

Drilling Down into DNS DDoS

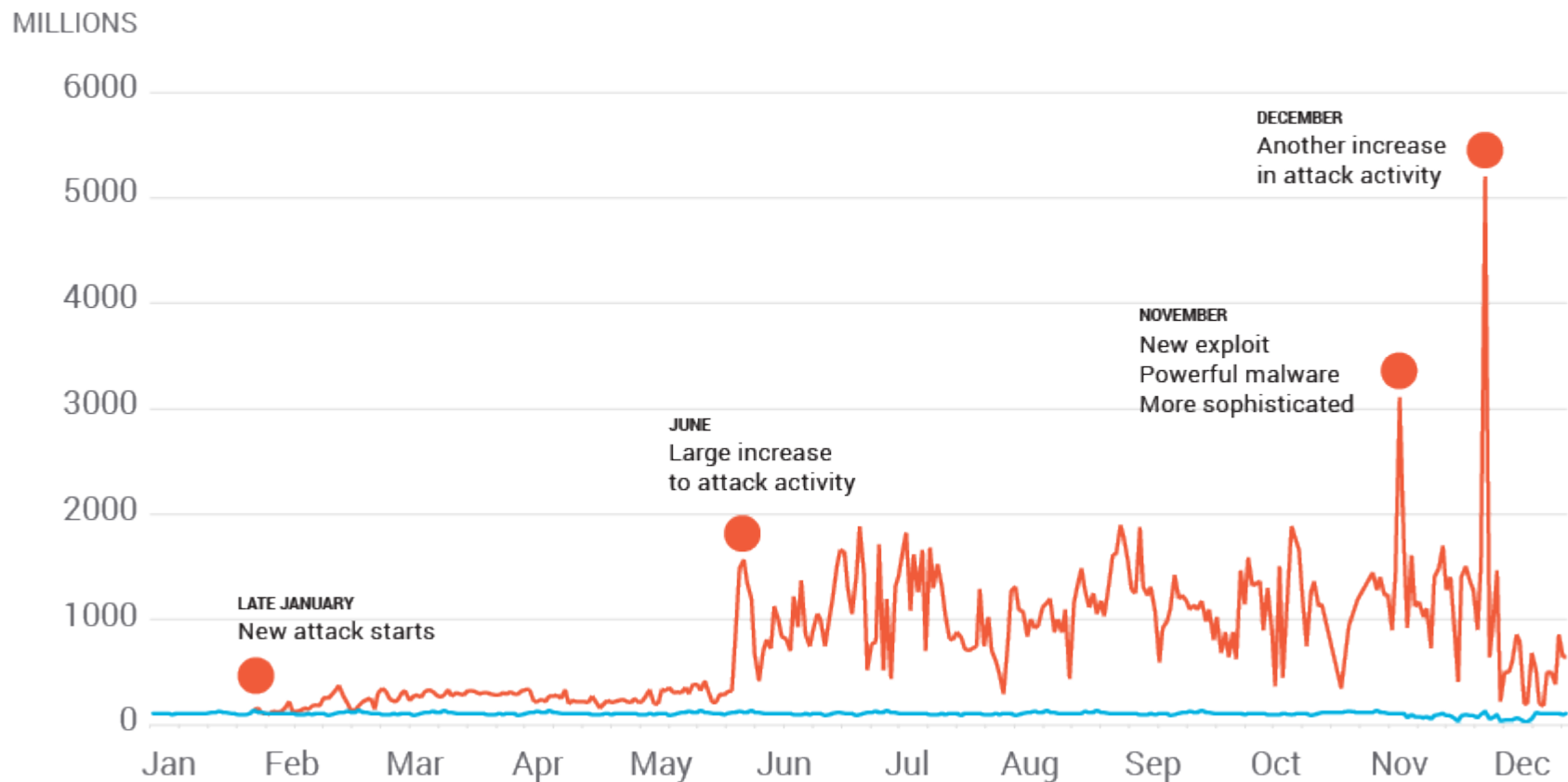
NANOG 63

DNS DDoS in Increasing: 2014 Data

MILLIONS OF UNIQUE NAMES

■ ATTACK TRAFFIC ■ NORMAL TRAFFIC

DATA REPRESENTS ABOUT 3% OF GLOBAL ISP DNS TRAFFIC



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 2014 – Highly focused attacks

Different Kinds of “Random”

nbpdestuvjklz.pay.shop6996.com.

1lHecqrP.xboot.net.

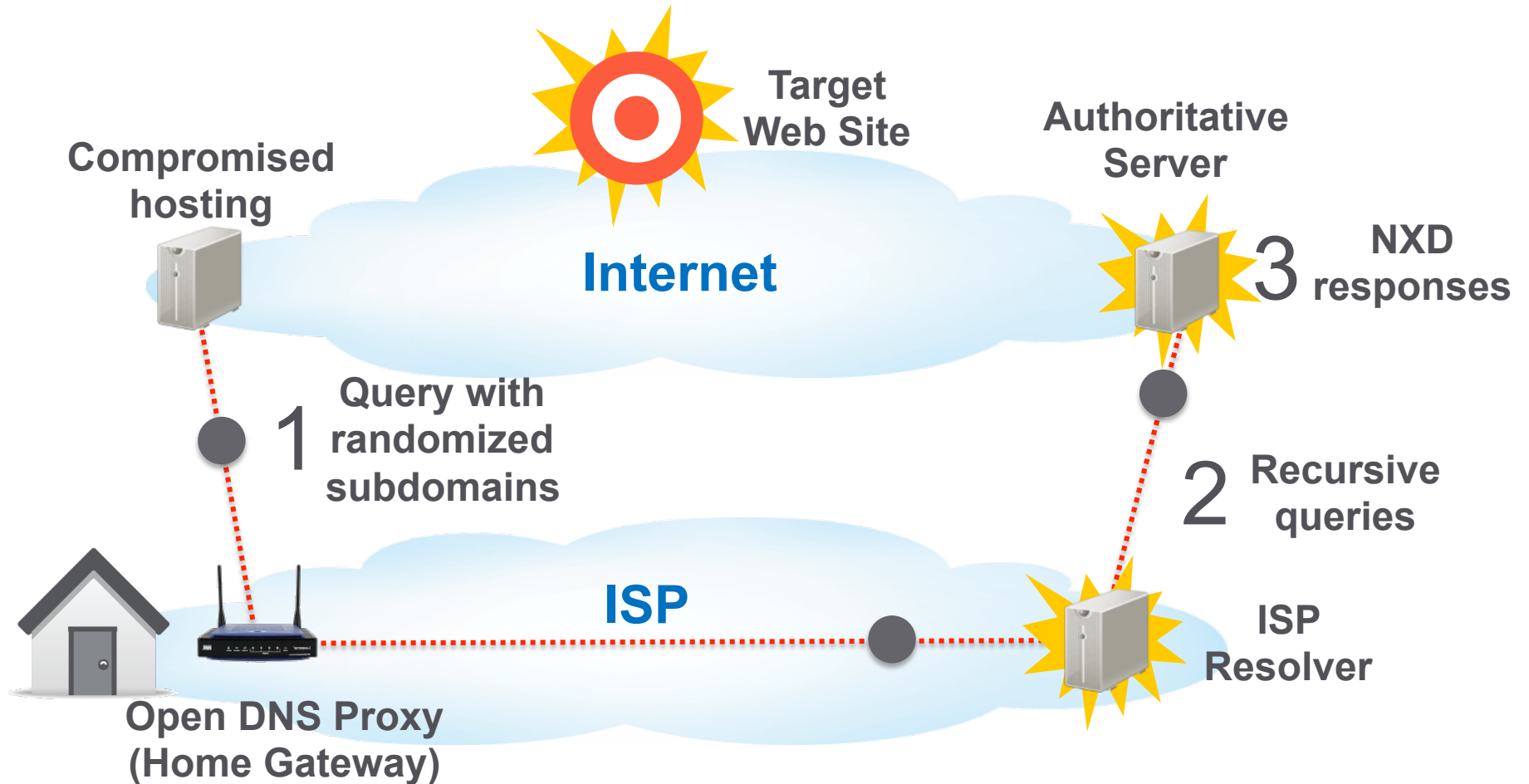
hxdfmo.iyisa.com.

a6ca.cubecraft.net.

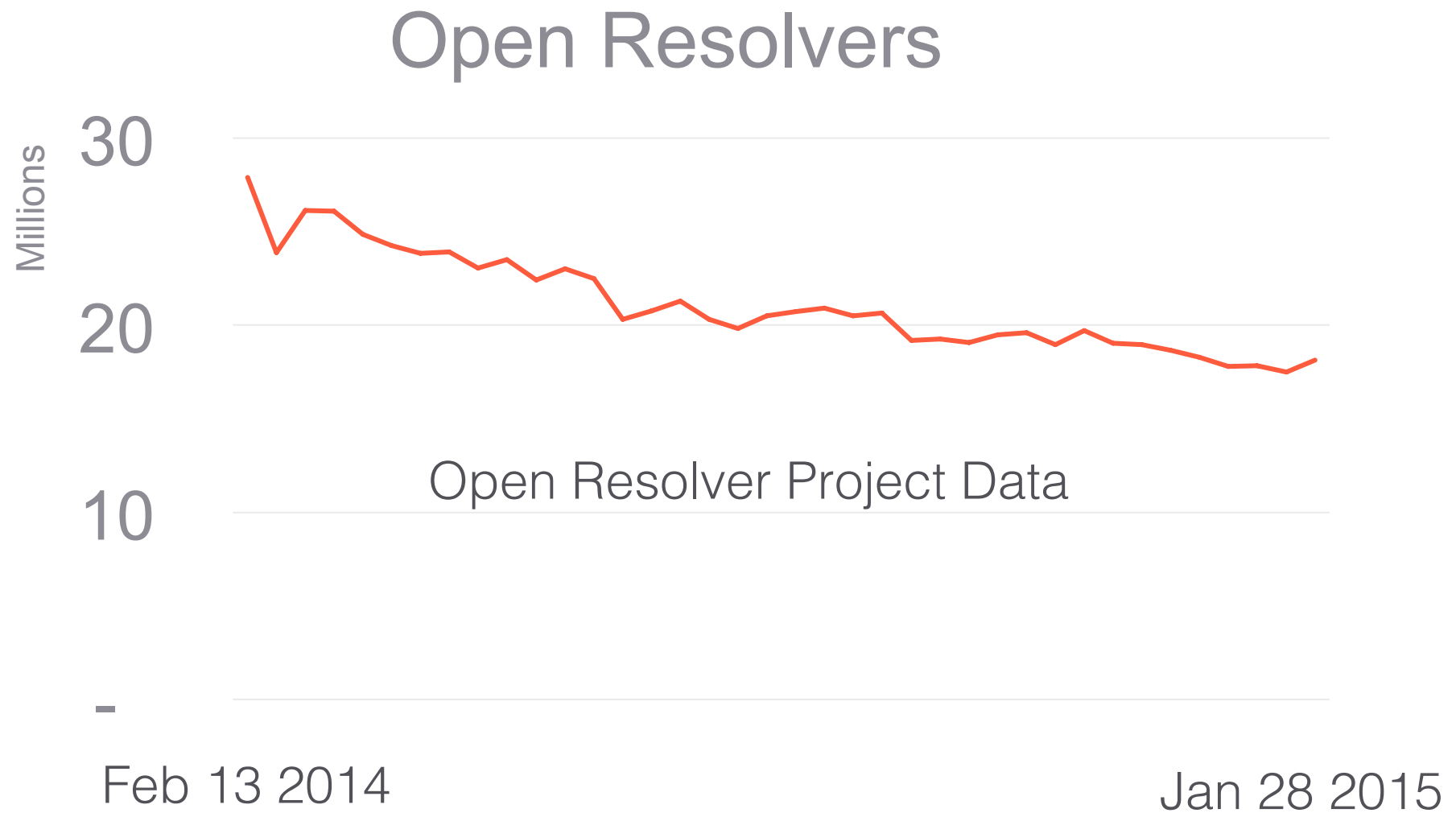
Different Patterns = Different Attacks

First Method of Attack

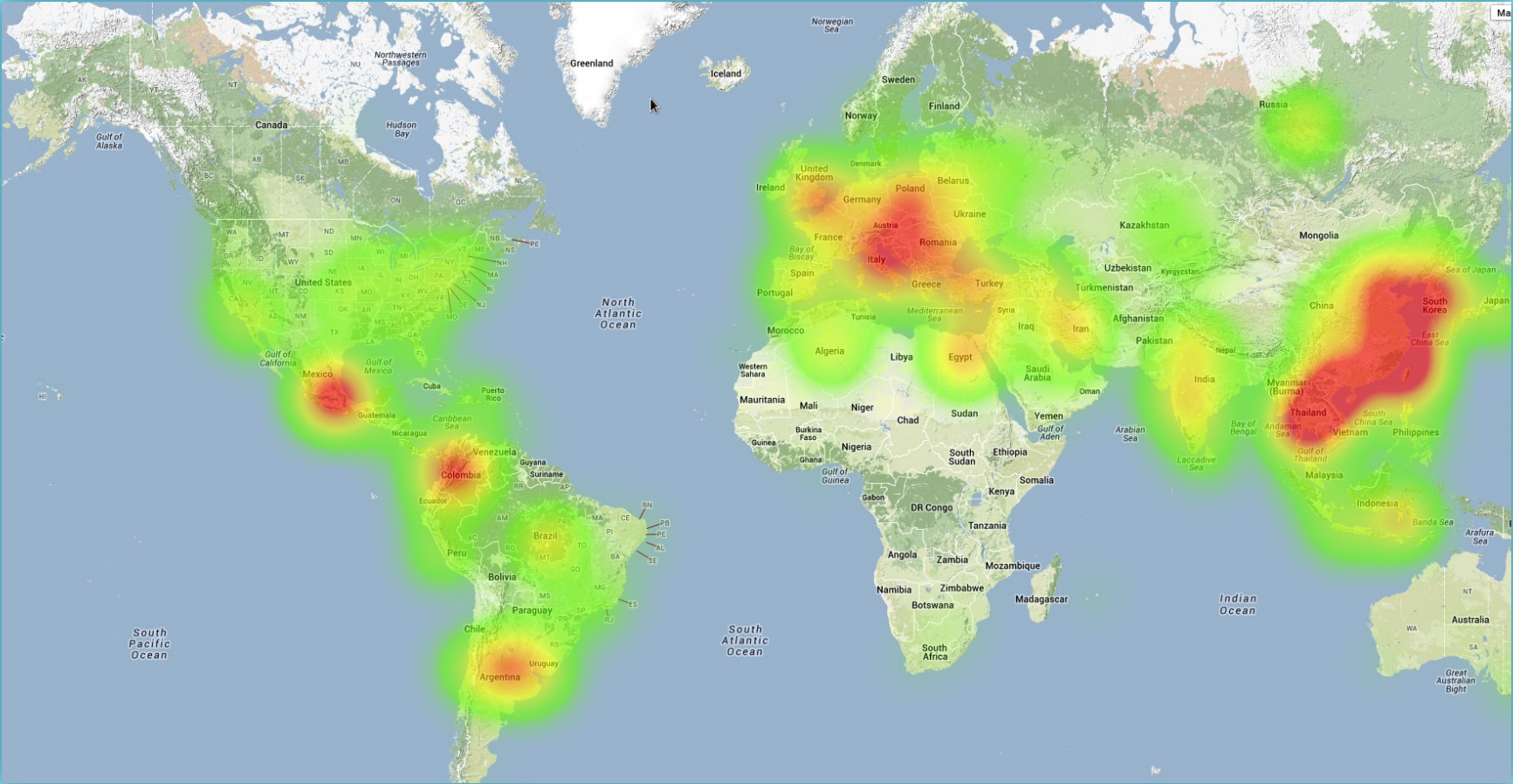
Attacks Using Open DNS Proxies



Open Resolvers Are Declining

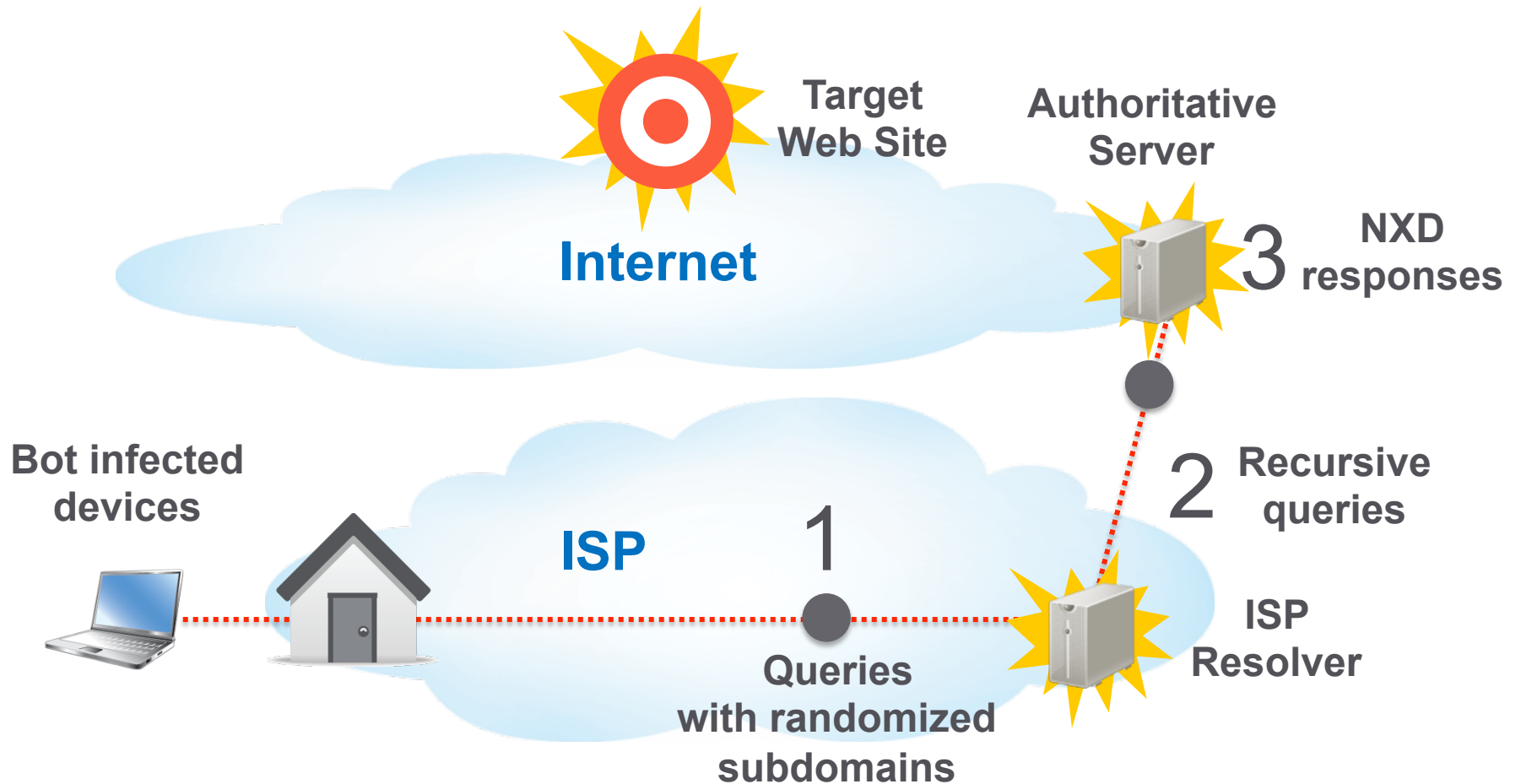


Where Are They Now?



Second Method of Attack

Attacks Using Bots



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*



RouterPasswords.com

Welcome to the internet's largest and most updated default router passwords database,

Select Router Manufacturer:

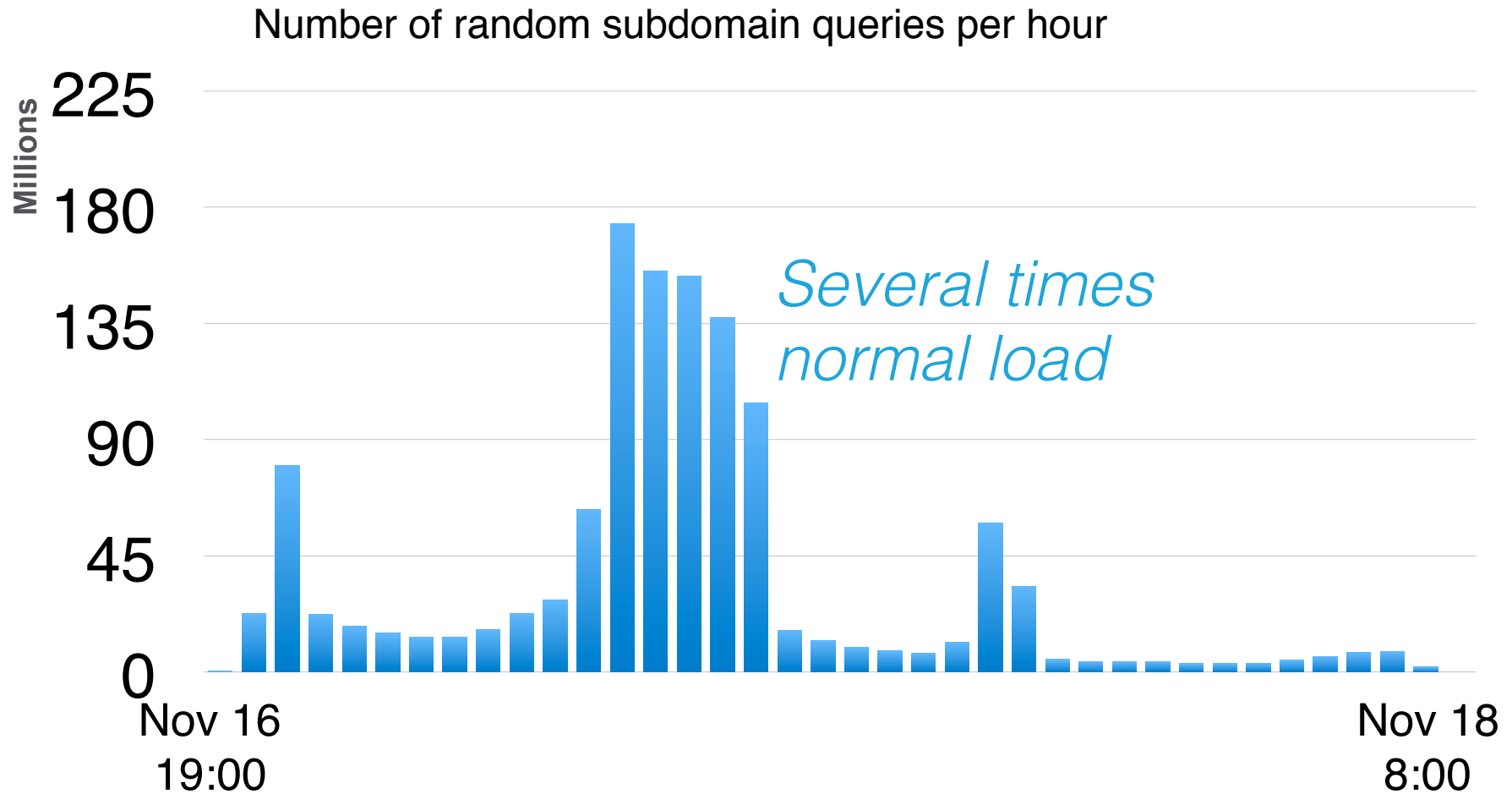
BELKIN ▼

Find Password

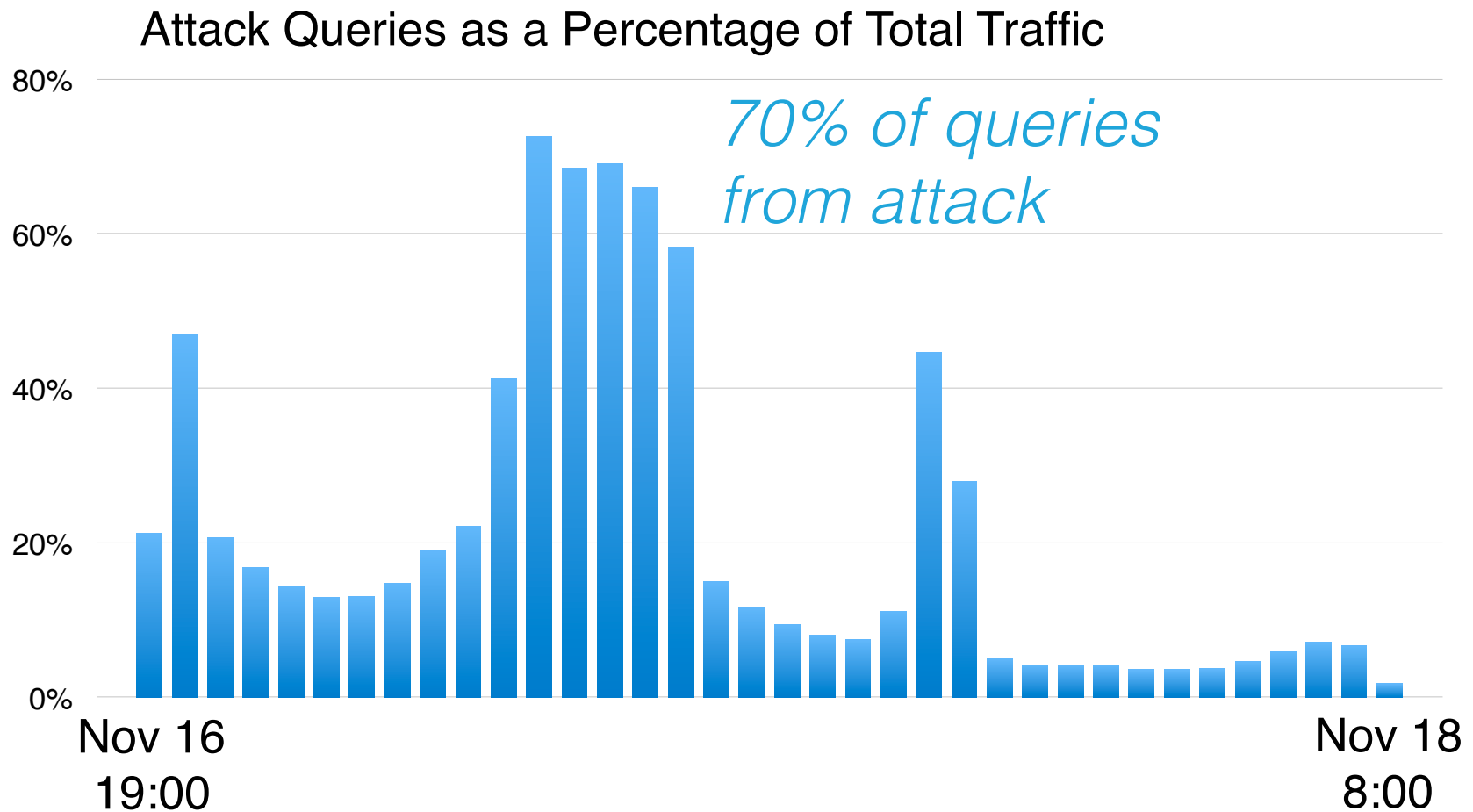
Copyright © 2014 RouterPasswords.com.
All rights reserved

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

Example Attack: One DNS Server



Example Attack Data



Example Attack Data

