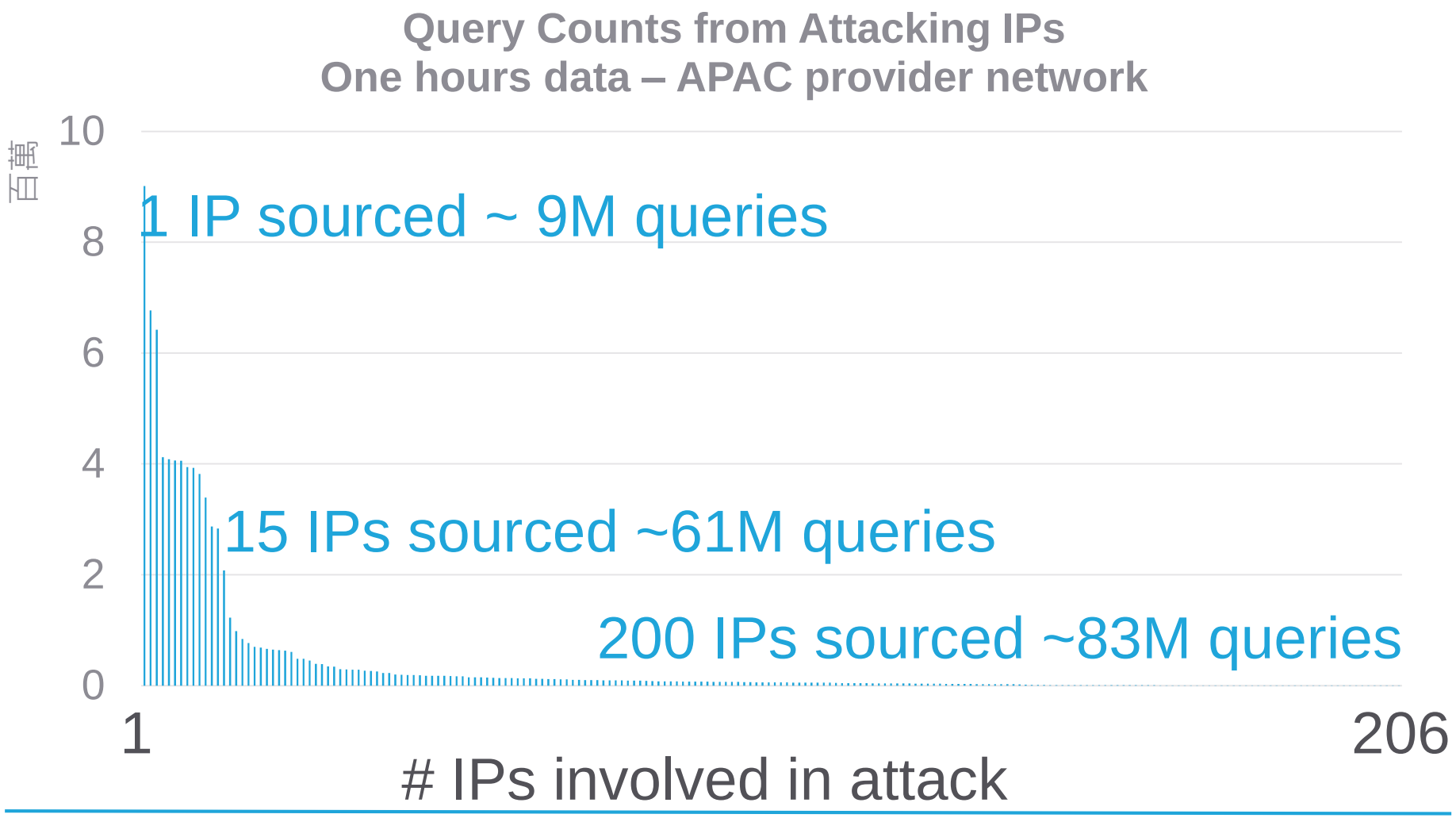
http://openhouse.target.com/#/



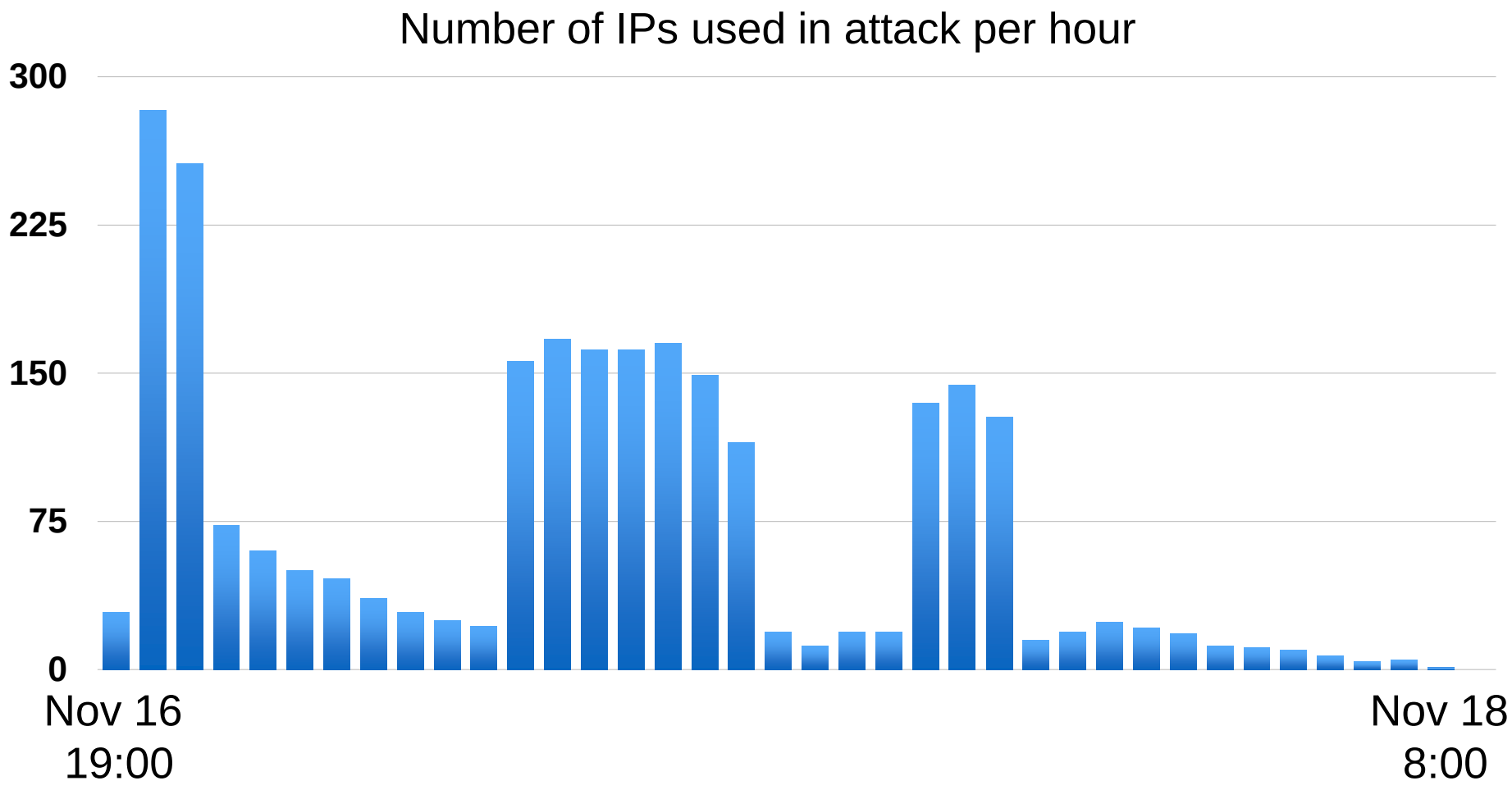
The Problem With “Things”

- Cost pressure
- Time to market pressure
- Vendors with little or no security knowledge
- Homogenous SW ecosystem - monoculture
- Can’t count on consumers to be vigilant
  - Changing defaults
  - Patching
- Etc

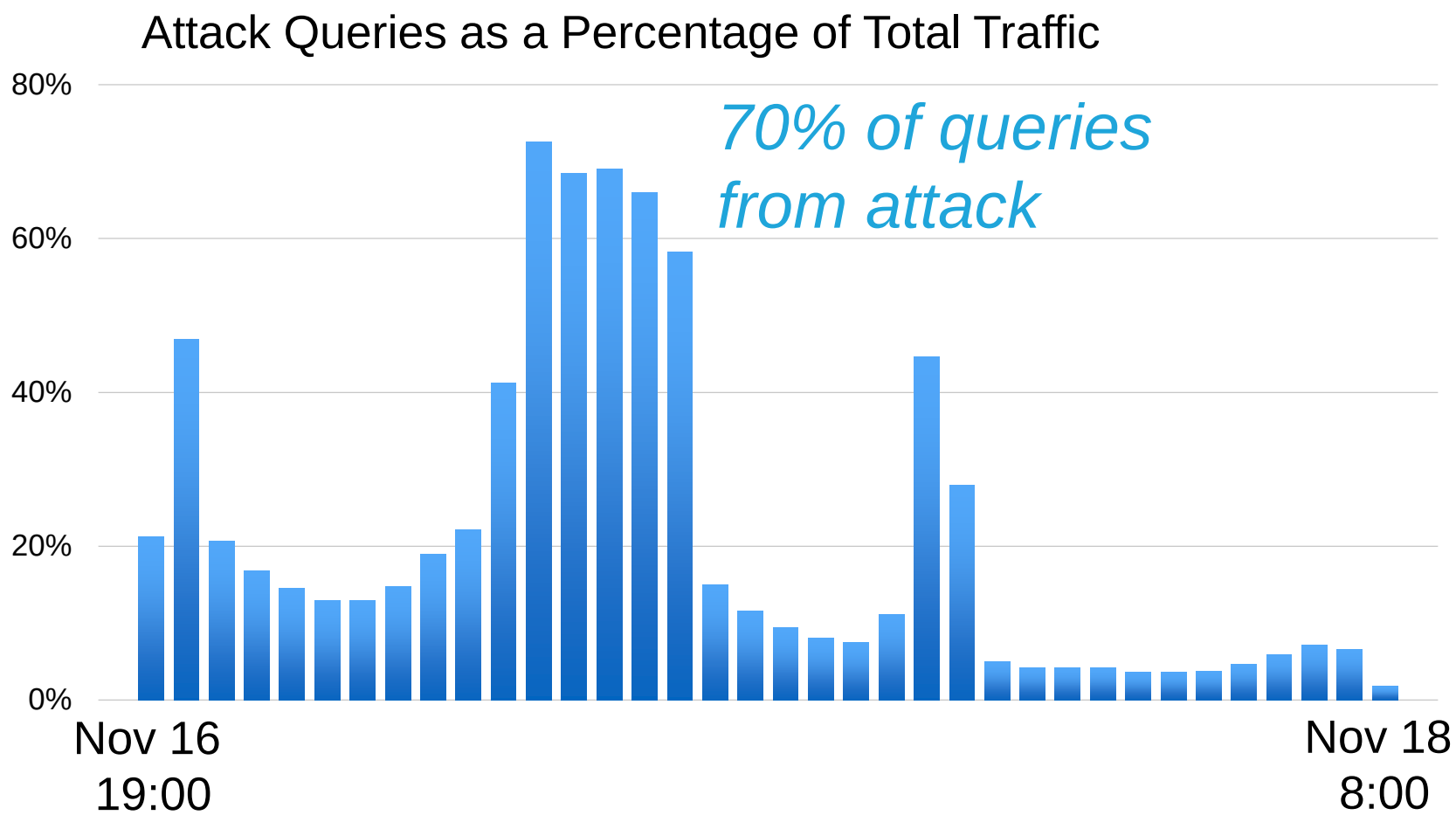
“Things” Generate Intense Attack Traffic



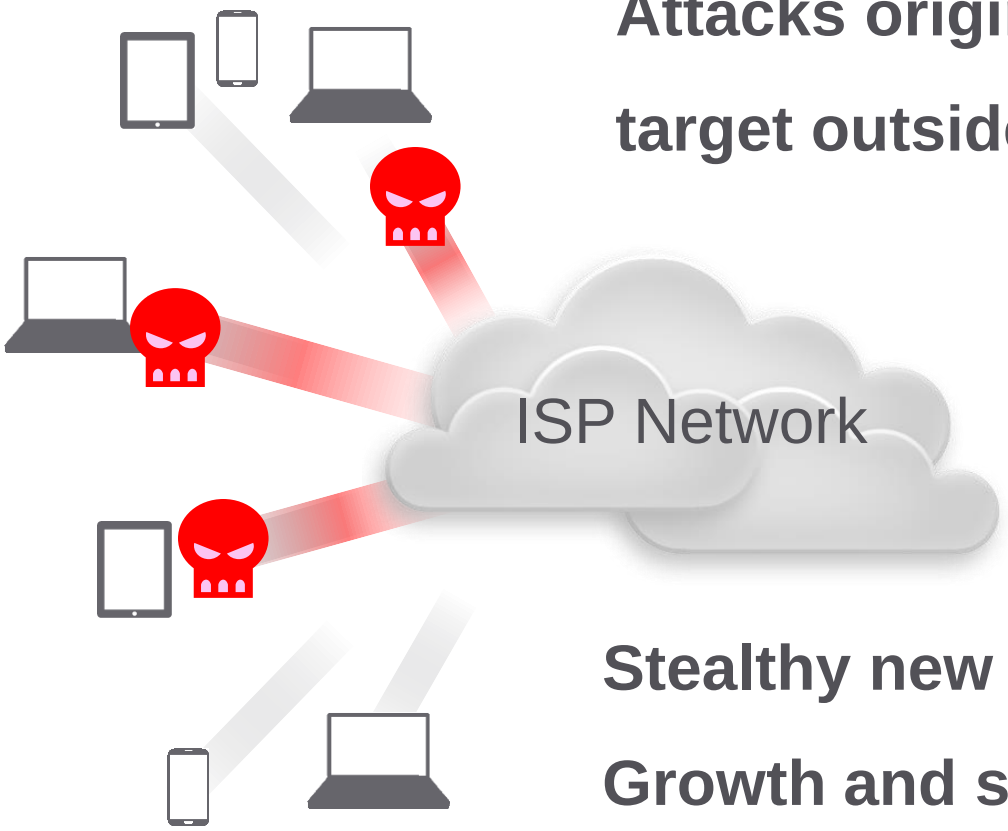
Typical Attacks: 2 Days Data



Example Attack Data



Existing Defenses Don’t Cover Today’s Exploits



Attacks originate inside networks &

target outside resources - “inside-out”

Stealthy new DNS DDoS attacks

Growth and sophistication of botnets

DNS tunnels stealing service

Way Forward: Protecting the DNS

- Ingress filtering
  - PROTECT “GOOD” TRAFFIC
  - Block “BAD” traffic
- Dynamic threat lists
  - Track target domains by the minute
  - Adapt as attacks evolve

For Details of Effectiveness of Ingress Filtering See:

DNS-OARC May 2015 Ralf Weber

“Digging Down Into DNS DDoS Data”

https://indico.dns-oarc.net/event/21/timetable/#20150509

Summary

- Constant DNS-based DDoS evolution
- Open Home Gateways remain a problem
- Malware-based exploits have occurred
- “Things” may create new exposure

- Attackers refining techniques
- Remediation needs to be undertaken with care
  - Clients want answers!!
  - Critical to protect good traffic