CLOUDFLARE

December 3, 2014

Nick Sullivan
@grittygrease

Splicing and Dicing 2014

Examining this year's Botnet attack trends

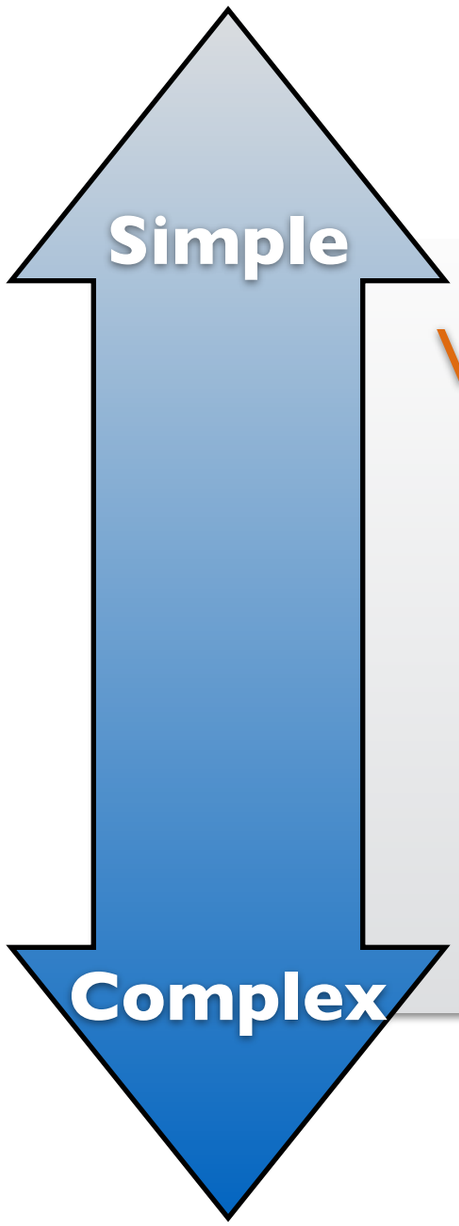
What this talk is about

- How bots are used to attack websites
- Examples of attacks
- New trends in 2014

What this talk is not about

- Malware analysis
- Botnet identification

Attack Landscape



Type	Attribution	Target
Volumetric DDoS	Low	Routers/Switches
DNS Flood	Medium	DNS Infrastructure
HTTP Flood	High	HTTP Server
Weaponized	High	Backend Software

CLOUDFLARE®

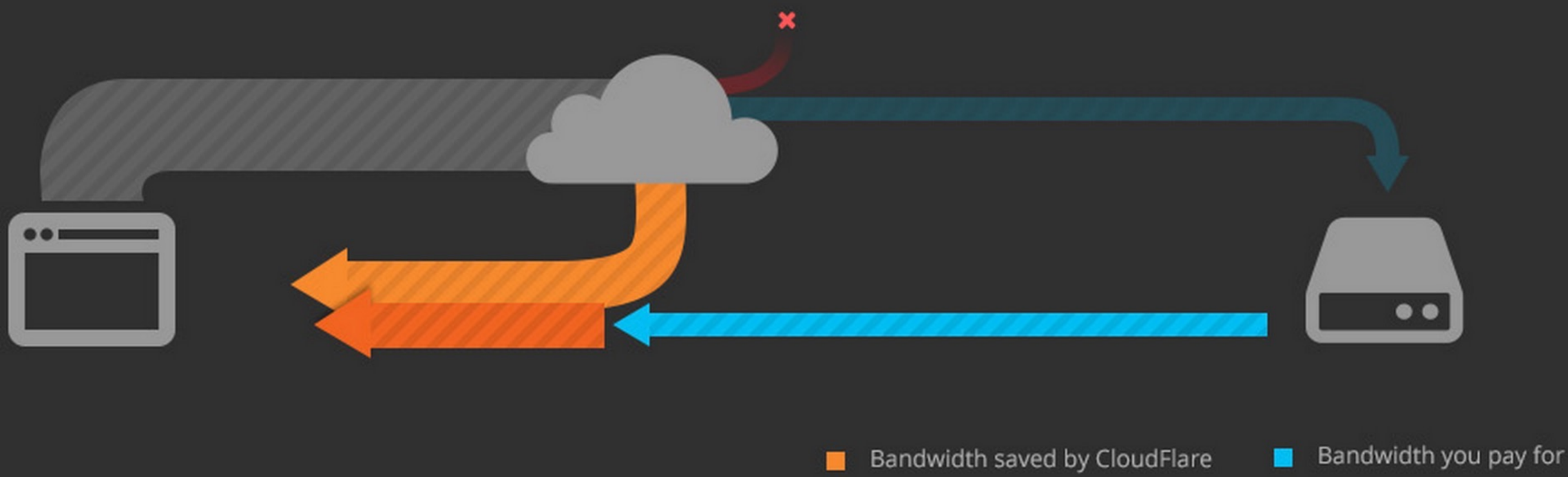
Building a Better Web

CloudFlare

- Website protection & acceleration
- DNS & HTTP(S)

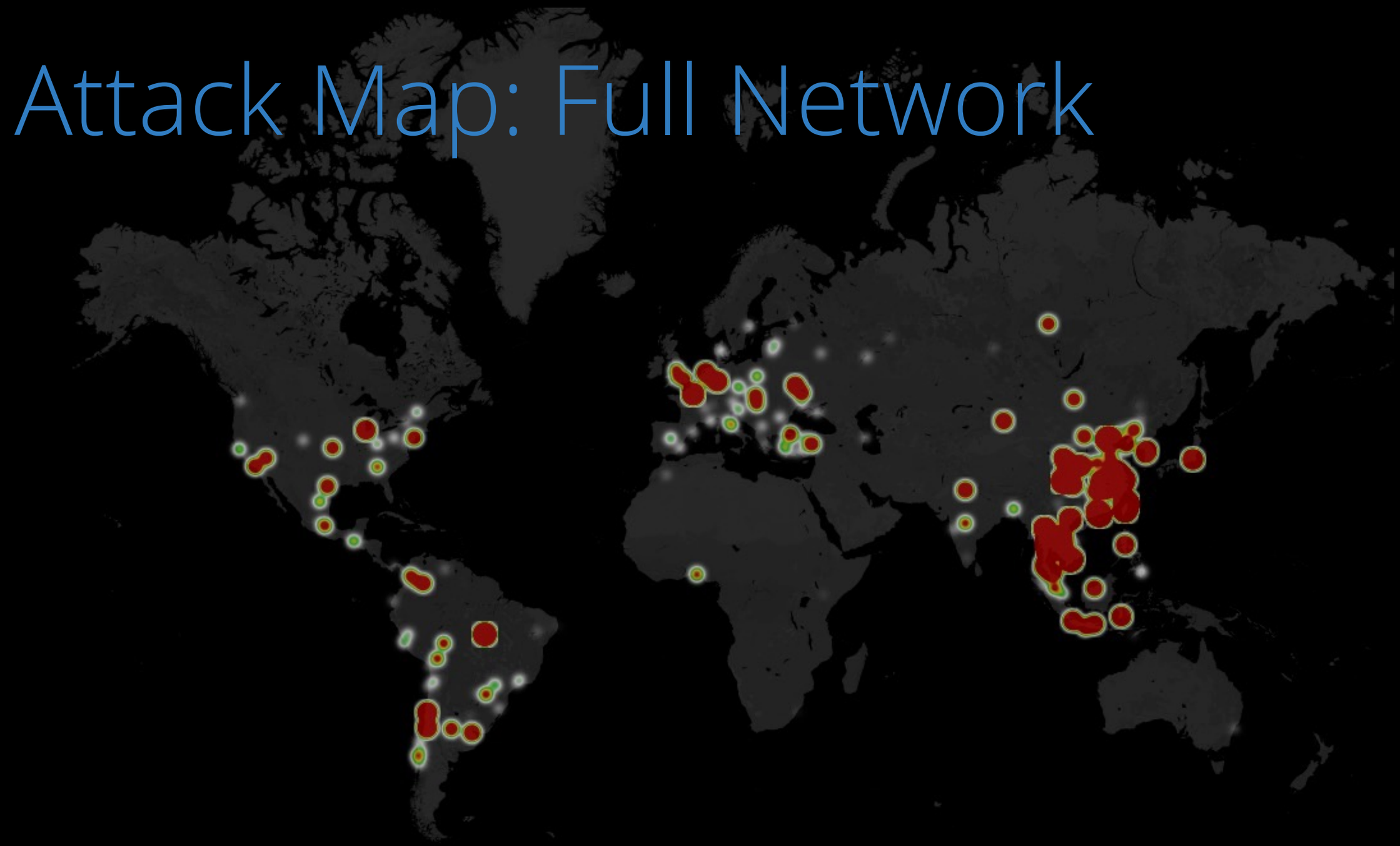
- Core technologies:
  - Reverse proxy
  - Anycast network

CloudFlare Reverse Proxy

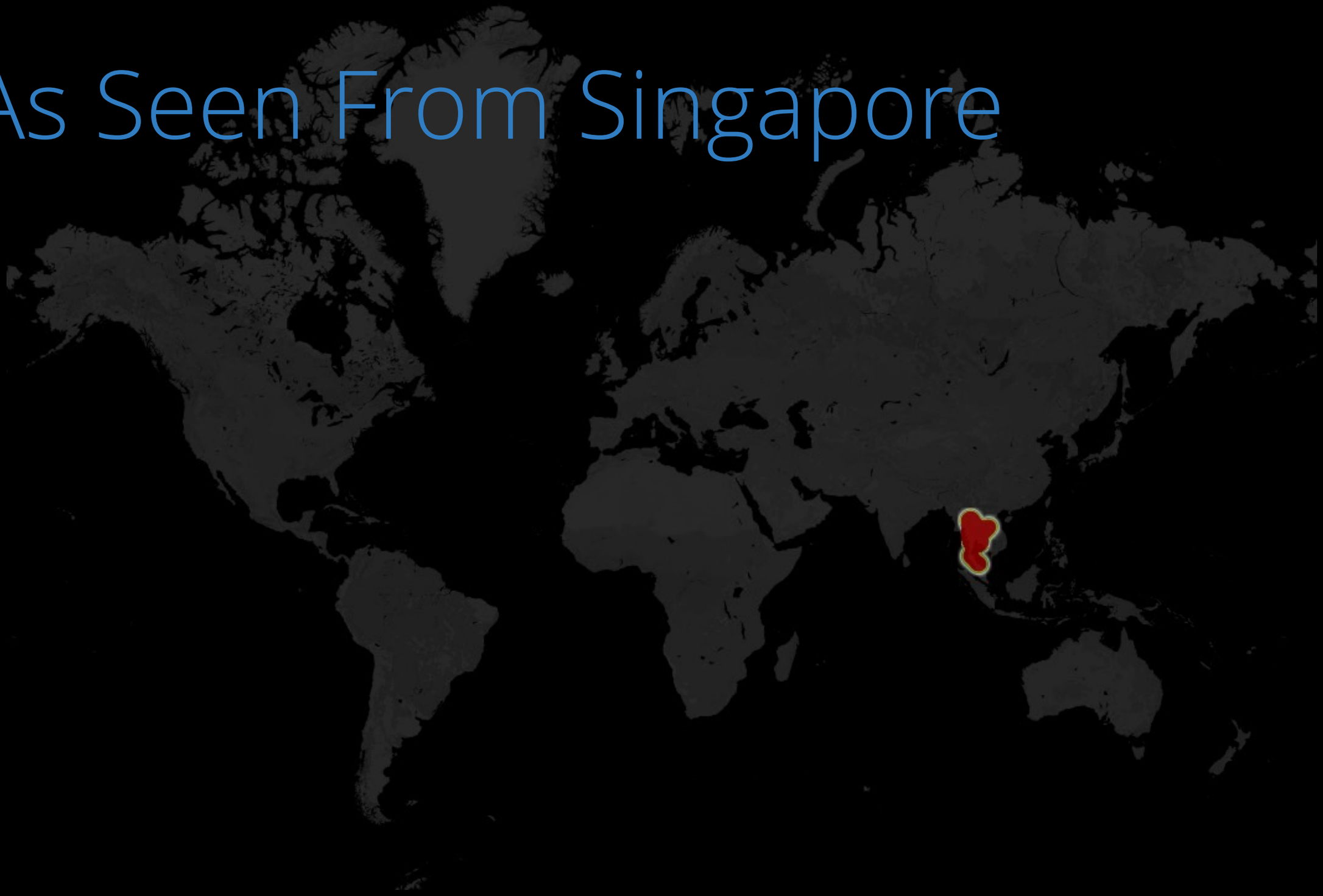


CloudFlare Anycast Locations

Attack Map: Full Network



As Seen From Singapore

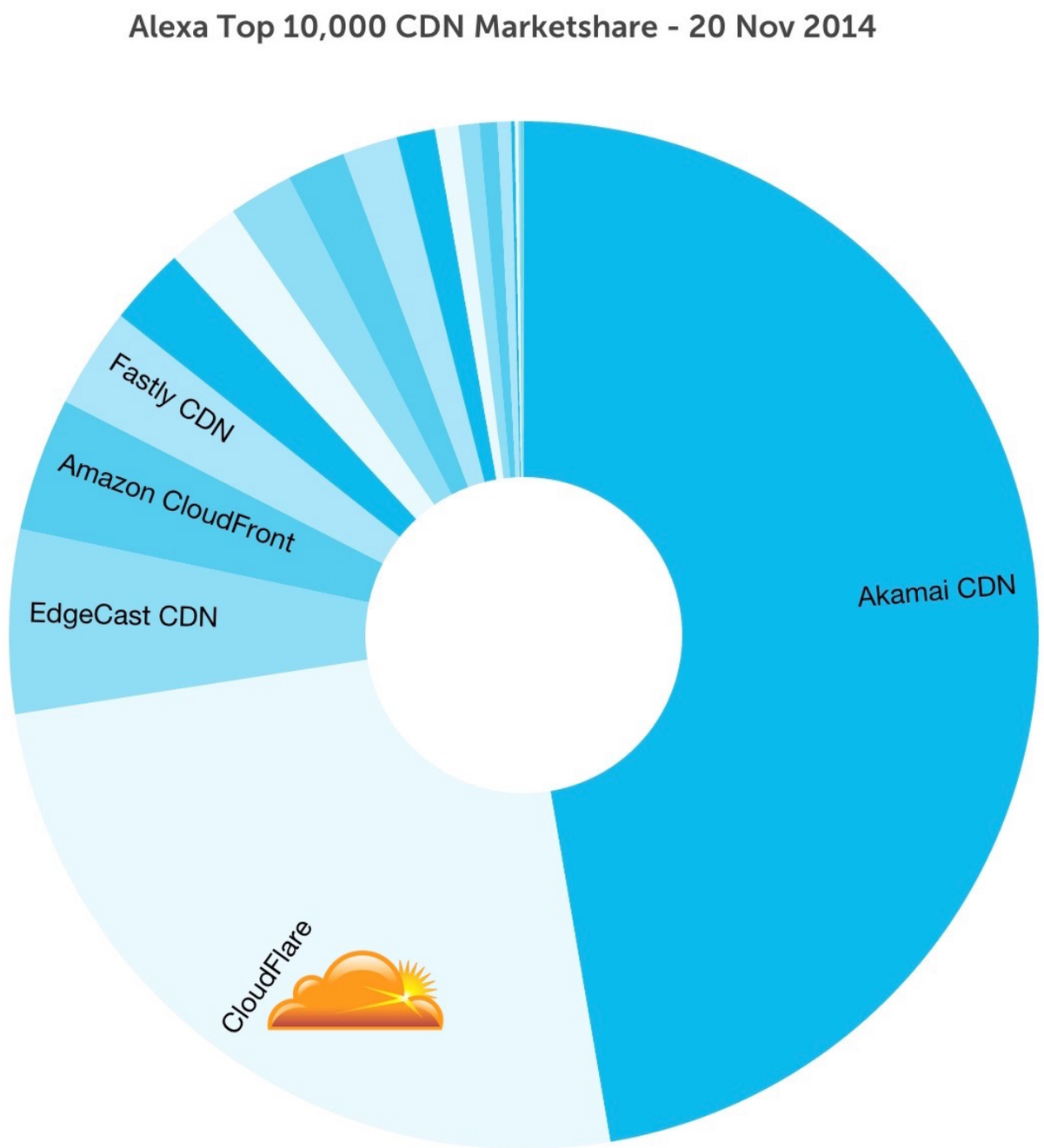


As Seen From Santiago

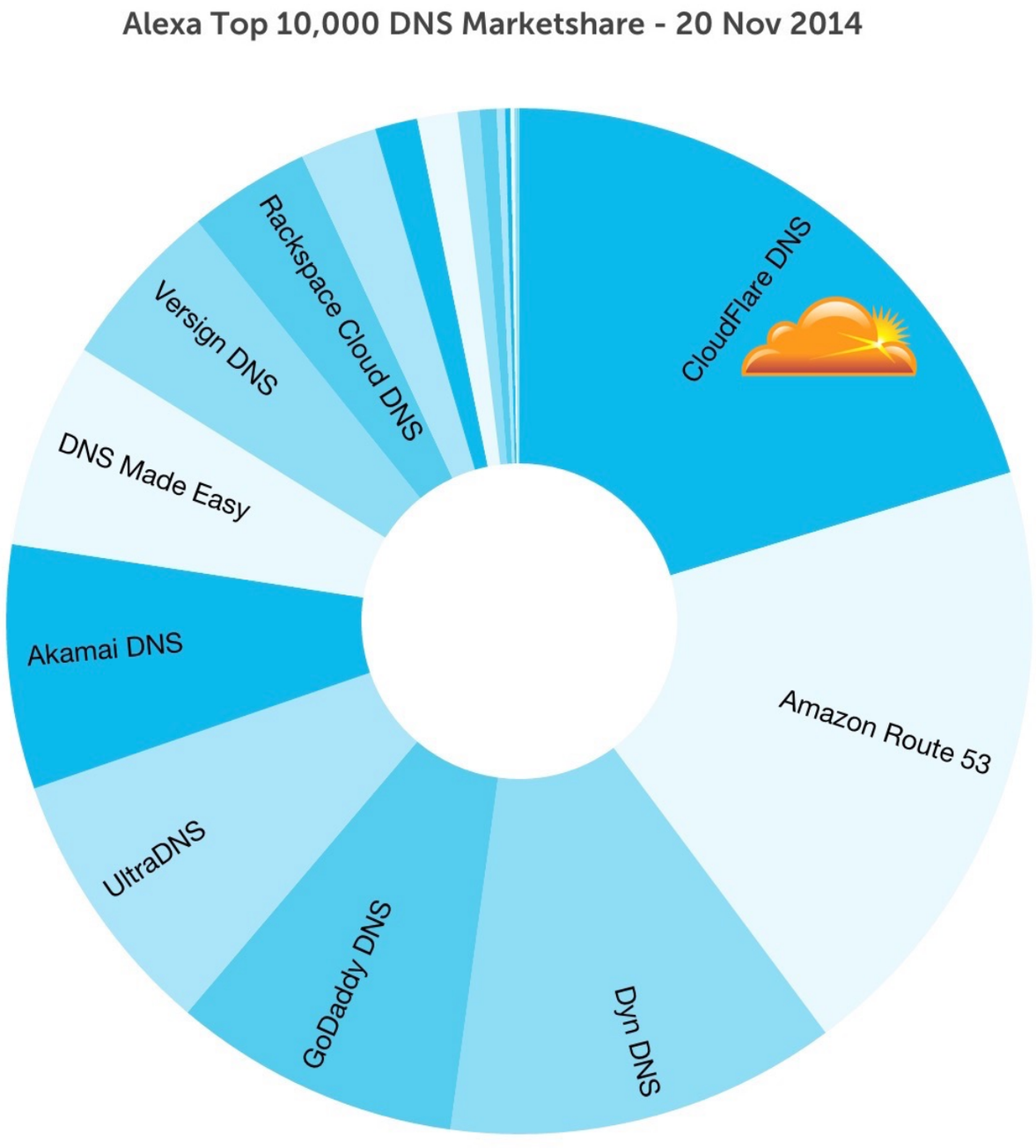
Not a “big data” company

- But we have a lot of data
- And we get attacked by botnets constantly

CDN or Reverse Proxy



Authoritative DNS



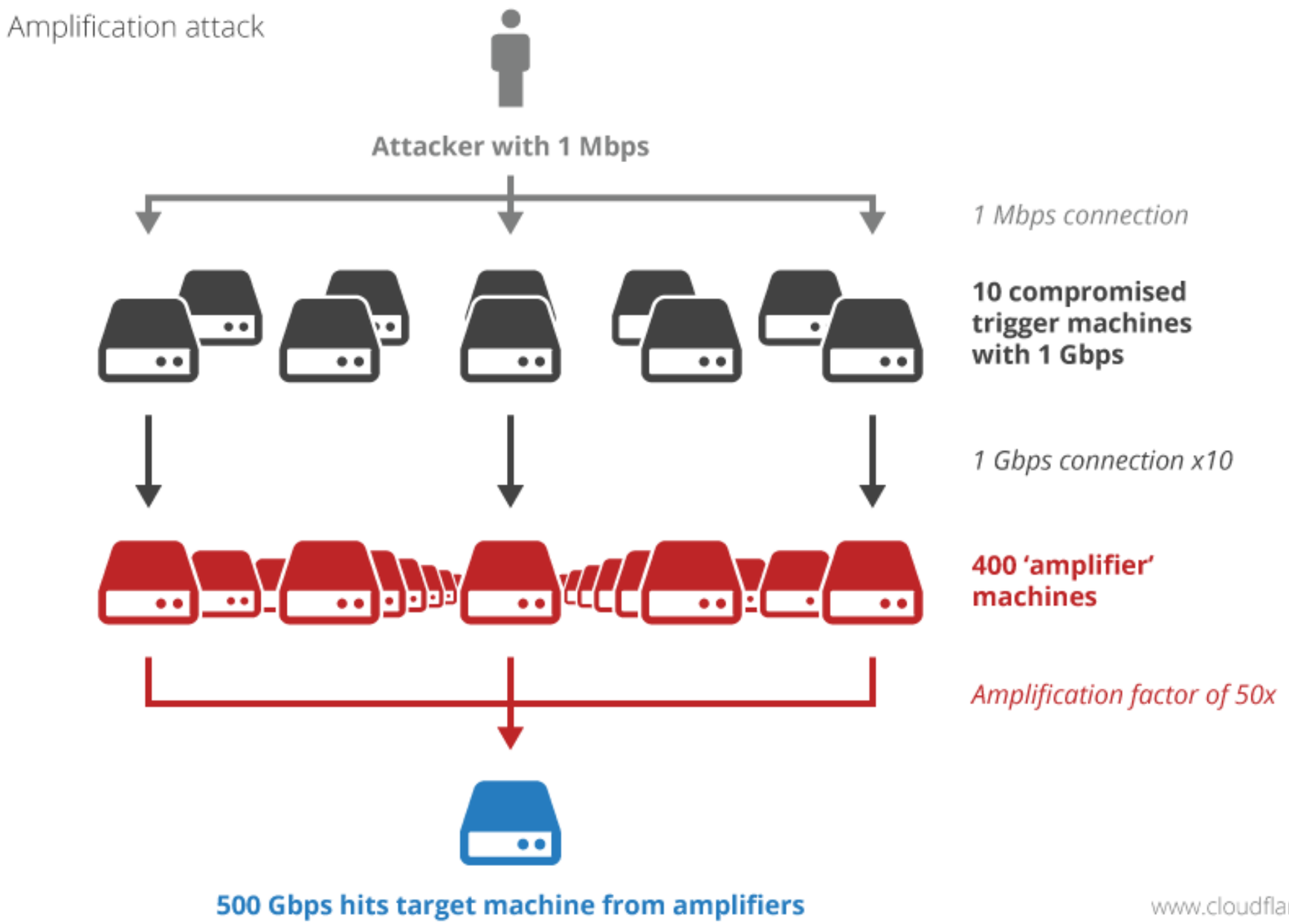
Volumetric DDoS Attacks

The brute force approach

Volumetric Attacks

- Large volume of traffic (number of IP packets, bytes)
- Goal: make a site unavailable through bandwidth exhaustion

Reflection & Amplification Attacks

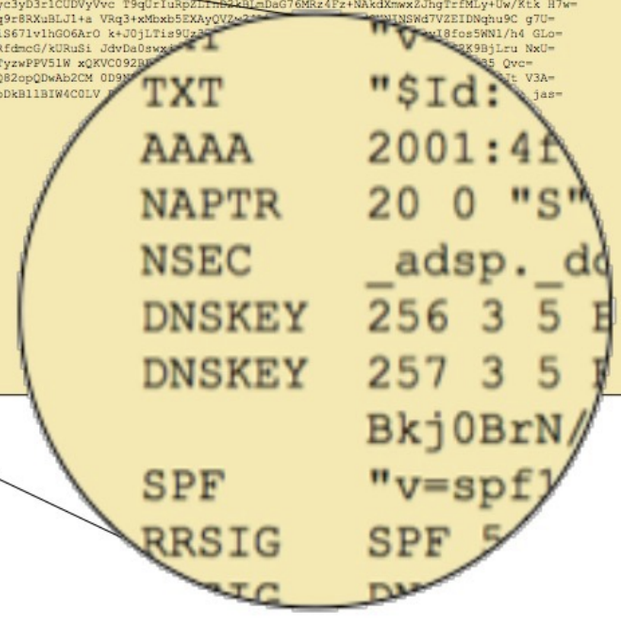


```
$ dig ANY isc.org @63.21*.**.** +edns=0 +notcp +bufsize=4096
```

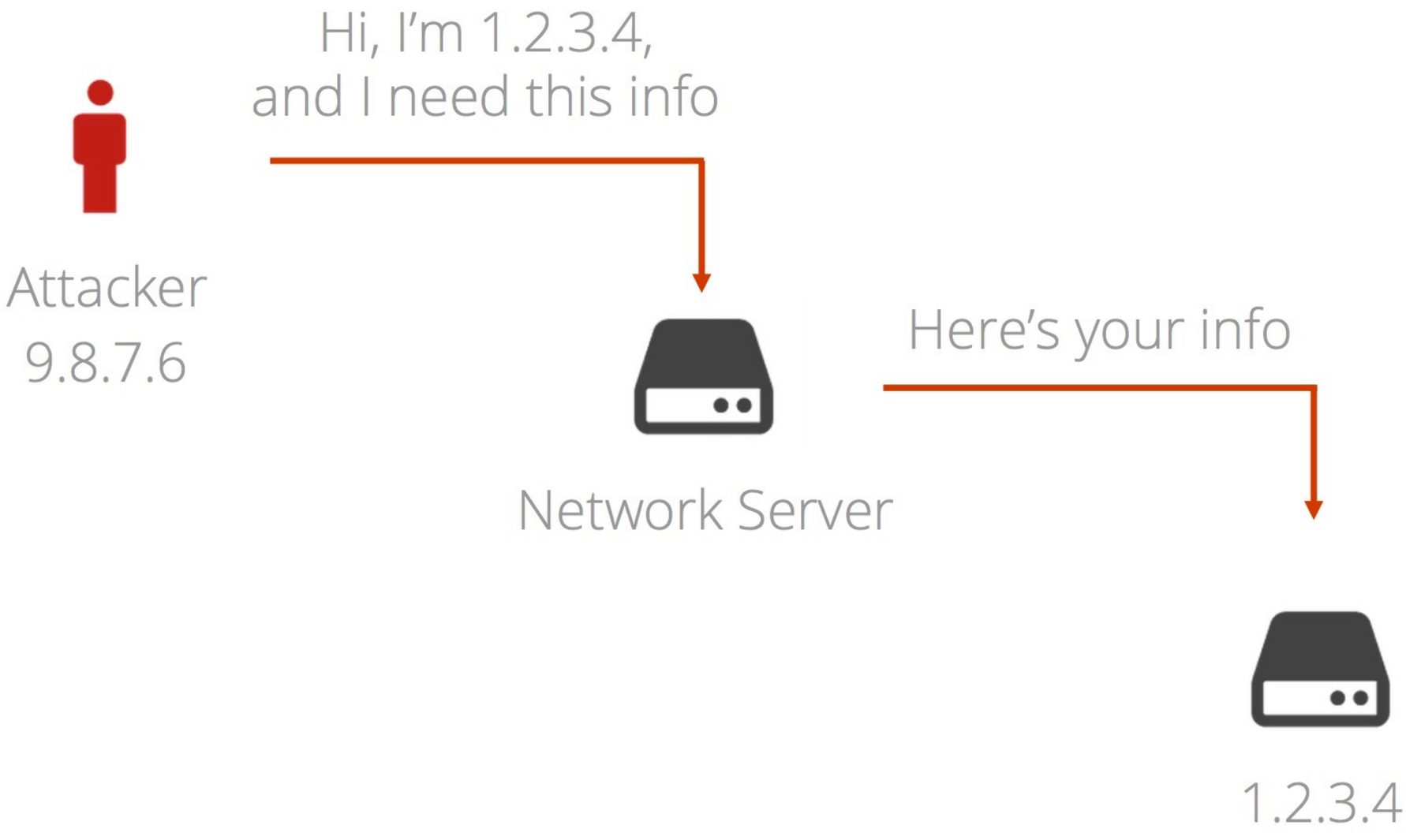
64 byte query

```
;; ANSWER SECTION:
isc.org.                7147    IN      SOA     ns-int.isc.org. hostmaster.isc.org. 2013073000 7200 3600 24796800 3600
isc.org.                7147    IN      NS      ns.isc.afilias-nst.info.
isc.org.                7147    IN      NS      ord.sns-pb.isc.org.
isc.org.                7147    IN      NS      ams.sns-pb.isc.org.
isc.org.                7147    IN      NS      sfba.sns-pb.isc.org.
isc.org.                7       IN      A       149.20.64.69
isc.org.                7147    IN      MX      10 mx.paol.isc.org.
isc.org.                7147    IN      TXT     "v=spf1 a mx ip4:204.152.184.0/21 ip4:149.20.0.0/16 ip6:2001:04F8::0/32 ip6:2001:500:60::65/128 ~all"
isc.org.                7147    IN      TXT     "$Id: isc.org,v 1.1835 2013-07-24 00:15:22 dmahoney Exp $"
isc.org.                7       IN      AAAA    2001:4f8:0:2::69
isc.org.                7147    IN      NAPTR   20 0 "S" "SIP+D2U" "" _sip._udp.isc.org.
isc.org.                3547    IN      NSEC    _adsp._domainkey.isc.org. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY SPF
isc.org.                7147    IN      DNSKEY  256 3 5 BQEAAAADwuHz9Cem0BJ0JQTO7C/a3McR6hMaufljs1dfG/inaJpYv7vH XFrAGm/MeXpt/x6eT4QLru0KoZkvZJnqTI8JyaFTw2OM/ItBfh/hL2lm Cft2O7n3MfeqYtvjPnY7dWghYW4sVfH7VVEGm958o9nfi79532Qeklxh x8pXWdeAaRU=
isc.org.                7147    IN      DNSKEY  257 3 5 BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hWLDMvoOMRXjGr hhCePvAZih7yJHf8ZGWGn43RhXG/xylYCO6Krpbdojwx8YMXLA5/kA+ u50WILBZR1R6KTbsYVMf/Qx5RiNbPC1w+vT+U8eXEJmO20jIS1ULgqy3 47cBBlzMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/zZrQz
                        Bkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix5WcJt+xzqZ7+ysyL KOOedS39Z7SDmsn2eA0FKtQpwA6LXeG2w+jxmwJuA81VUgEf/rzeC/bB yBNsO70aEFTd
isc.org.                7147    IN      SPF     "v=spf1 a mx ip4:204.152.184.0/21 ip4:149.20.0.0/16 ip6:2001:04F8::0/32 ip6:2001:500:60::65/128 ~all"
isc.org.                7147    IN      RRSIG   SPF 5 2 7200 20130828233259 20130729233259 50012 isc.org. XDoOYzkTHEV1W1V4TT50SsqXn4cxNhPvEuz3iFjq/oskLY9UOaK4GYDO GqHAjwnT8t6pUakKTQ3GvBjUBufPcEauCO17L7kb8/cC6zYifUCoW0pS moiQxmyqfrPDTzyVA894myUONGgMmB6QW68HGPVvc6HzGWx9bOmjvFyX uOs=
isc.org.                7147    IN      RRSIG   DNSKEY 5 2 7200 20130828230128 20130729230128 12892 isc.org. COfF8fU6a8TBUG97SI/X+u2eKv7/mw+ixD3IWBnr3d3cWZmzFlsV8bWT YbuJebwnJMgN5OEB9PLeN+4QT617OjBeldUF2M9jZeBiWsSsvvrdHnHM P8KwX6eayByDUoFsYe9VAH6C94Xm0VXTQ7h7Cr0ytaVSXUytqFZV+DGn
                        v3kqSi50V3YkFNPAJDqqs0treWjwV/SPlqWVqEAoU/KMZMtYpCEMbHVP 8nbRP3jj/10WLccPtjHhiw4Ka9Sk4o+b7BMYCgXGXlhaap2lSUqkytHt 8RJdVxxd5Cj7Bi+O4LXODlS4bA2EDG7UuHR7MzXtvMZogsNyyNUKHSs FtUvBg==
isc.org.                7147    IN      RRSIG   DNSKEY 5 2 7200 20130828230128 20130729230128 50012 isc.org. Mbr/QqJPoIuf3K5jCuABUIG0/zSHQ8iWZpqvHx7olVBEmTxhi3/vW+IE DW6VCE1EpZc1SI1MMRZUnbBnVSpe0rZ13BxoL1RQqVmb63jD15Se41WB DscD0S63C0GLqI9IhSyVugtlpqhA3CaluSqtABHbAktPP05Rm00tST2Y A5Q=
isc.org.                3547    IN      RRSIG   NSEC 5 2 3600 20130828233259 20130729233259 50012 isc.org. V7G42xY7TY9wFlvsBlRFuJ2ror/QjftLoRrDCMfqFW6kb5Zswjkt5zho 4o2sIrylTqad68O+lMxrDcg+7c2D8Hdh84SC0DEkjunBXkGBtLtaJvO5 zMw4d/OqUY5O7wtkerybJwZeiHcFxIkMRIcvsPKJYZWKCdaaCWibne7c wls=
isc.org.                7147    IN      RRSIG   NAPTR 5 2 7200 20130828233259 20130729233259 50012 isc.org. gWDvD0KACaYgsCgtRS4iKkHBBidfJfqS4drUf4kuPX2Et19fjlYrqOQK QFB5kBrzJLKhlIF4YpV+KYVUF8213AtpsohpUH5Uyc3yD3rlCUDVyVvc T9qUrIuRpZLInB2kBLmDaG76MRz4Fz+NAkdXmwxZJhgTrfMLy+Uw/Ktk H7w=
isc.org.                7       IN      RRSIG   AAAA 5 2 60 20130828233259 20130729233259 50012 isc.org. dfzIoOVGT0MptTaPoua3tFwDxSpeuOg127QedlqLGTxKGN1ppV/bd6R0 WktMagZY9rSqmjfXNP1F3Q+7YeTpMssQhHqjE/tDoj9q9r8RXuBLJ1+a VRq3+xMbxb5EXAyQVZw2
isc.org.                7147    IN      RRSIG   TXT 5 2 7200 20130828233259 20130729233259 50012 isc.org. WtB3SYzcOKpNbOtBlnmtsIODCbB4Kiv/HBY24PTZyWF/3tI8l+wZ+/p MfJ/SblbAzT67DO5Rfx1Ohr8UlRKVa70oqinQp5+rqiS67lvlhGO6ArO k+J0jLTis9Ug
isc.org.                7147    IN      RRSIG   MX 5 2 7200 20130828233259 20130729233259 50012 isc.org. BSXC42oV6MCF0dX2icyxnvyijhy569BJCoanm5VrIIuiNeTeo261FQJx 7ofFCWa4fKOoa+EZ0qloNPfDiczStr8MmK8Lznu6+8IRfdmcG/kURuSi JdvDa0swx
isc.org.                7       IN      RRSIG   A 5 2 60 20130828233259 20130729233259 50012 isc.org. Gmb8tt8d7kxx4HsA8L6IdFYGGSJCA8PTWexUP3CBLna39e4a6gVzjoNd dEI7B5mySAujZBEXNx3dSagpjiTJYfMML8AY0uO0tgyjqaTyzwPPV51W xQKVC092
isc.org.                7147    IN      RRSIG   NS 5 2 7200 20130828233259 20130729233259 50012 isc.org. RBvXLeTH0726iKvElmBZYUE+AWG3s2YRxKxuCnrhg7o9qIQGKXvEXrb3 wJeC/74KY2FW+RRz4F0QxODnPm+frpWIPbCpRf0SUFDQ82opQDwAb2CM 0D9N
isc.org.                7147    IN      RRSIG   SOA 5 2 7200 20130828233259 20130729233259 50012 isc.org. iiDnH6tvmap0h2cdULI8Ihme+zbtQ2+D3ycKRqBc9TRfA0poNaaZ97aF 15EIKyIpjiVybkP2DNLm5nkpNsgA+Ur+YQ6pr0hZKzbDkB11BIW4C0LV

;; AUTHORITY SECTION:
isc.org.                7147    IN      NS      ns.isc.afilias-nst.info.
isc.org.                7147    IN      NS      ord.sns-pb.isc.org.
isc.org.                7147    IN      NS      ams.sns-pb.isc.org.
isc.org.                7147    IN      NS      sfba.sns-pb.isc.org.

;; ADDITIONAL SECTION:
ns.isc.afilias-nst.info. 56648  IN      A       199.254.63.254
ns.isc.afilias-nst.info. 56652  IN      AAAA    2001:500:2c::254
ord.sns-pb.isc.org.     31018   IN      AAAA    2001:500:71::30
ord.sns-pb.isc.org.     31018   IN      A       199.6.0.30
ams.sns-pb.isc.org.     31018   IN      AAAA    2001:500:60::30
ams.sns-pb.isc.org.     31018   IN      A       199.6.1.30
sfba.sns-pb.isc.org.    31018   IN      AAAA    2001:4f8:0:2::19
sfba.sns-pb.isc.org.    31018   IN      A       149.20.64.3
mx.paol.isc.org.        3547    IN      AAAA    2001:4f8:0:2::2b
mx.paol.isc.org.        3547    IN      A       149.20.64.53
_sip._udp.isc.org.      7147    IN      SRV     0 1 5060 asterisk.isc.org.
```

3,363 byte response



IP Spoofing


Hi, I'm 1.2.3.4,
and I need this info
Attacker
9.8.7.6
Network Server
Here's your info
1.2.3.4

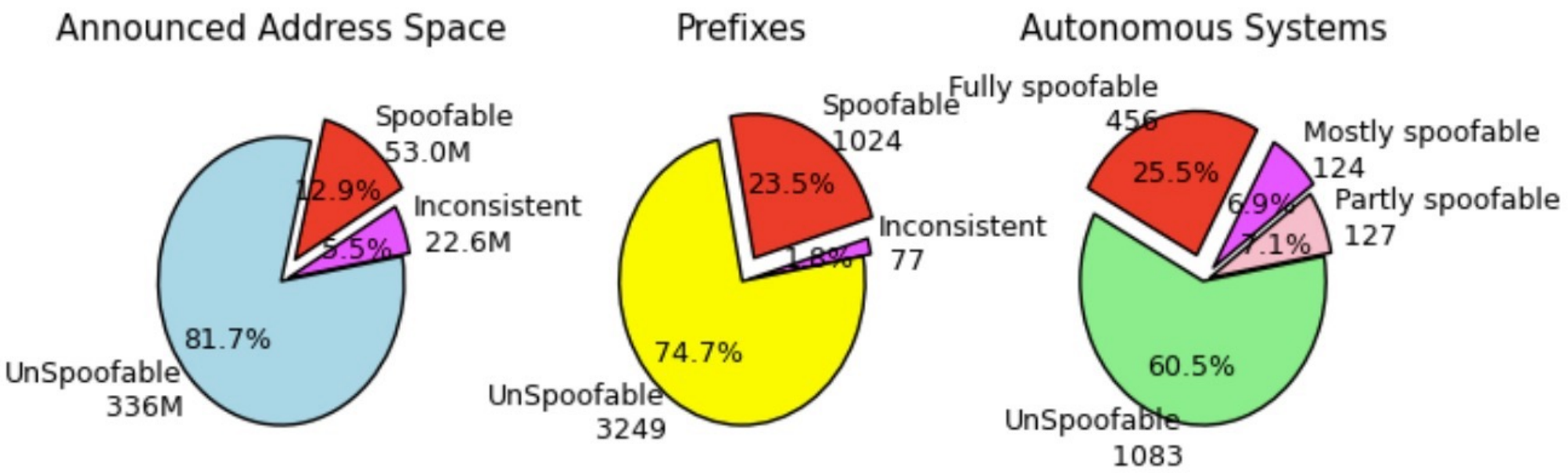
IP Spoofing

- BCP 38 — egress filtering blocks spoofed packets
- Botnets on networks that allow IP spoofing are more valuable

25% of networks allow IP spoofing

Summary:

Data Range: *Fri Feb 11 08:16:52 EST 2005 to Wed Feb 19 09:45:06 EST 2014*
Total Tests: *20426*
Unique IPs tested: *16200*
Unique Routed Prefixes tested from: *8866*
Unique ASes tested from: *2786*



http://spoofer.cmand.org/

Trends

- DNS reflection attacks peaked in March 2013 (300Gbps+)

The DDoS That Almost Broke the Internet

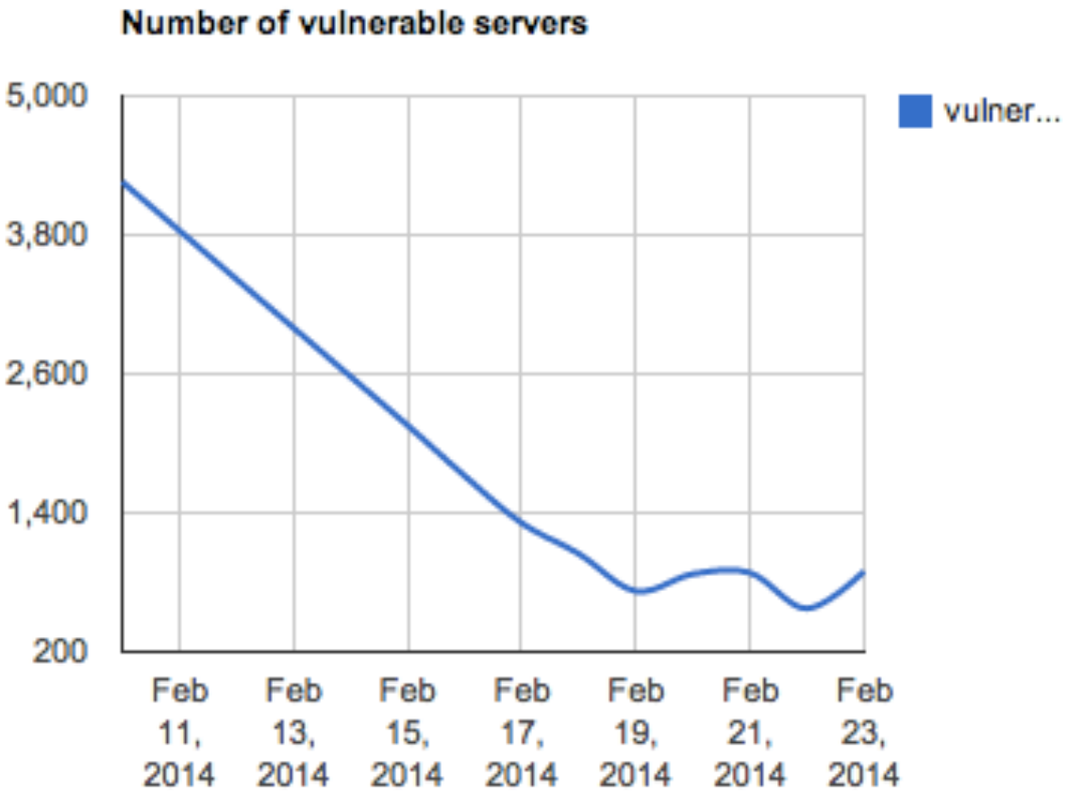
27 Mar 2013 by Matthew Prince.

Trends

- NTP reflection attacks peaked in February 2014 (400Gbps+)
- ~200x amplification

Trends

- NTP reflection attacks continue
- Smaller size due to misconfigured servers being shut down



History/Future

- 2013
  - DNS (5-50x amplification)
  - March: Spamhaus (300+Gbps)
- 2014
  - NTP (~200x amplification)
  - February: NTP attack (400+Gbps)
- 2015
  - SNMP (650x) ???
  - 600+Gbps ???

DNS Infrastructure Attacks

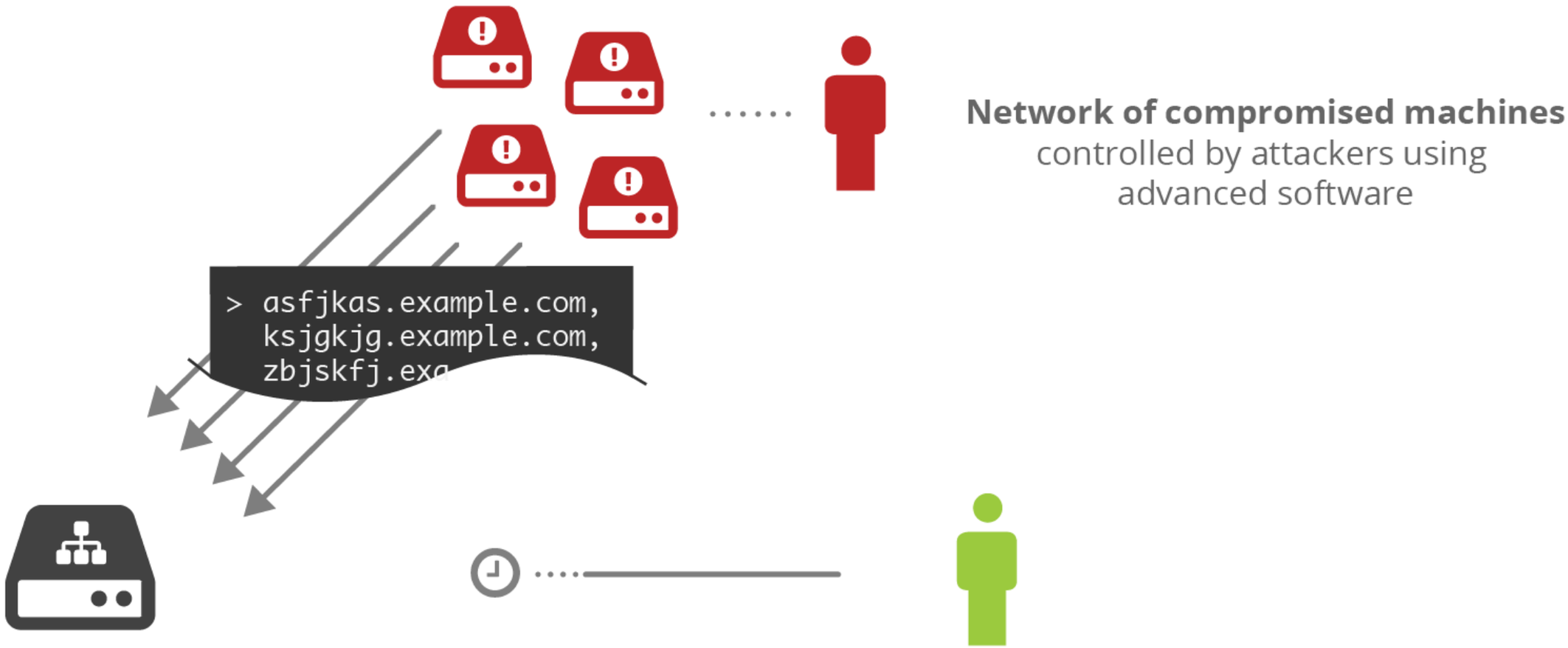
Taking down the name servers

DNS Infrastructure Attacks

- Massive flood of DNS requests
- Started in January 2014
- DNS resolver cache-busting

DNS Infrastructure Attacks

- New trend in 2014

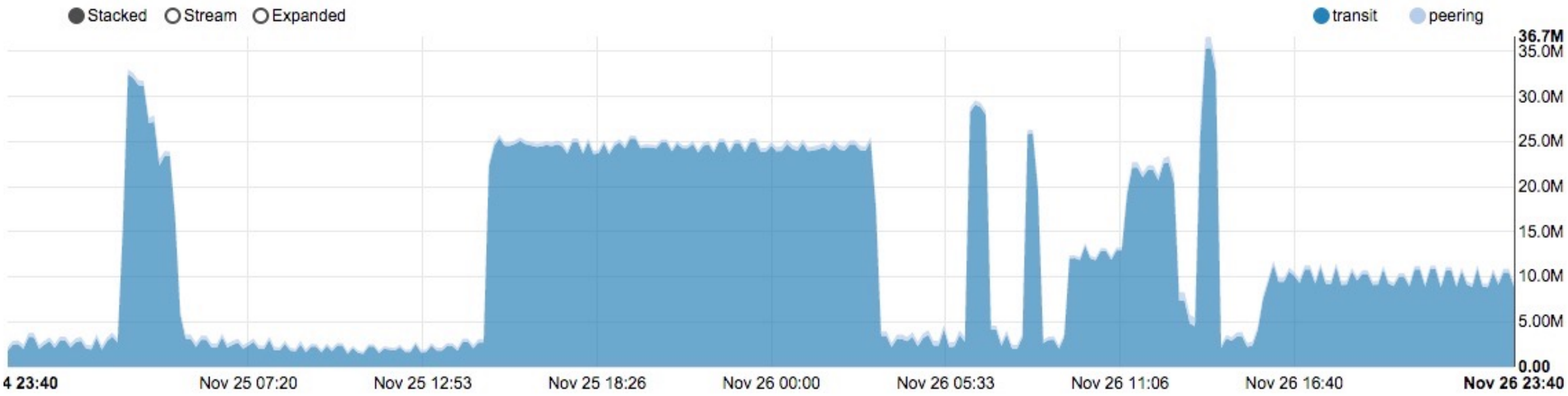


DNS Infrastructure Attacks

1. Frequency & Duration
2. Characteristics
3. Source
4. Trends

DNS Infrastructure Attacks - Frequency & Duration

- Multiple attacks per day
- From less than a minute to several days



DNS Infrastructure Attacks - Characteristics

- Random Prefix
  - ask for “<random>.www.example.com”
  - rotating random prefix forces resolvers to overload authoritative servers
- Single hostname flood
  - ask for “www.example.com”
- Size
  - Upwards of 100 Gbps

DNS Infrastructure Attacks - Source

- Coming from correct AS for IP
- Random IP from within an AS (partial spoofing)
- Majority of attacks from mainland China

DNS Infrastructure Attacks - Trends

- 2014: First large (100Gbps+) random prefix floods
- 2015: Increased complexity and sophistication

HTTP Attacks

Brute force against web servers

HTTP Attacks

- Attacks on Layer 7 Infrastructure
- Not spoofable due to TCP
- Botnets used for bandwidth, anonymity, and cost

Case Study 1 - Russian TV Site

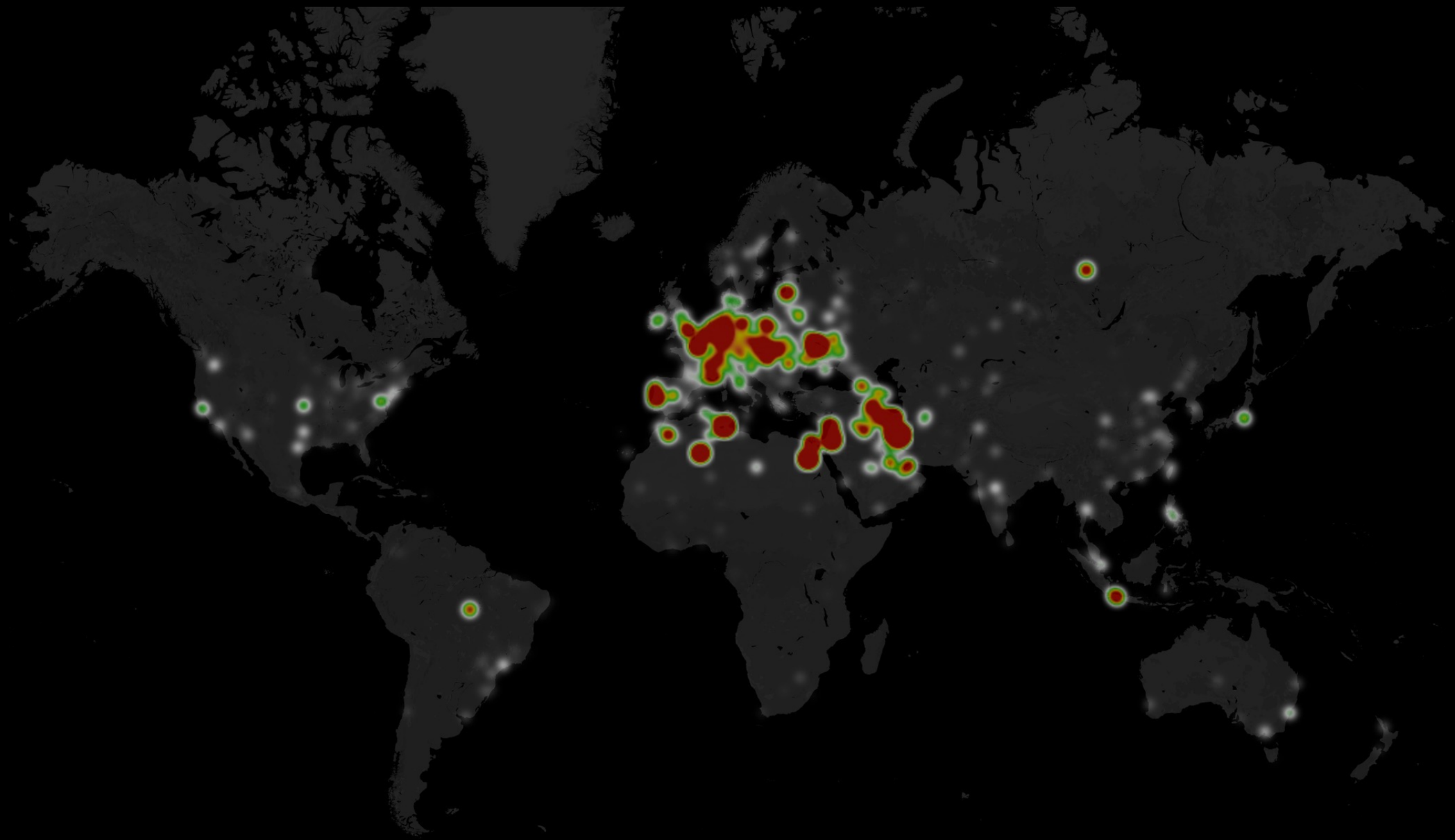
- August 2014
- HTTP GET with identical URI
- Geo distribution
  - Ukraine 32%
  - Russian 19%
- 160,000 requests/sec for over 24 hours

Case Study 2 - Turkish Site

Case Study 2 - Turkish Site

- November 2014
- HTTPS attack
- 96% of requests from Thailand
- Random URI attack
- https://www.site.com/<random>

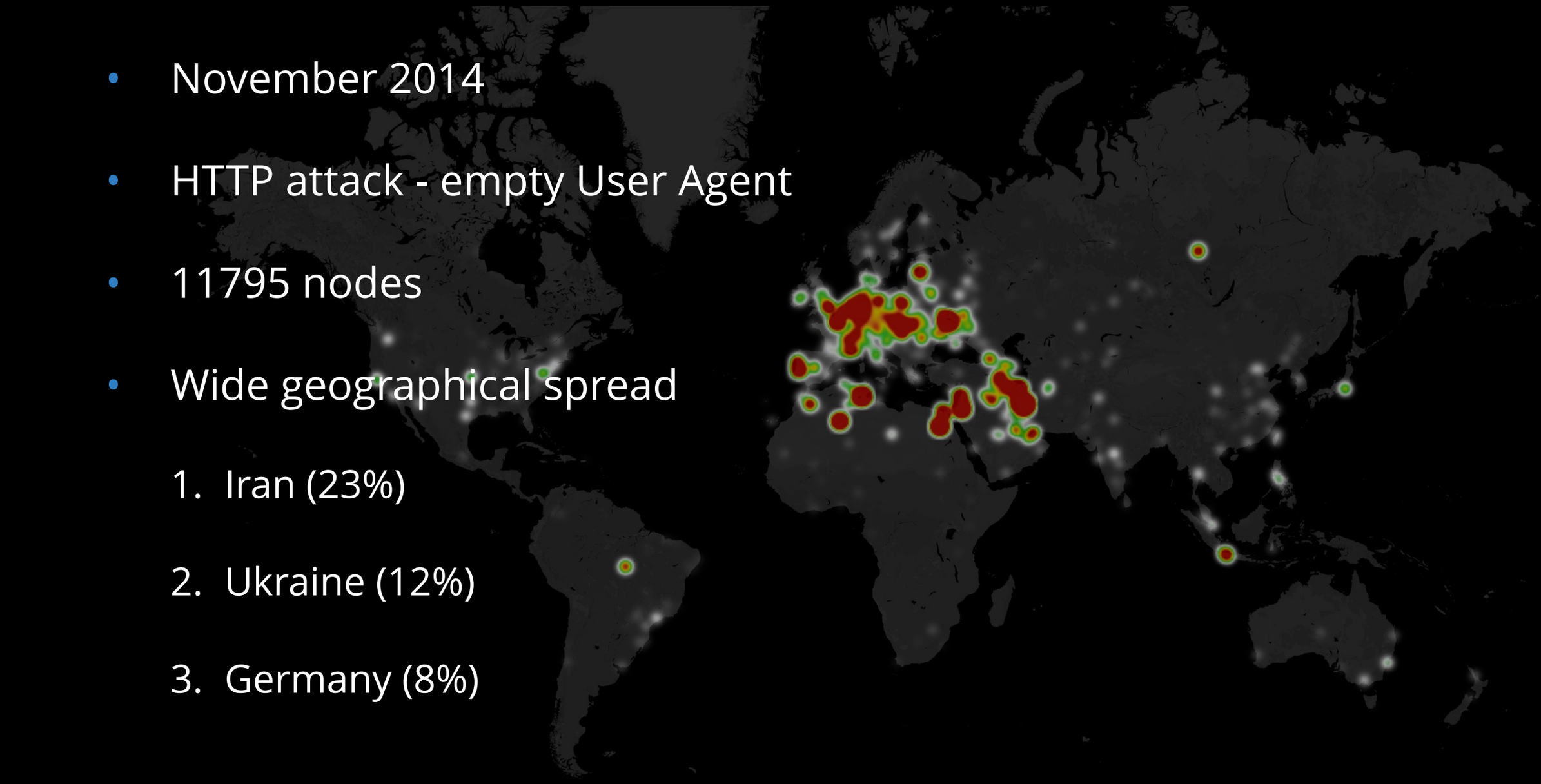
Case Study 3 - Geolocation service



Case Study 3 - Geolocation service

- November 2014
- HTTP attack - empty User Agent
- 11795 nodes
- Wide geographical spread

1. Iran (23%)
2. Ukraine (12%)
3. Germany (8%)



Case Study 4 - Fake ID site

Case Study 4 - Fake ID site

- HTTP attack
- Only 458 nodes
- 43% from China
- Random valid User Agents
  - Uniform distribution

Case Study 5 - AWS botnet

- September 13, 2014
- 40,000 nodes, 27,419 on Amazon Web Services
- 2 weeks before ShellShock released
- Not effective due to low volume

New trends

- Large botnets
  - Typically 1,000 to 10,000 nodes
  - Up to 50,000
- Unix botnets
  - Compromised cloud services
- Referer headers & User agent strings
  - Improved quality to mimic browsers

Potential trends

- IPv6 attacks
  - Less than 0.05% of attacks
- HTTPS cipher choices
  - Use expensive cipher suite in TLS connection (3DES)

Geographic breakdown

- Hard to definitively measure
- Many attacks are too small to notice
- Major November attacks: top countries (unique IPs)

1. Vietnam
2. China
3. Iran
4. United States
5. Phillipines

Weaponized Attacks

Exploiting backend vulnerabilities

Malicious Payload

- Requests sent to exploit vulnerability on server
  - ShellShock is major example
- 1.2 billion requests per day blocked by WAF

Shellshock

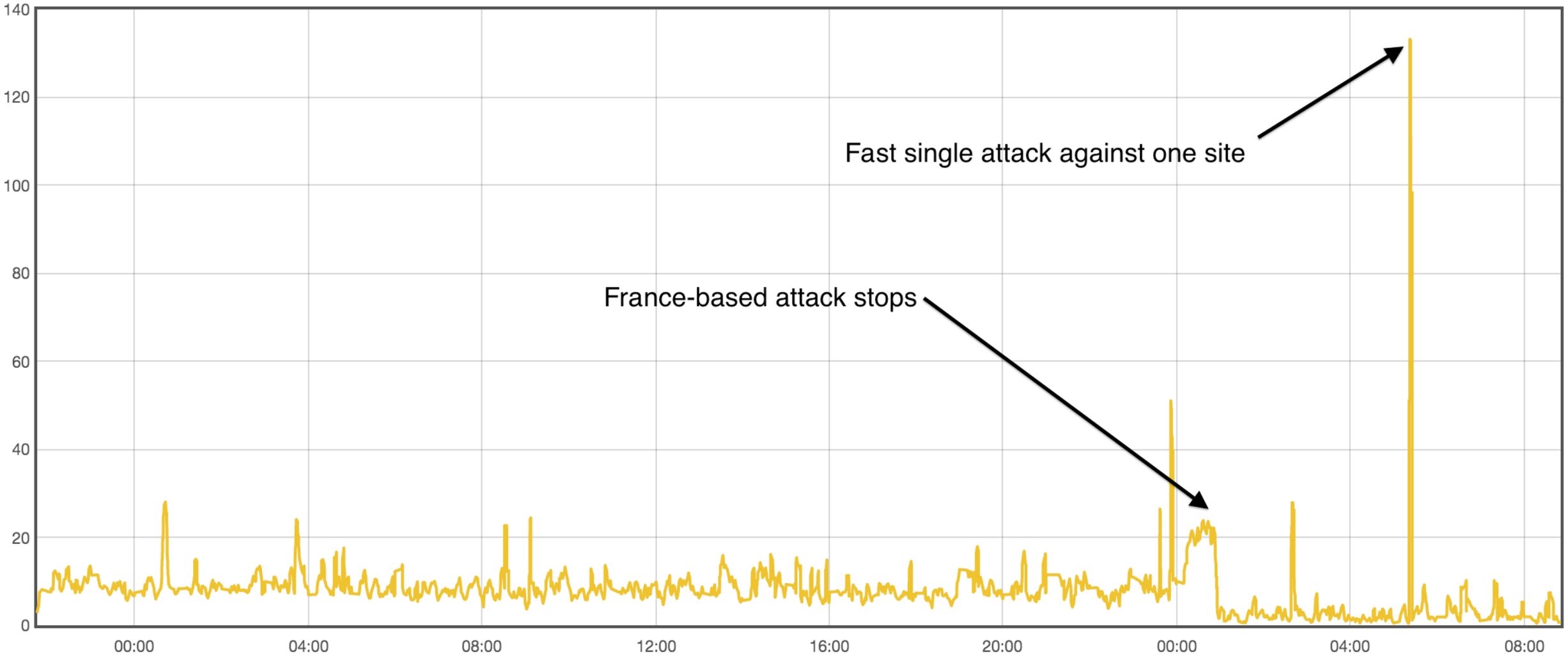
- 10 to 15 attacks per second during first week

Top Countries

1. France (80%)
2. US (7%)
3. Netherlands (7%)

Shellshock

- Attacks per second



Weaponized attack trends

- Classics still prevalent
  - SQLi
  - OWASP top 20
- Attacks start immediately after vulnerability announced
  - Heartbleed
  - Wordpress and Drupal vulnerabilities
  - Shellshock

Conclusions

Attacks are getting more sophisticated

- Volumetric DDoS evolving (NTP came and went)
- Larger botnets
- Cloud services used in botnets
- DNS floods on the rise
- Application-level attacks increasing
  - >1% of requests are malicious
- Politically motivated attacks

December 3, 2014

Nick Sullivan
@grittygrease

Questions?