nominum™

Harness Your Internet Activity

DNS-Based DDoS
Evolving Threat

UKNOF Sept 2015
Manchester, UK

Ralf Weber

Nominum Research

- 2 Terabytes of data analyzed per day
  - Anonymized from ISPs worldwide
  - Estimate about 3% of ISP DNS resolver traffic
- Team of data scientists
- Algorithms searching for:
  - DDoS
  - Bots
  - Malware
  - Machine generated traffic
  - Many other trends

DNS DDoS: Rapid Evolution

2012 Authorities see surge in DNS amplification

Resolvers see spikes in amplification

2013 Open Resolver Project reports 30 M open resolvers

Open DNS proxies in home gateways discovered

“Purpose built” amplification domains

Random subdomain attacks generate huge spikes

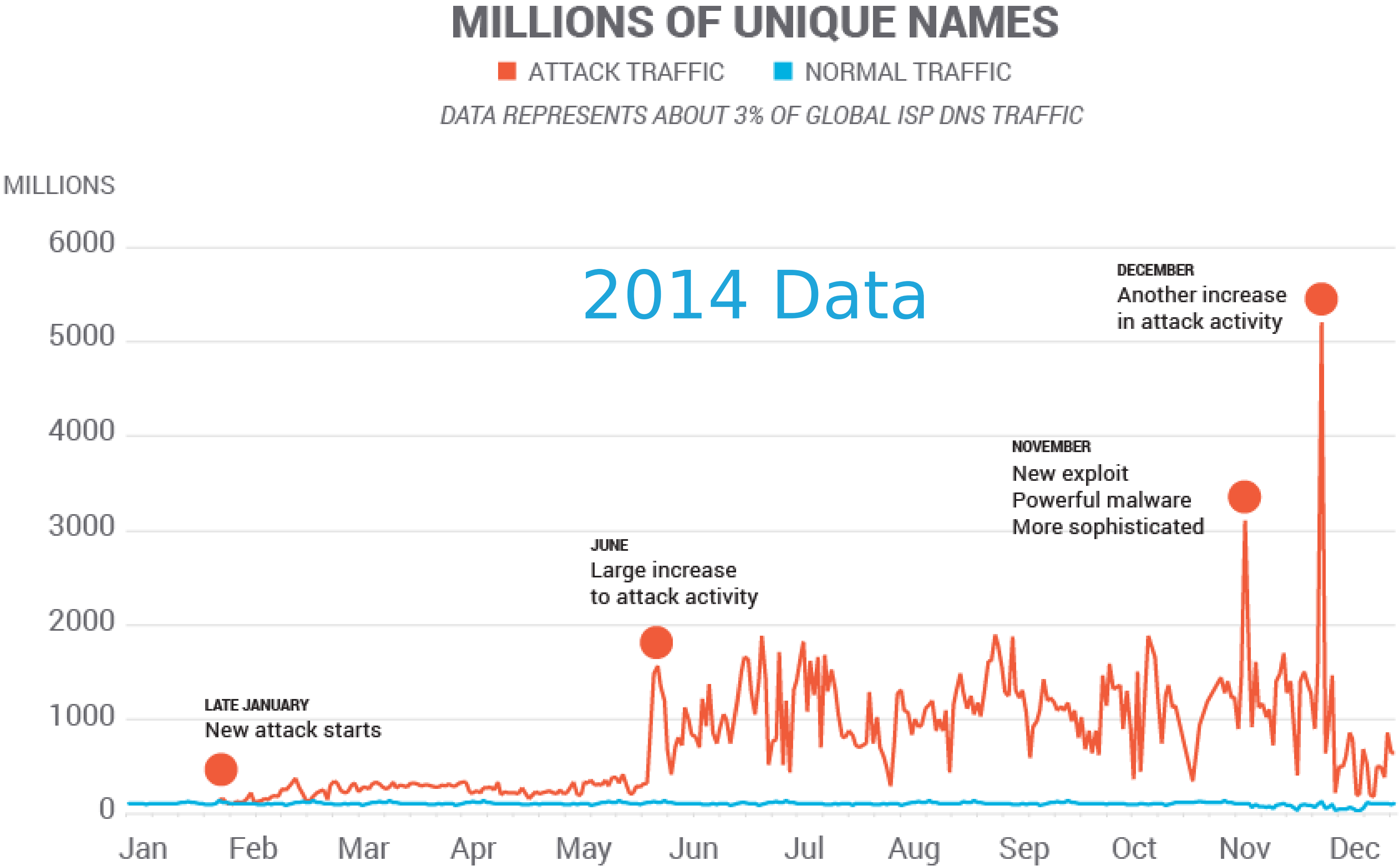
2014 Attacks targeting popular domains (Alexa 1000).

Bot-based DNS DDoS malware

2015 Attackers refine their exploits - stealth

New attacks combine randomization & amplification

2014 Random Subdomain Attacks



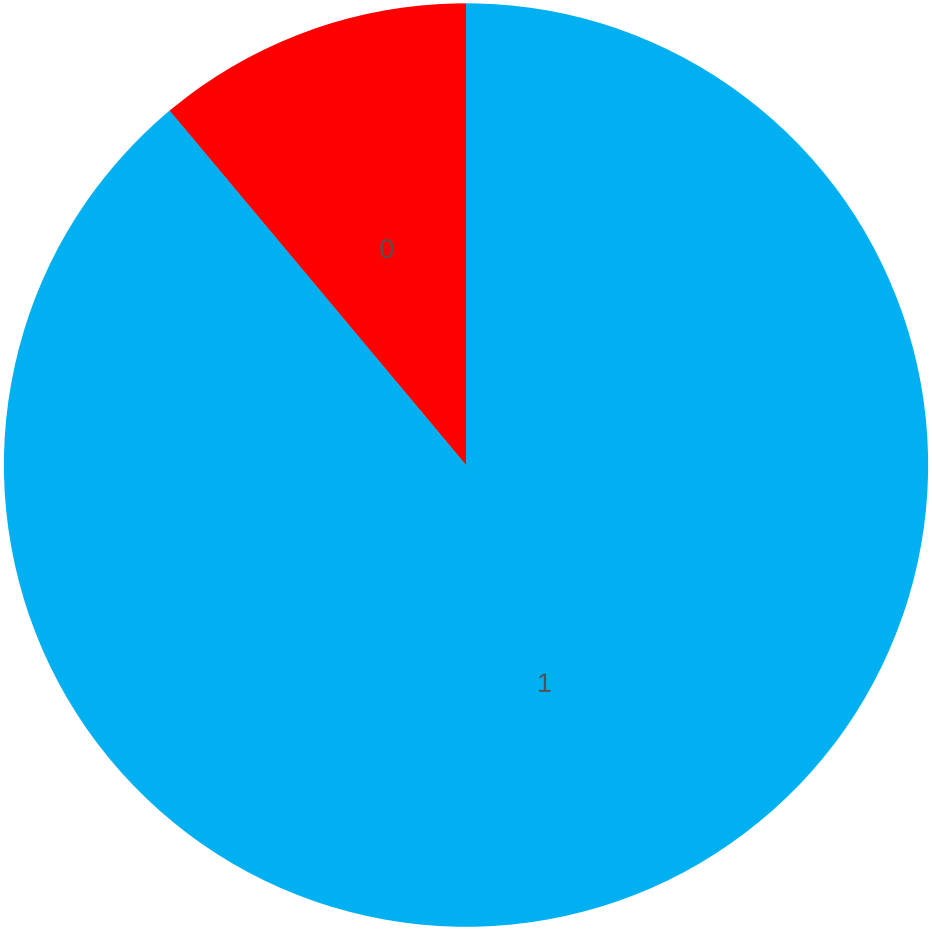
2015 Random Subdomain Attack Activity

- No big spikes
- Concentrated attacks – observed as much as 8000QPS from a single IP
  - Identified as a surveillance camera!
- Small number of IPs – 100-200 per attack
  - ~100 IPs took down large network
- Attacks seem to be stealthier

Typical "Day in the Life"
DNS Queries Seen at a Resolver

DDoS

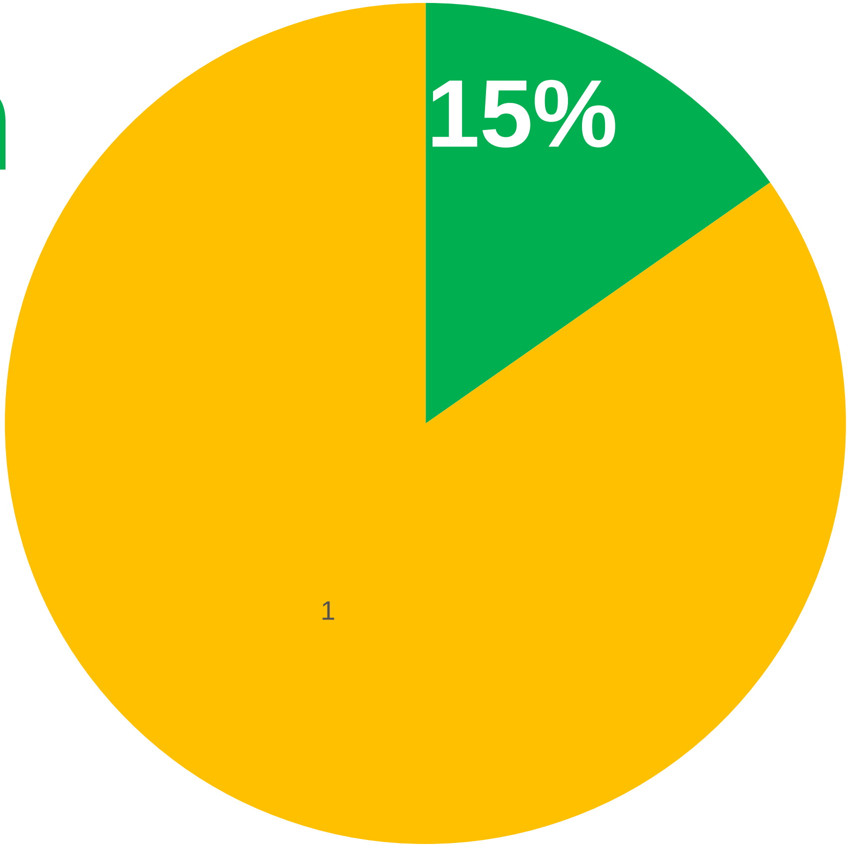
Other



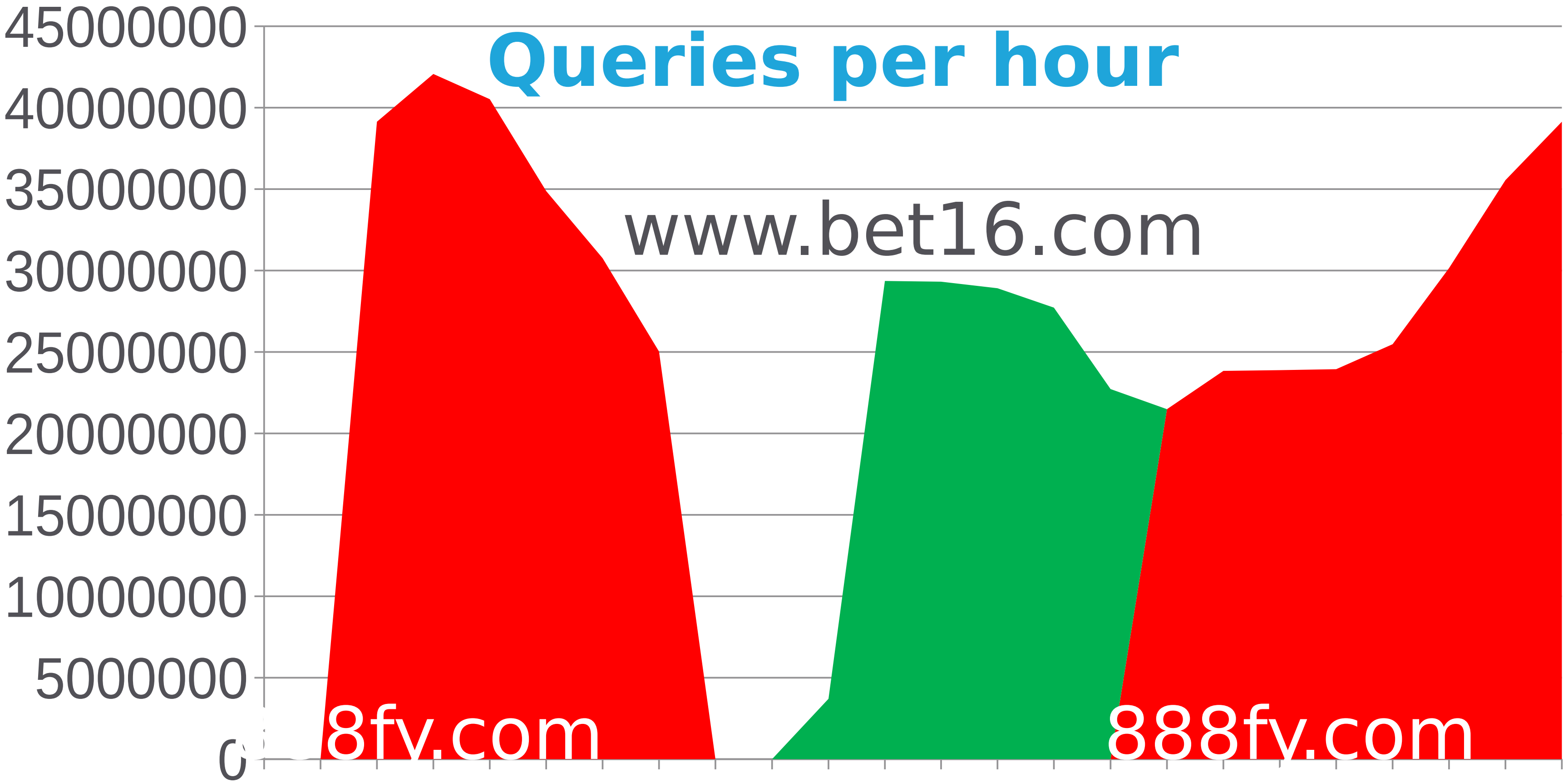
Typical Day in The Life
DDoS Queries Seen at a Resolver

Amplification

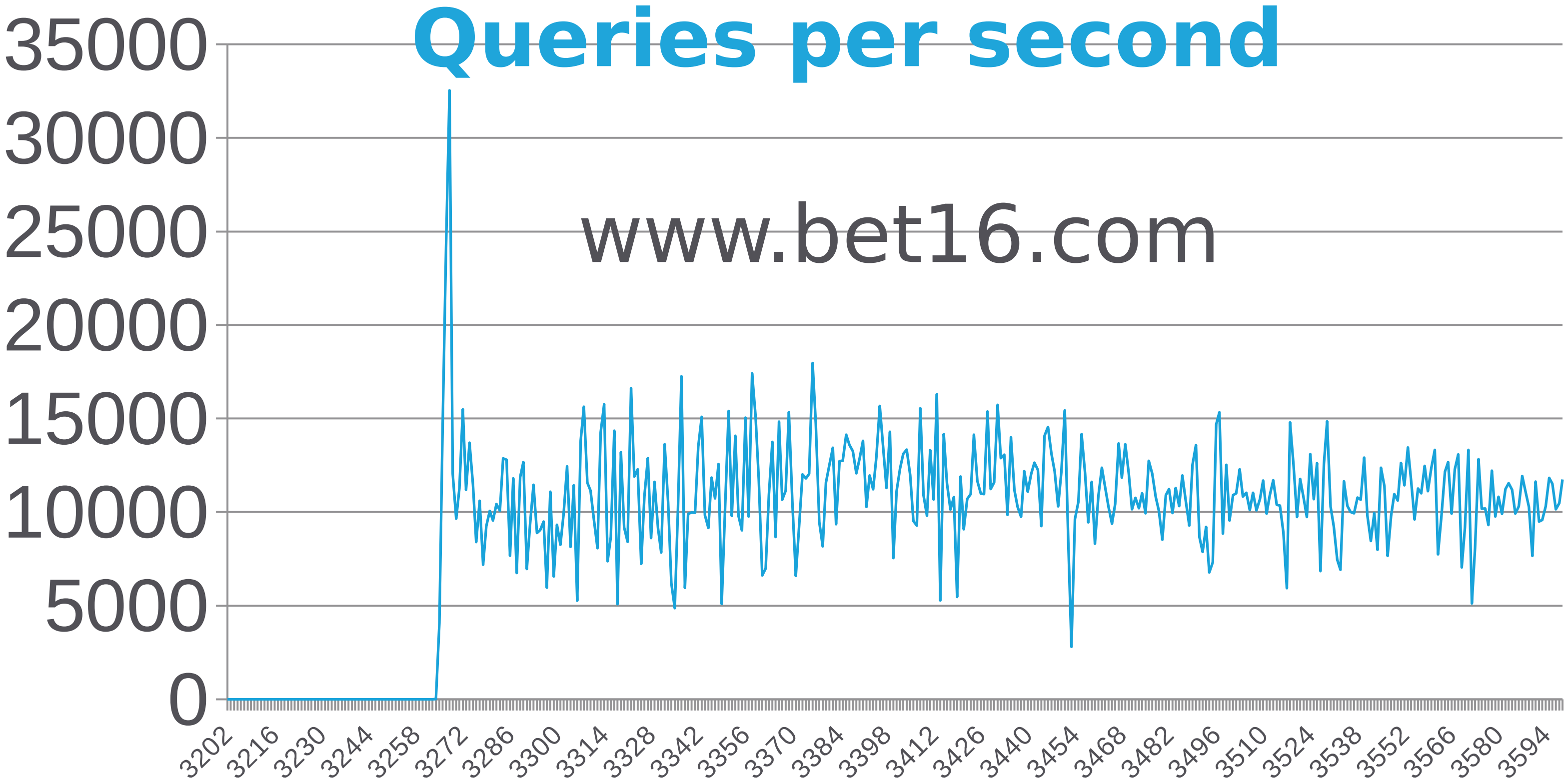
Random Subdomain



Typical Day in The Life
Random Subdomain Queries Seen at a Resolver

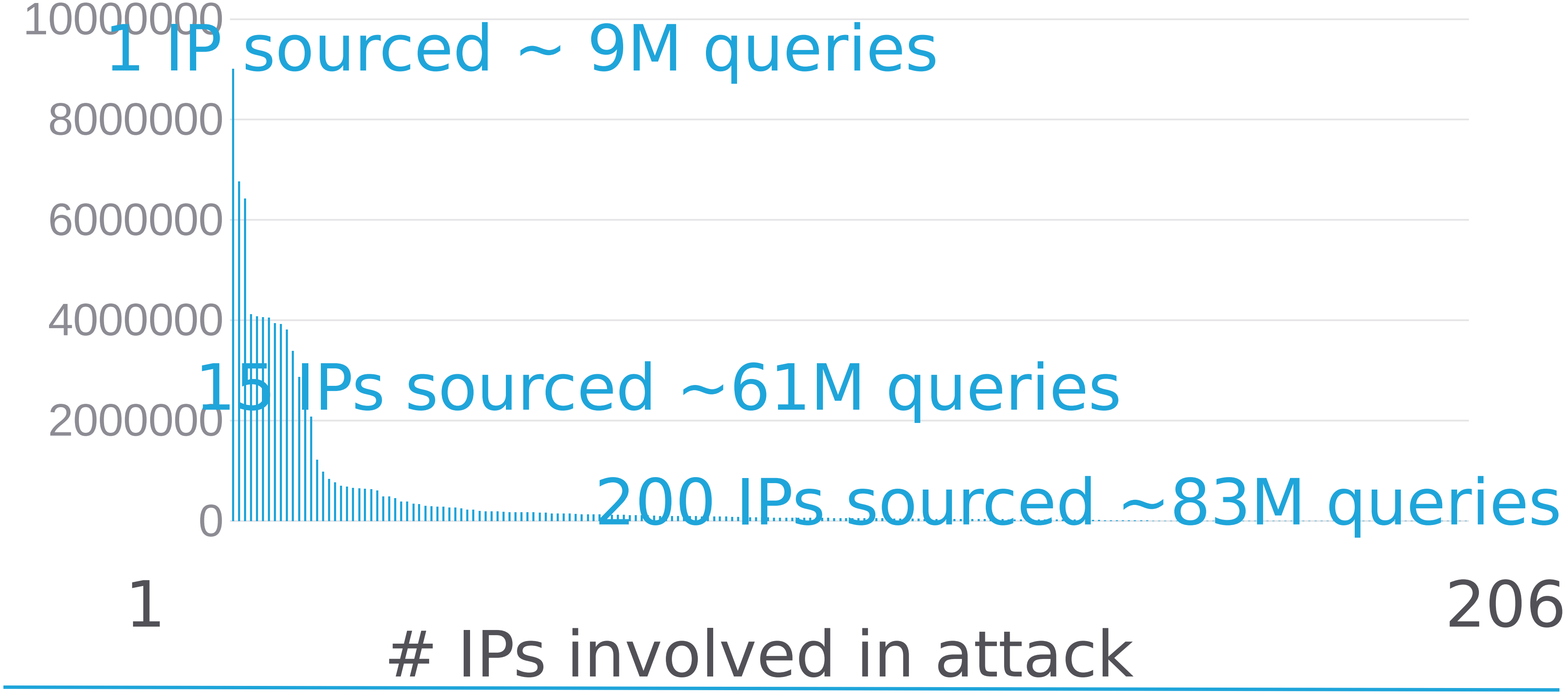


An Hour in The Life
Random Subdomain Queries Seen at a Resolver



A Few “Things” Generate Intense Attack Traffic

Query Counts from Attacking IPs
One hours data – APAC provider network



1 IP sourced ~ 9M queries

15 IPs sourced ~61M queries

200 IPs sourced ~83M queries

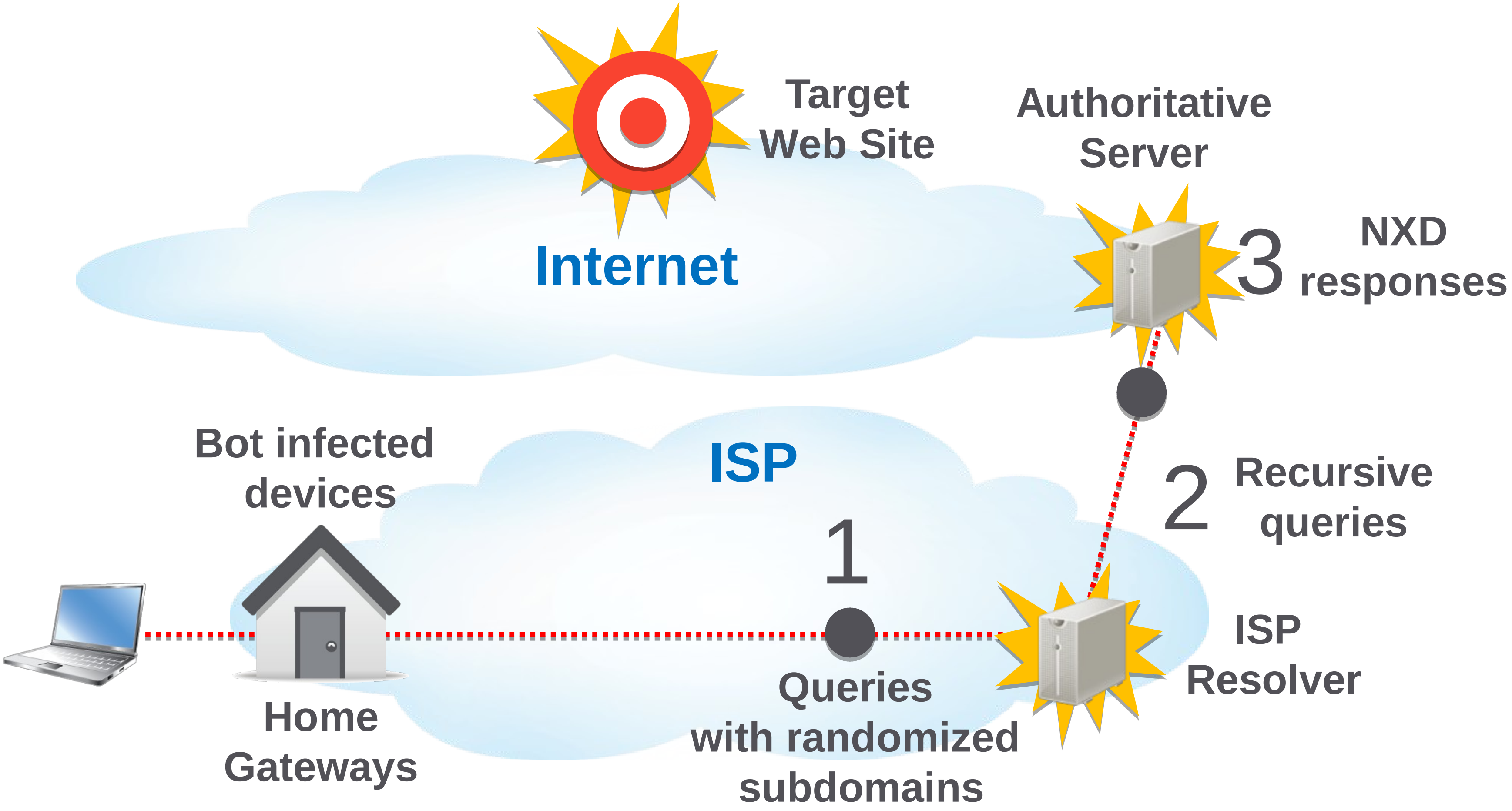
Diverse Attacks

- 4 major kinds of attacks
  - – Early attacks used open DNS proxies in home gateways
  - – Latest attacks use bot malware in home gateways and other “Things”
- LOTS of other attack activity out in the long tail

fferent Random Label Patterns = Different Attac

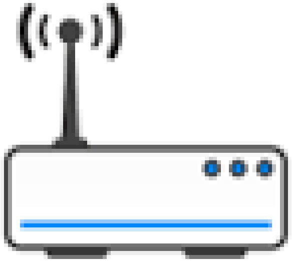
nominum

Attacks Using Bots

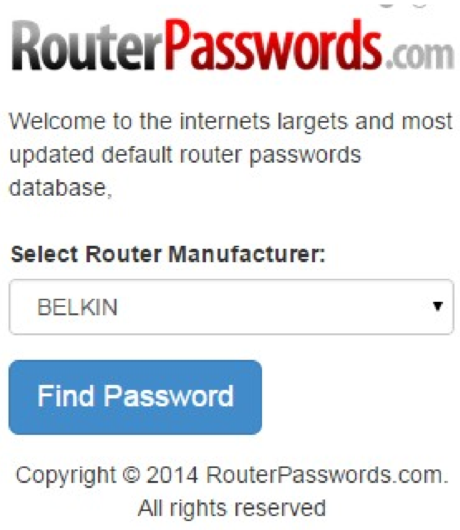


What’s Happening?

Network scans for vulnerable devices:
Home gateways or other “Things”



Attempts login with default passwords



RouterPasswords.com

Welcome to the internets largets and most updated default router passwords database,

Select Router Manufacturer:

BELKIN ▾

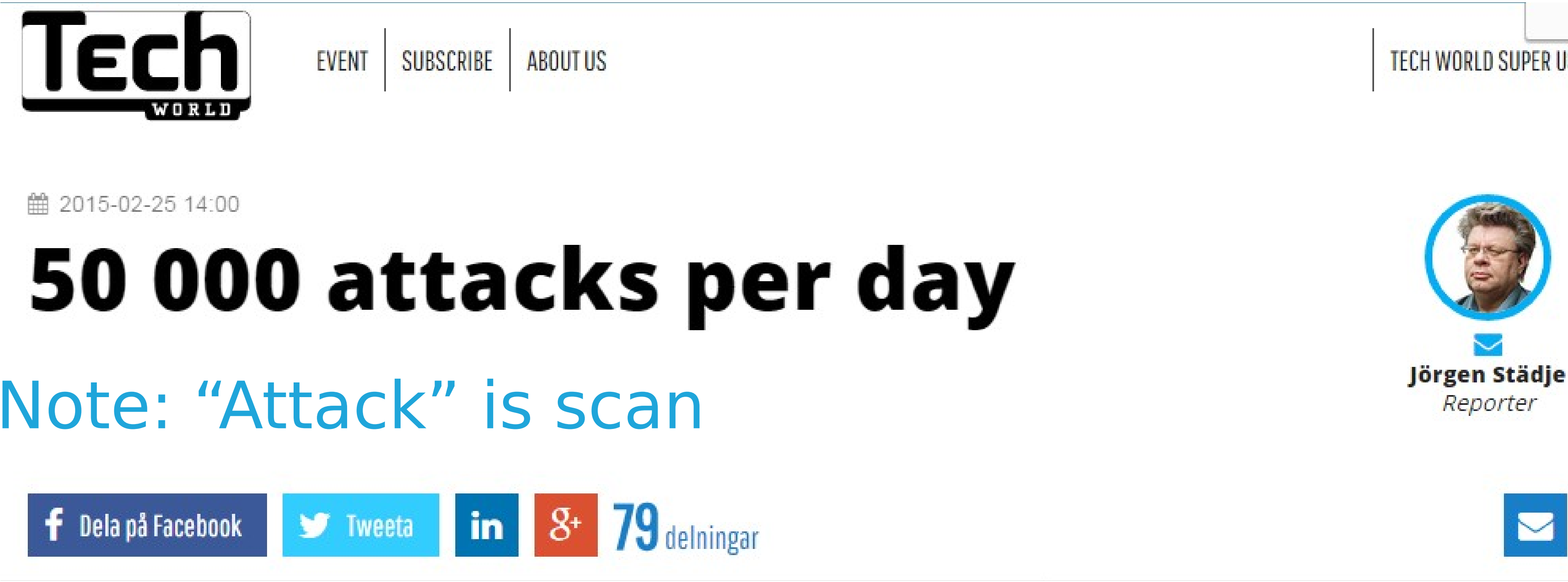
Copyright © 2014 RouterPasswords.com. All rights reserved

Most consumer devices use Busybox:
Many utilities at the attackers disposal
Load and run malware

Other vectors possible: Bots with loaders, Rompager

Lots of Scanning Activity

TechWorld Feb 25, 2015
(translated from Swedish)



2015-02-25 14:00

50 000 attacks per day

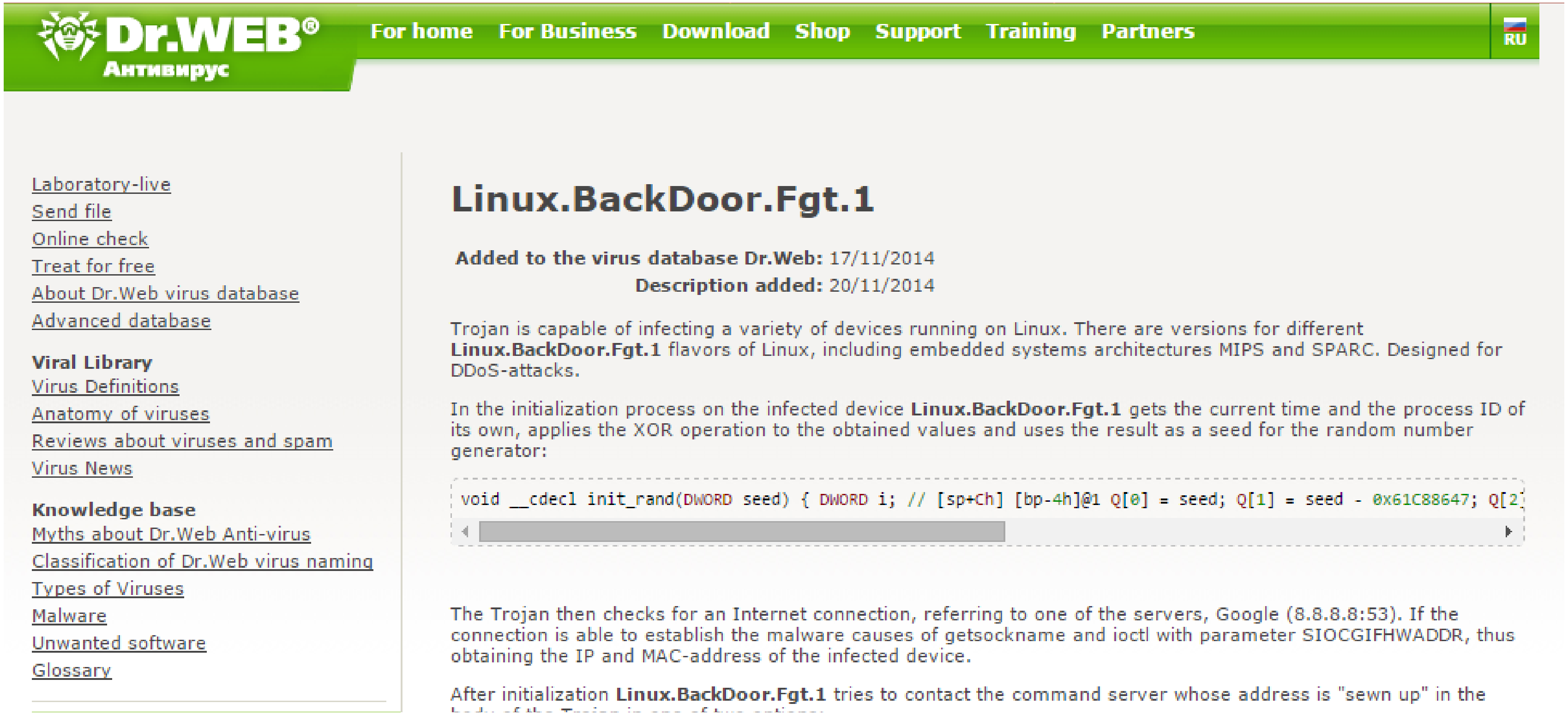
Jörgen Städje
Reporter

Note: “Attack” is scan

http://techworld.idg.se/2.2524/1.608986/50-000-attacker-per-dygn

Likely Source of Home Gateway Malware

escription of malware translated from Russian hows how busybox is used



Laboratory-live
Send file
Online check
Treat for free
About Dr.Web virus database
Advanced database

Viral Library
Virus Definitions
Anatomy of viruses
Reviews about viruses and spam
Virus News

Knowledge base
Myths about Dr.Web Anti-virus
Classification of Dr.Web virus naming
Types of Viruses
Malware
Unwanted software
Glossary

Linux.BackDoor.Fgt.1

Added to the virus database Dr.Web: 17/11/2014
Description added: 20/11/2014

Trojan is capable of infecting a variety of devices running on Linux. There are versions for different **Linux.BackDoor.Fgt.1** flavors of Linux, including embedded systems architectures MIPS and SPARC. Designed for DDoS-attacks.

In the initialization process on the infected device **Linux.BackDoor.Fgt.1** gets the current time and the process ID of its own, applies the XOR operation to the obtained values and uses the result as a seed for the random number generator:

```
void __cdecl init_rand(DWORD seed) { DWORD i; // [sp+Ch] [bp-4h]@1 Q[0] = seed; Q[1] = seed - 0x61C88647; Q[2
```

The Trojan then checks for an Internet connection, referring to one of the servers, Google (8.8.8.8:53). If the connection is able to establish the malware causes of getsockname and ioctl with parameter SIOCGIFHWADDR, thus obtaining the IP and MAC-address of the infected device.

After initialization **Linux.BackDoor.Fgt.1** tries to contact the command server whose address is "sewn up" in the

http://vms.drweb.com/virus/?i=4242198

Bots Can also Load DDoS Malware And They're Everywhere

Threat Type	Query Count
Spybot	1,679,616
Vobfus	925,323
Nitol	883,376
Gamarue	878,672
VBInject	864,944
Spambot	613,449
Ramnit	418,984
Bladabindi	90,486

Threat Type	Query Count
Dorkbot	52,935
Morto	35,912
Sality	35,711
Virut	32,027
SMSsend	16,000
Jeefo	14,645
Gbot	11,853
GameOver	9,407

Bot queries on a typical day

Bots with loaders in RED

Attacks Cause *Many* Problems

- 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
- RRL by authorities increases work for resolvers & authorities
  - This seems to have gone away for now

Remediation

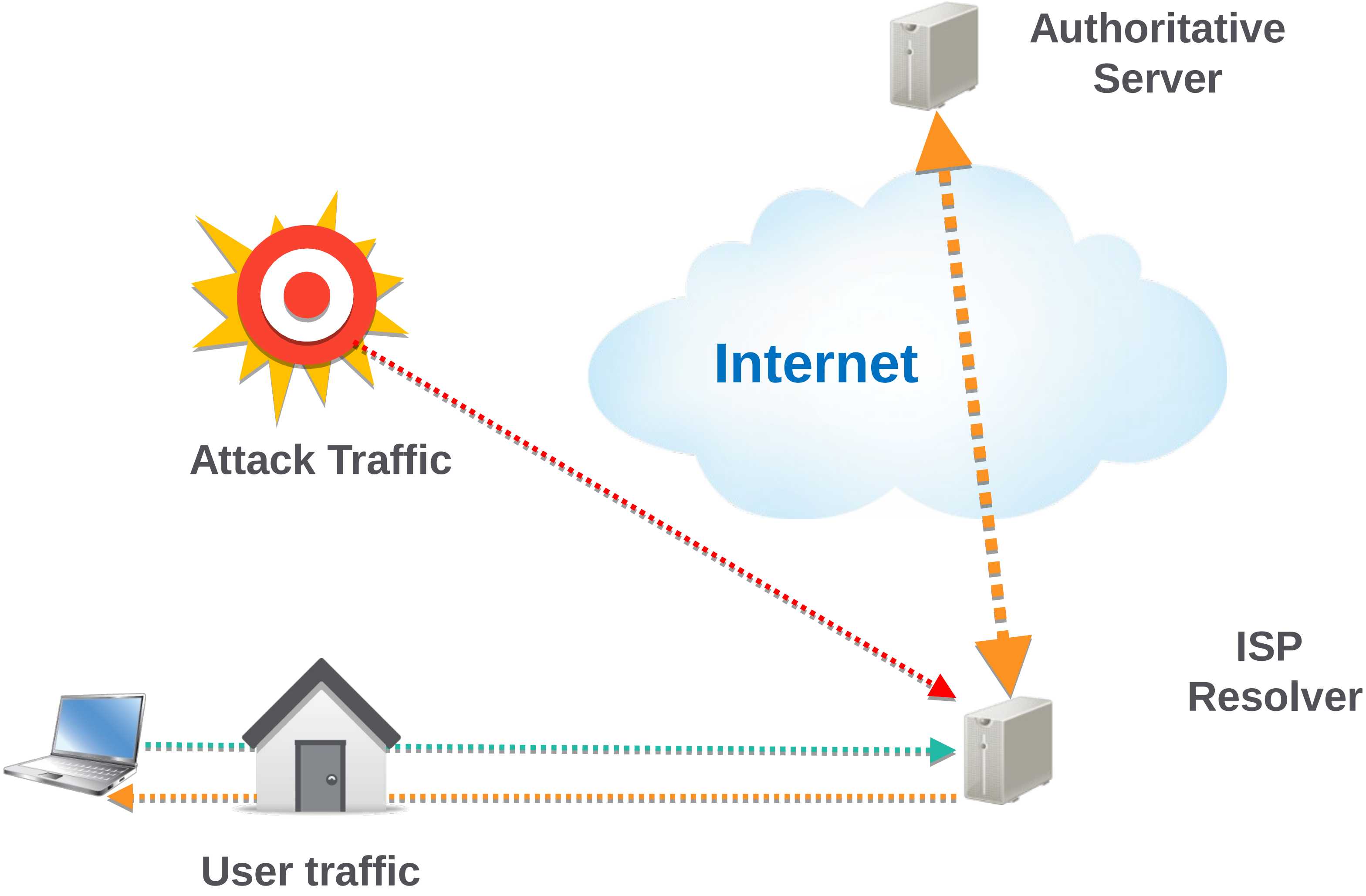
Traditional approaches are ineffective

- Filtering DNS (port 53) at borders
- In-place DDoS equipment
- Scripts

DNS defenses

- Ingress filtering at resolvers
- Rate limiting queries to authoritative servers

Testing efficiency of rate limiting



Setup for testing efficiency

- Auth Server only answer a certain rate (e.g 100qps)
- Normal User traffic gets 100% replies
- Insert Attack Traffic
- This will overflow the auth server rate
- Measure good replies

Challenge: Protecting Good Traffic

Example: Recent attack on Amazon.co.uk

Blocking amazon.co.uk queries won’t work!

Blocklists and whitelists are needed

Protecting Good Traffic

- Whitelist to protect legitimate queries

www.appledaily.com.tw.
liebiao.800fy.com.
www.23us.com.
wuyangairsoft.com.

- Blocklist to eliminate malicious traffic

*.www.appledaily.com.tw.
*.liebiao.800fy.com.
*.www.23us.com.
*.wuyangairsoft.com.

Examples

Query: www.appledaily.com.tw.

Answered, protected by whitelist

Query: avytafkjad.www.appledaily.com.tw.

Blocked by blocklist

Query: www2.appledaily.com.tw.

Answered through normal resolution

Summary

- Constant DNS Based DDoS evolution
- Open Home Gateways remain a problem
- Malware-based exploits create broad exposure

- Not clear where attacks are headed
- Evidence attackers refining techniues
- Remediation needs to be undertaken with care