



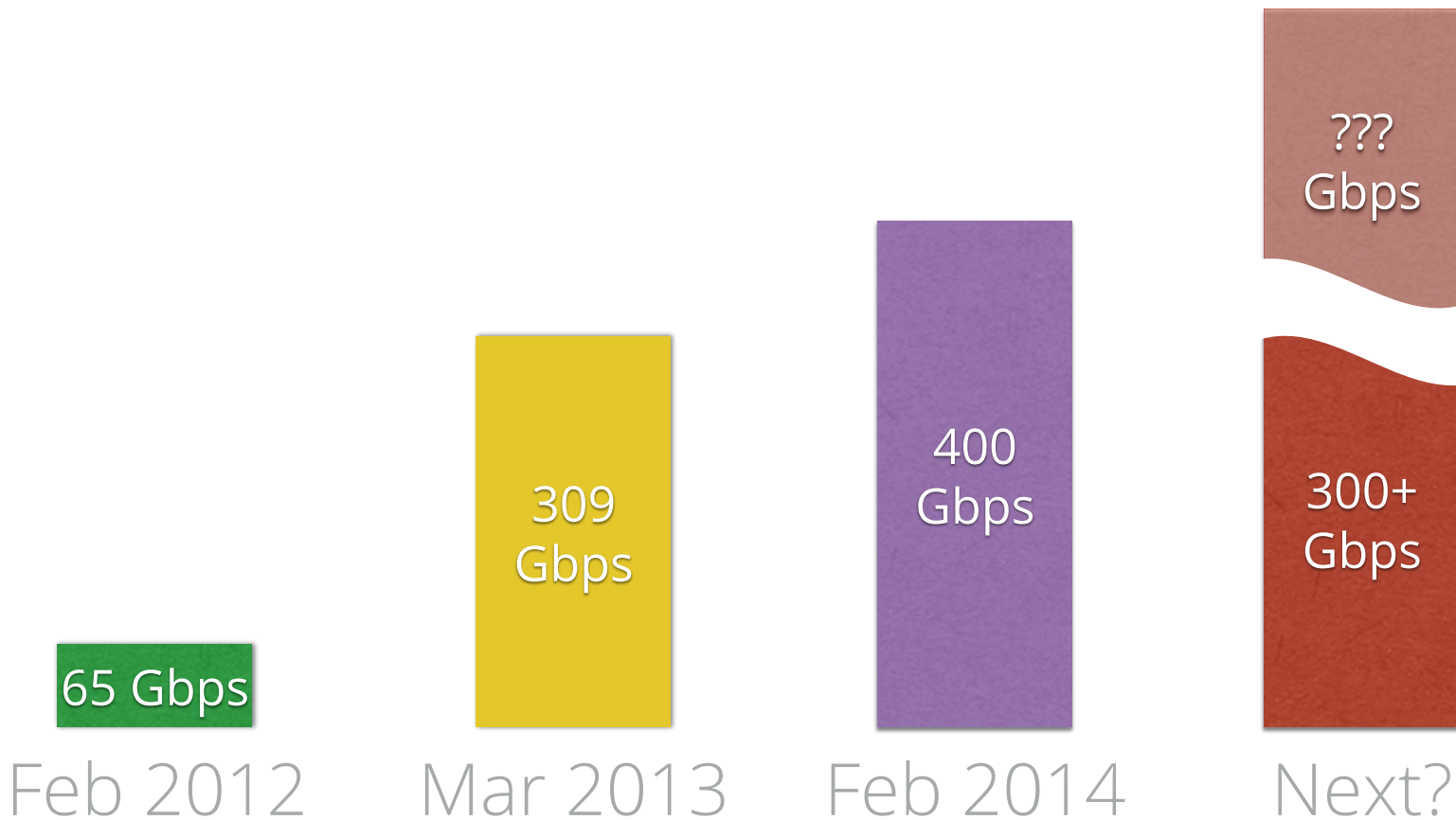
# Surviving a DDoS Attack: Securing CDN traffic at CloudFlare

ENOG8 Baku  
September 9, 2014

Martin J. Levy, Network Strategy  
[www.cloudflare.com](http://www.cloudflare.com)

DDoS Attacks are becoming massive, and easier to initiate

# Major Attacks against CloudFlare Customers



# CloudFlare

# CloudFlare core locations



# CloudFlare sample customers



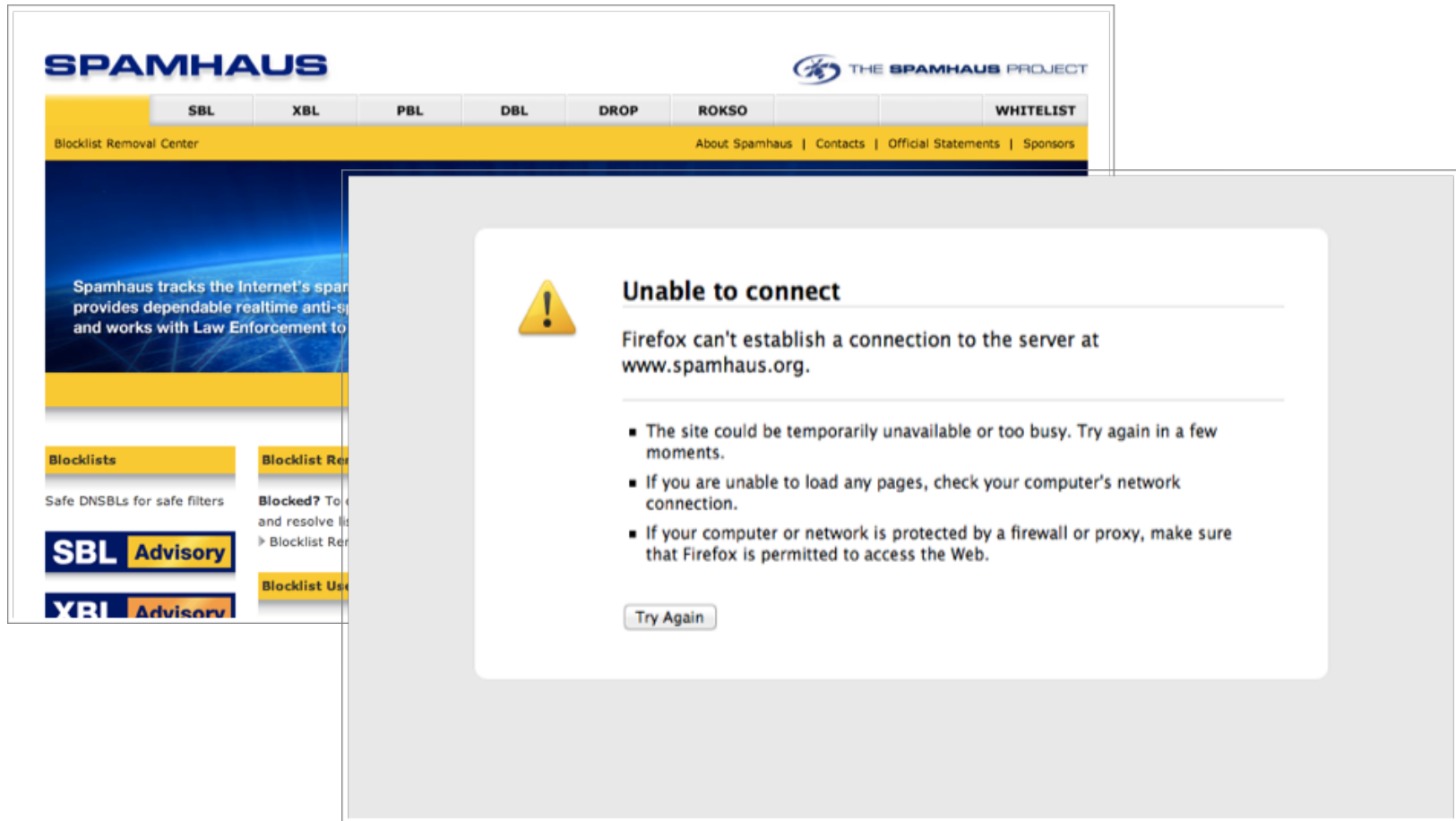
# 1.5 million customers

# Chronology of the major attacks



# March 2013

# The Spamhaus attack

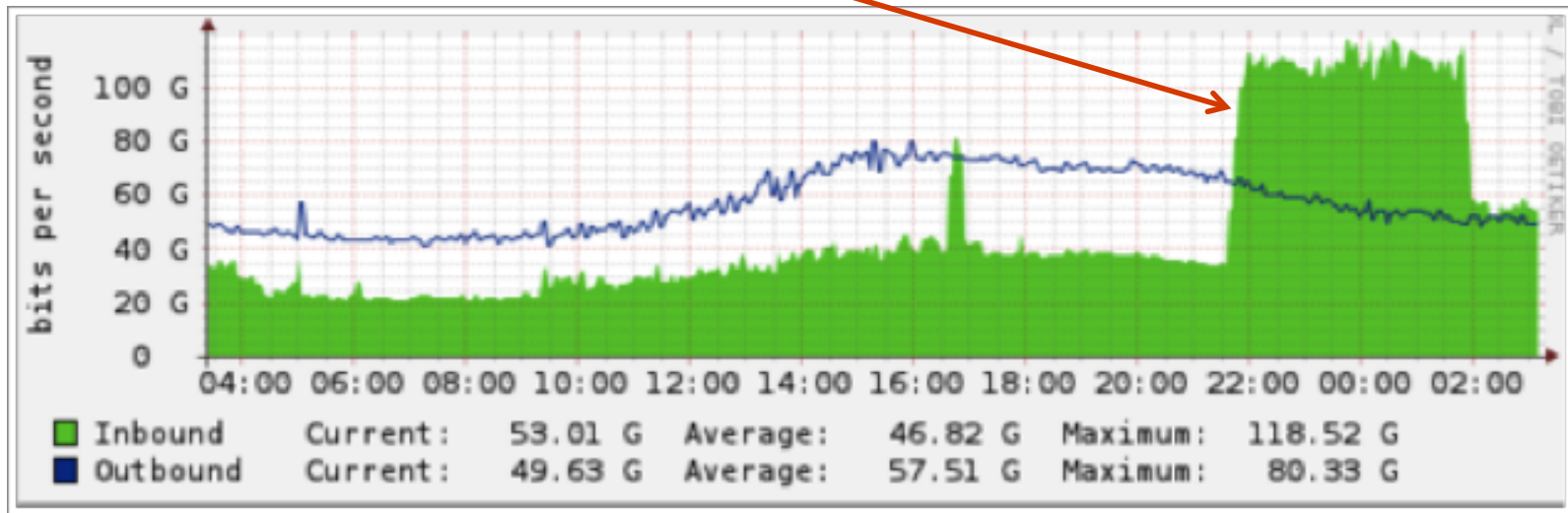


# Monday, March 18th thru 21st

“Annoyance” attacks, 10-80Gbps

# Wednesday, March 20th

“Instant on”

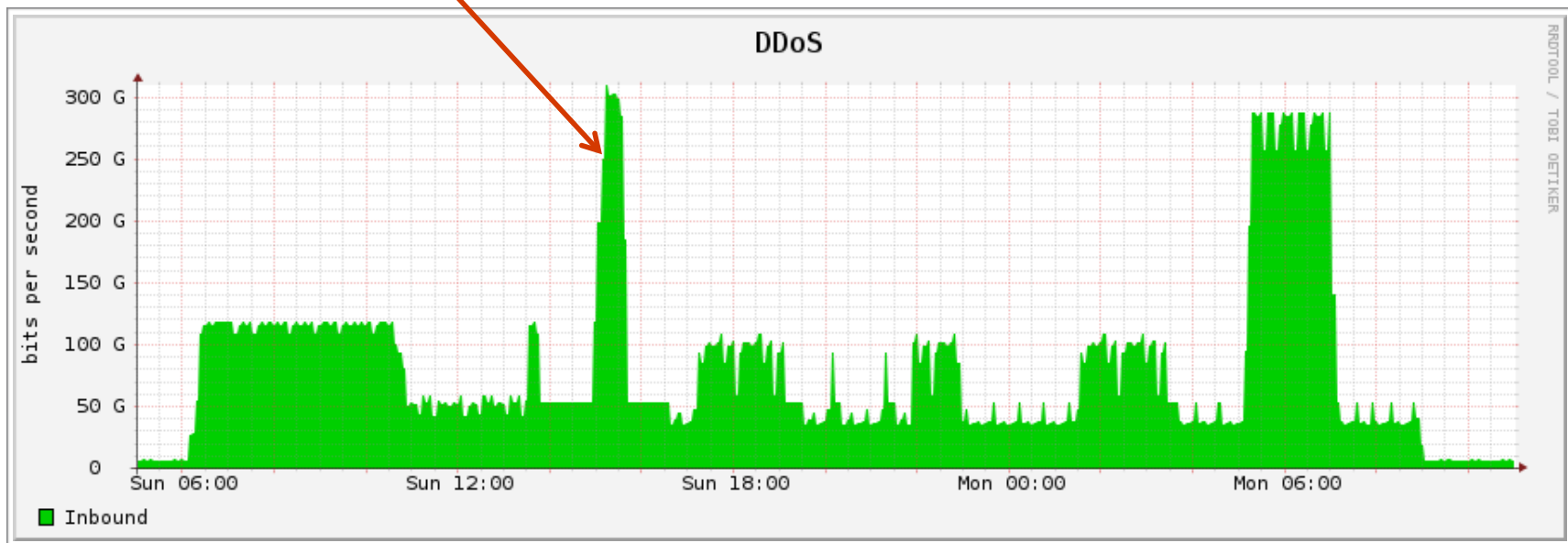


~75Gbps attack

Then, it got real ...

# Sunday, March 24th thru 25th

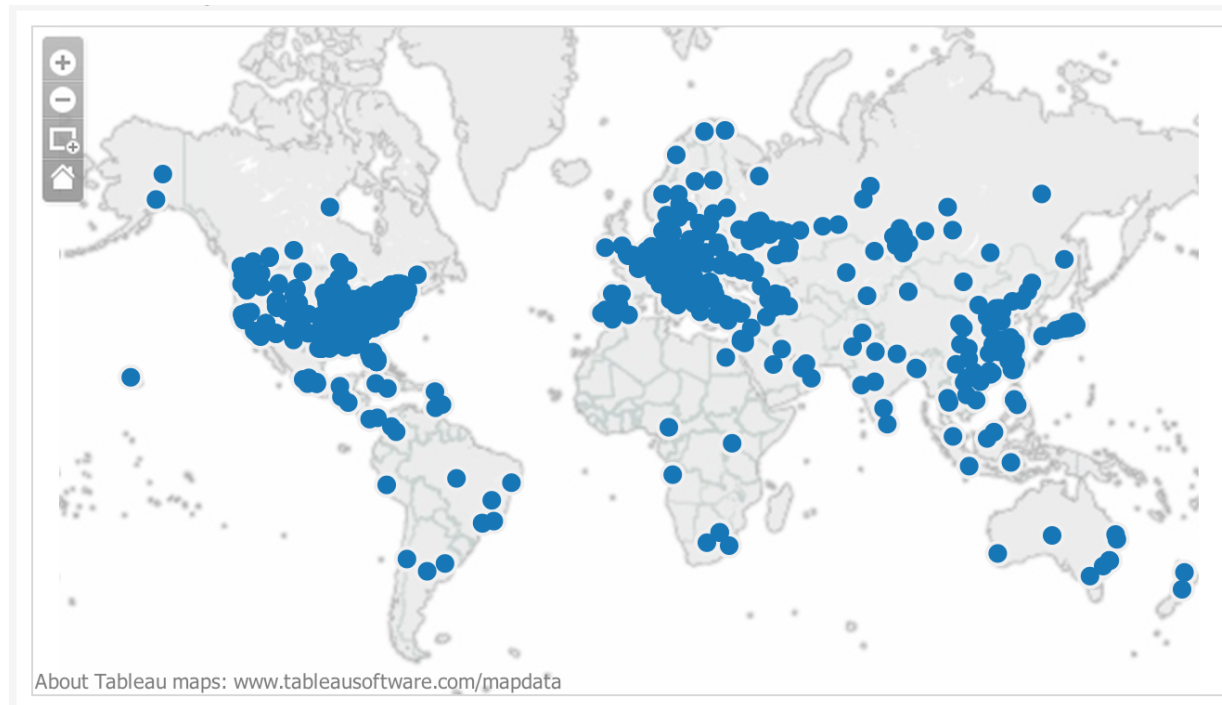
"Instant on"



Peaks of the attack reached 309Gbps

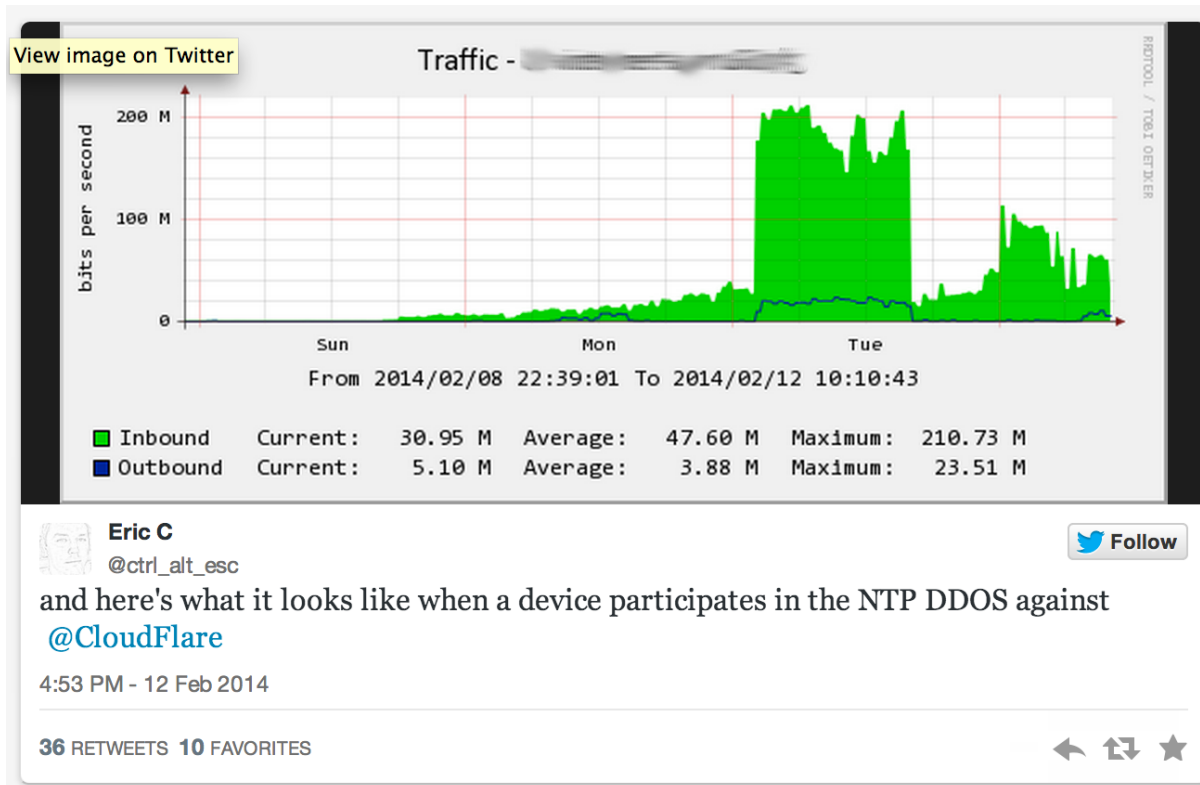
# February 2014

# Monday, February 10th, 2014

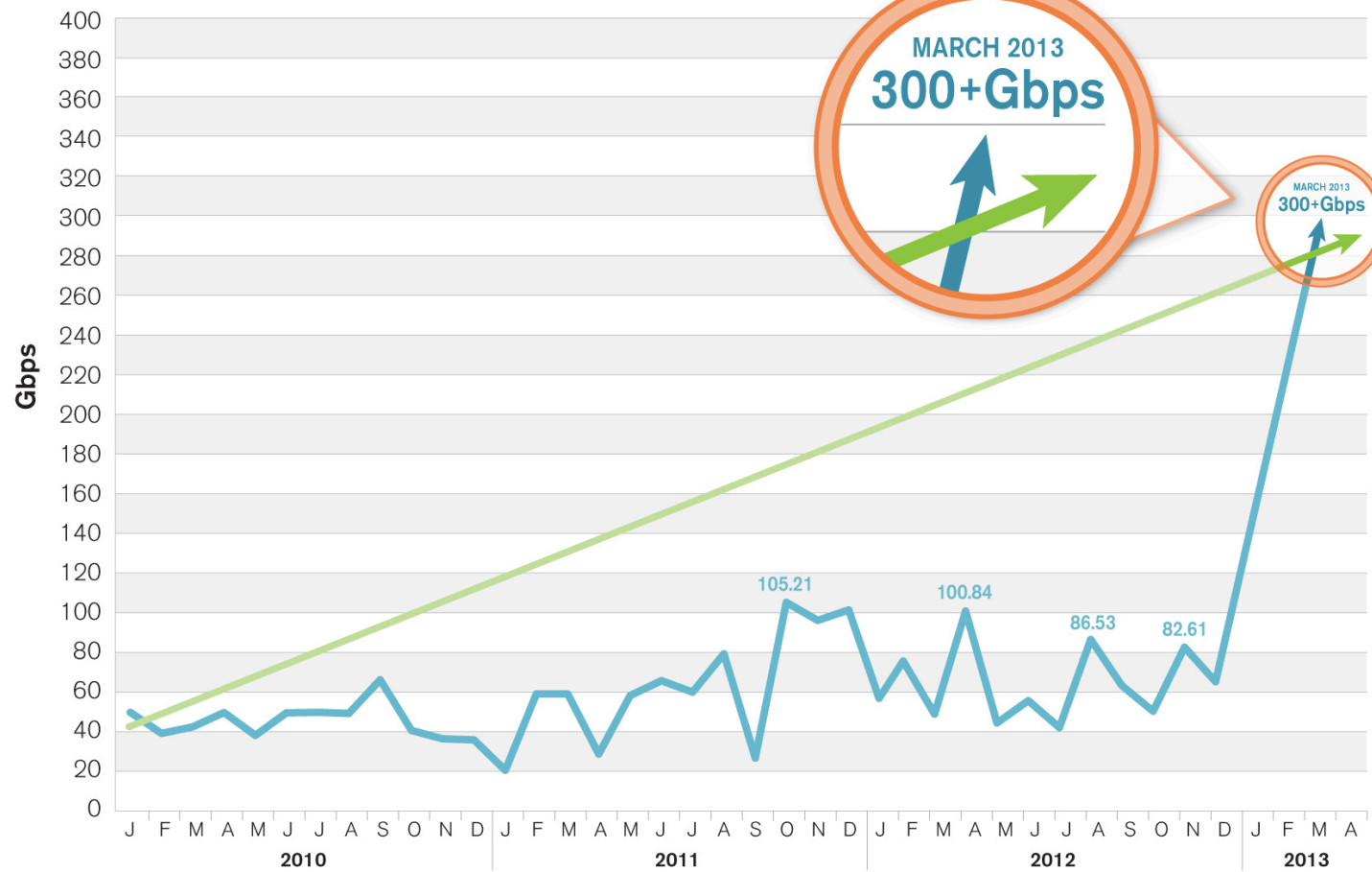


## 400Gbps, Globally Distributed Attacks



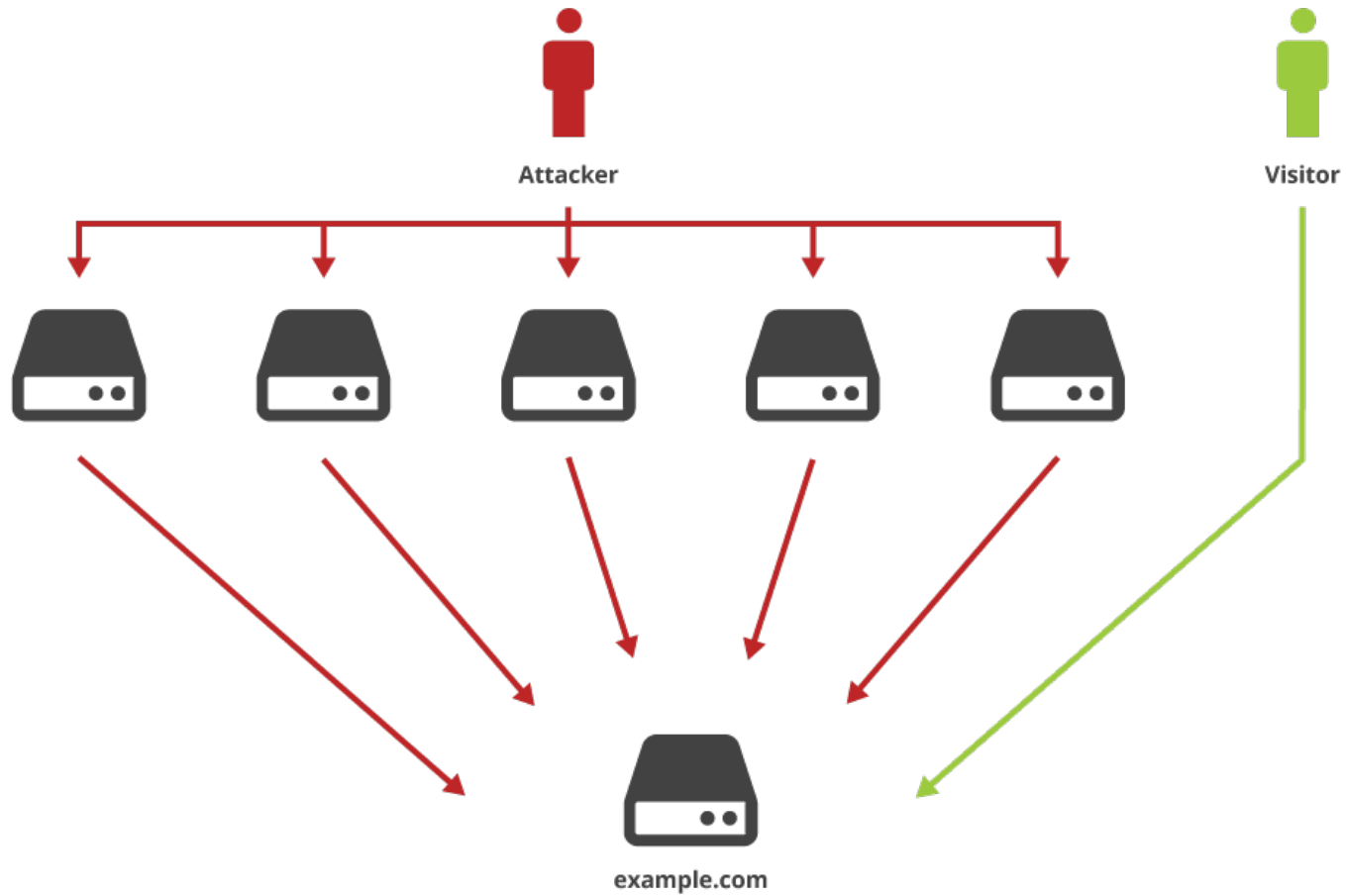


Peak DDoS Attack Size (January 2010-Present)

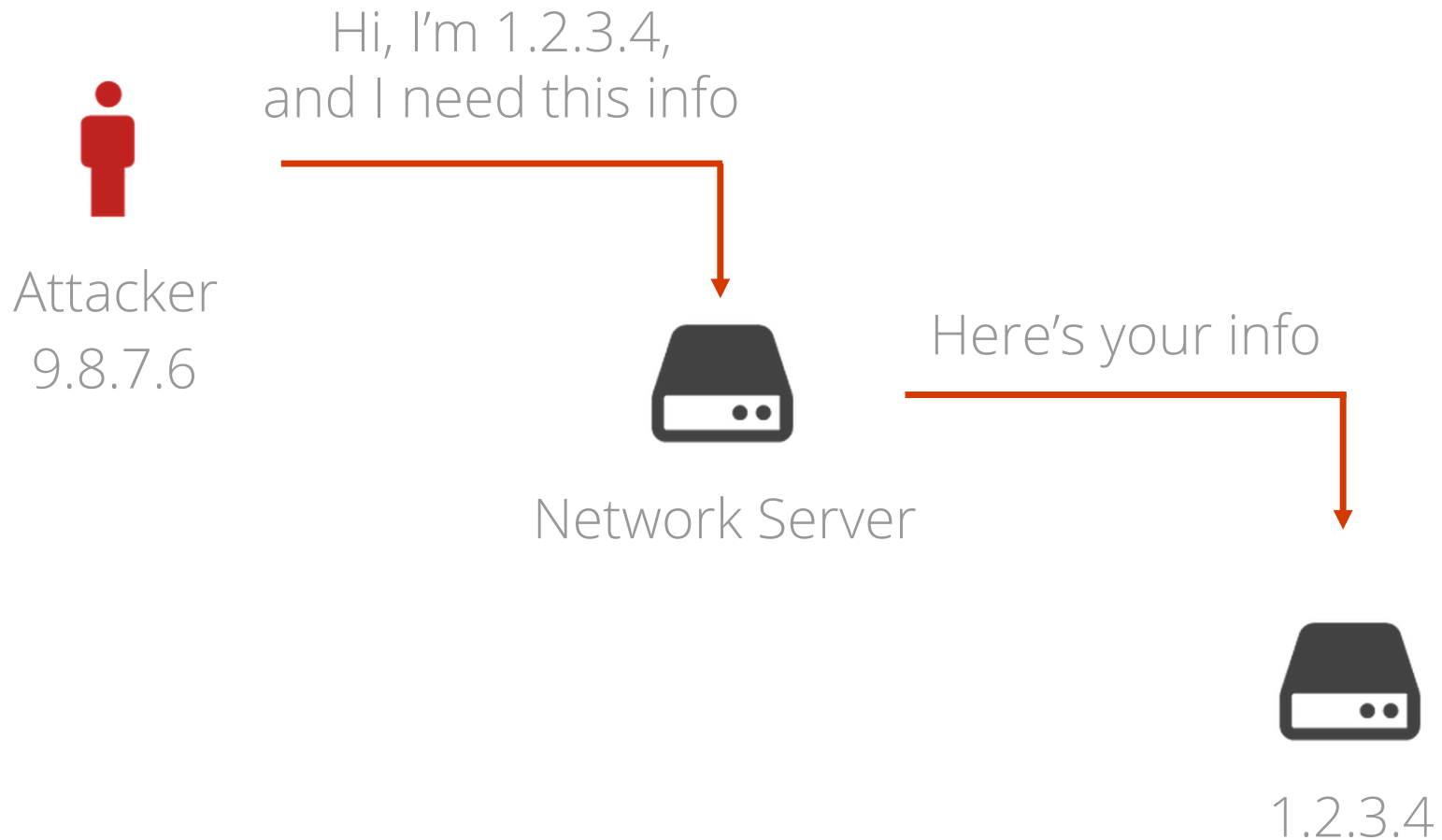


# Breaking Down the Attacks

# DDoS mechanics



# IP Spoofing



# IP Spoofing

## Summary:

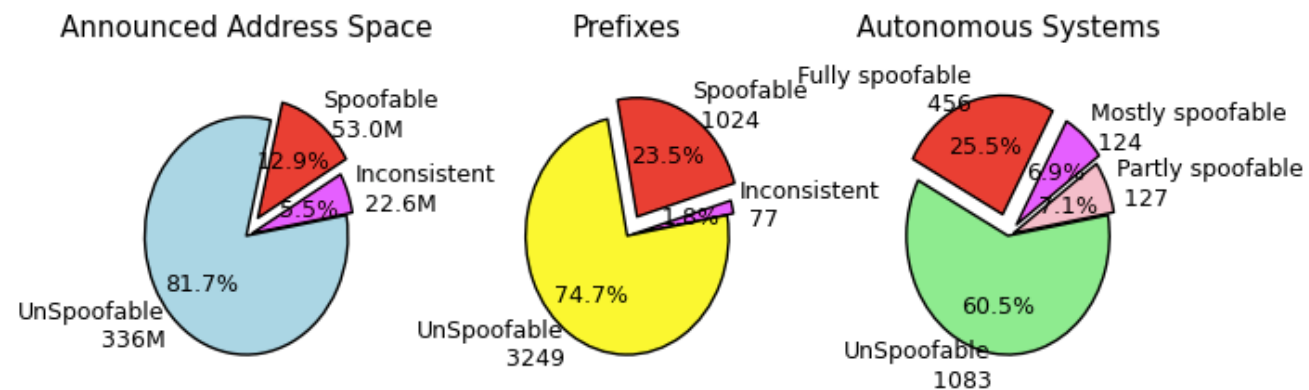
Data Range: Fri Feb 11 08:16:52 EST 2005 to Wed Feb 19 09:45:06 EST 2014

Total Tests: 20426

Unique IPs tested: 16200

Unique Routed Prefixes tested from: 8866

Unique ASes tested from: 2786



<http://spoofer.cmand.org/>

25.5% of networks allow spoofing

# Attack #1 – Spamhaus Attack:

309Gbps

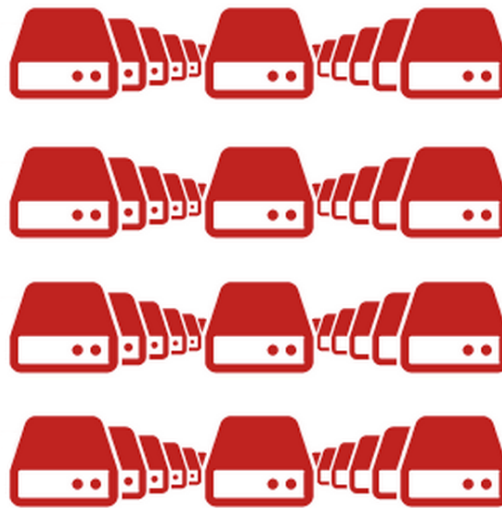
UDP

DNS

# Getting to 309Gbps

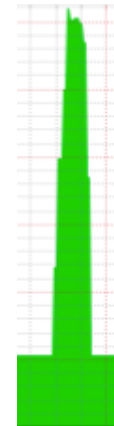


10 Mbps X



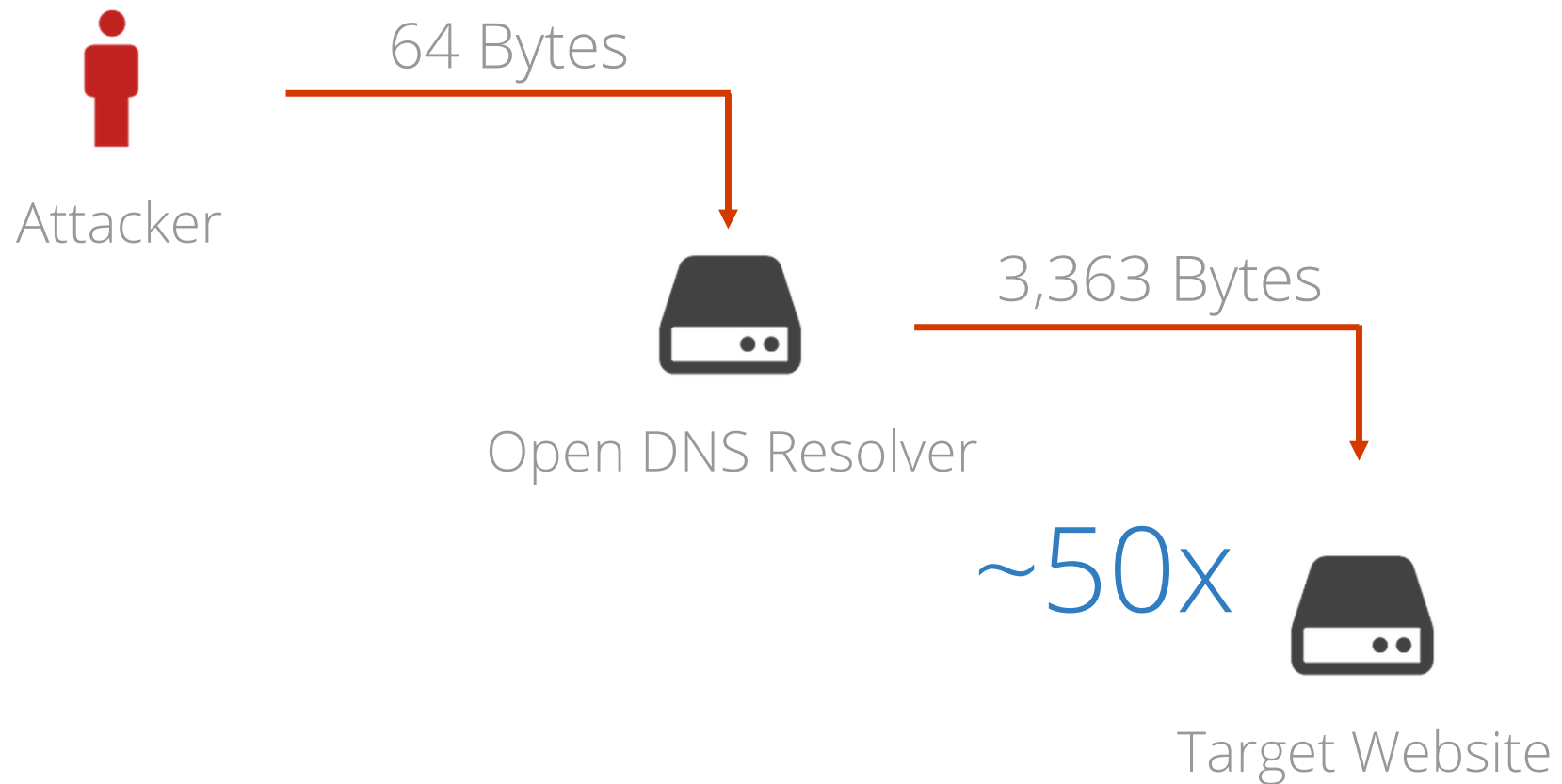
30,900

= 309,000 Mbps





# An easier way: DNS Amplification



How easy is it to  
create a query packet?

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

```

11 ANHMER 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.afiliat-ns.int.info.
isc.org. 7147 IN NS ord.sns-pb.isc.org.
isc.org. 7147 IN NS sms.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.paoli.isc.org.
isc.org. 7147 IN TXT "v=spf1 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 "V=ISC ISC.org 1999-2013-07-24 00:15:52 shahoney Exp 0"
isc.org. 7 IN AAAA 200:aef8:02::69
isc.org. 7147 IN NAPTR 20 0 "" SIP+D2UW "" sip_udp.isc.org.
isc.org. 3547 IN NSEC adsp.dominkey.isc.org. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY SFP
isc.org. 3547 IN NSEC 256 5 SOBAAAAABwHdCmehTOLQYOTvGx3MchMamufaijaidf/inadpV7vlTmXqL/x6e74QuRk0K6t5yngTl83yfrTW2OM/iSbf/hzlzm CFe20n3MfeqgTvryjn7dWghTW4vFv7HV7Wm9S8o9nfi795320knkh xSpXndeAAARU=
isc.org. 7147 IN DNSKEY 257 3 5 BEBAAAAHHqbChqhtpqggzWUpb5Q4UxkoVFWZMLDMwOxmJGr hHCeV4zihi7yJHf20t4idhNKOxylVQCEKRpdgw8XVKKLAS/AAS u5OWILSRk16Kt6PbsVVMF/Qx5RIK6PCLwvt+vU8eKhMo20j181Ulgyq3 47CBBlmnzz/4JlpAdaScQK6rJA2547315snMcwBs8/2/ZB63/zxrZq
[BK]BKH/BXekipks3jHdaI8xnkl3dy74R0901kSMct-xazgt7yyyl KMOde319278dmannZeOfPtWqAw6LxGe2vZEMTn4Ullgf/rzcC/bb yNs0t04EsdTd
isc.org. 3547 IN SIG 1 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 5 2 7200 2013082823259 2013072923259 50012 isc.org. XDOxyTFHEUvAT87V50Sogsk6cxdbhpRy31jq/oaKL190CAK4GYDU QdWtVnYv4v64jKtJ03v8b/UbuFCRaucO17L7kb/cCc6Yv1UCUOWp8 moImogyqrPDZYVA894mUONOGteb6CM688Pvvc6HzGX8b3omYvFYx uow=
isc.org. 7147 IN DNSKEY 5 2 7200 2013082823259 2013072923259 50012 isc.org. V704zx7V1WY9vWfVw1RfuPa2roz/qFT8RCDMPfMw6k5Jwyk7Skho 4ozLy1Tqd680+1MxrcDgr7c2BD8d84SC0DEKXunYhXBGMtLIJ3vJ5 2dLdOnT507v7keybyZweilPeZbl/CveayJPYZMCdAcWinheTc vIs=
isc.org. 7147 IN RRSIG 5 2 7200 2013082823259 2013072923259 50012 isc.org. HmxQp7toT3K5CoabMTU0t/sHQ84MGqviv7oVubMfhah/1w6Is DWOCVSeIcdL1MM8uXm9vpeFr13baal1R3CqLdLSce4Iws Dec08SC6COLd913hy3yVptp1ga3CalcuSepAbBHktP05RMotSTZV ASQ=
isc.org. 3547 IN NSEC 5 2 3600 2013082823259 2013072923259 50012 isc.org. V704zx7V1WY9vWfVw1RfuPa2roz/qFT8RCDMPfMw6k5Jwyk7Skho 4ozLy1Tqd680+1MxrcDgr7c2BD8d84SC0DEKXunYhXBGMtLIJ3vJ5 2dLdOnT507v7keybyZweilPeZbl/CveayJPYZMCdAcWinheTc vIs=
isc.org. 7147 IN NAPTR 5 2 7200 2013082823259 2013072923259 50012 isc.org. omvND0CAKGR3CR84ikHBMBId7Eq8d4ie4bKuzE191jVrrQPK QR85KbnJLh1F4vpv/KVVU9R213jaapebUuyHxycU3vYvT9gUJzUwMx2zhJhg7rEMlyUw/tKt h7w=
isc.org. 7 IN SIG 2 7200 2013082823259 2013072923259 50012 isc.org. dfoISOU0t3R2Poua7rPwcbpenugl2QoeilQdGwXNLNPj/OdSRO Wxtapag7PrsgzIDNVP3Qv7erPmsQbqjR/DojJbhBXUAL1+a Vn3+sbK8mXZ3Hg7rEMlyUw/tKt h7w=
isc.org. 7147 IN TXT 5 2 7200 2013082823259 2013072923259 50012 isc.org. wB3StzCq8bpmBm3mta10DCDBAd8/vW2v4zyW7/3rl1w2/p hfJ/Sd/bba7QD58ZSLohrBU8VKV7bqinGq+vg3rl871VldGGAr0 b-J0J1r5t8U9p3m3VfzccSNUI/4b GQ=
isc.org. 7147 IN MX 5 2 7200 2013082823259 2013072923259 50012 isc.org. BSXC4206WCMFD02icxyzmyy3jhy658BJ0oam5V1uiHnefo261FQUx 7oFFWafK4FO0H2E0q1nPFdcistrBMe8Lzu6+8IRdcmC/kURSI J0vd0e0evw=
isc.org. 7 IN SIG 5 2 60 2013082823259 2013072923259 50012 isc.org. Omibt8d7kxxhA861dfPgm3CkrXetWuxUP3Chlna3e4dg7vOm Ad158Myqaj1BBEXk3nSnp1J7VYMELDAvOb0Otgyag7vzPPVSV ICQCPQ928U=
isc.org. 7147 IN RRSIG 5 2 7200 2013082823259 2013072923259 50012 isc.org. B9bVtCv8ImBIZUYvAMQ3zYRkmoXNh7o9jQpGV8Zd3/ w6c774K7PW8R4F0gQ0dntrZrBKUPk6rSUWQUG0gWGaWCM Oq=
isc.org. 7147 IN SOA 5 2 7200 2013082823259 2013072923259 50012 isc.org. iIn8tEwtaph2kd02181The=xbtQ24Cp8R9TAOPkma597Af 1FE5kyqt1VybKpZTMkSmkg1Jh1NAACVLV

11 AUTHORITY SECTION:
isc.org. 7147 IN NS ns.isc.afiliat-ns.int.info.
isc.org. 7147 IN NS ord.sns-pb.isc.org.
isc.org. 7147 IN NS sms.sns-pb.isc.org.
isc.org. 7147 IN NS sfba.sns-pb.isc.org.

11 ADDITIONAL SECTION:
na.isc.afiliat-ns.int.info. 66448 IN A 199.254.63.254
na.isc.afiliat-ns.int.info. 66652 IN AAAA 2001:5001:7c1:254
ord.sns-pb.isc.org. 31018 IN AAAA 2001:5001:71:30
ord.sns-pb.isc.org. 31018 IN A 199.6.30.30
ams.sns-pb.isc.org. 31018 IN AAAA 2001:5001:60:30
ams.sns-pb.isc.org. 31018 IN A 199.6.31.30
sfba.sns-pb.isc.org. 31018 IN AAAA 2001:4f8:02:1:19
sfba.sns-pb.isc.org. 31018 IN A 149.20.64.3
mx.paoli.isc.org. 3547 IN AAAA 2001:aef8:02::2b
mx.paoli.isc.org. 3547 IN A 149.20.64.28
sip_udp.isc.org. 7147 IN SRV 0 1 5060 2001:5001:astisk
```

3,363 byte response



# 300Gbps+ of DDoS attack traffic

- 1 laptop
  - + 5-7 compromised servers
  - + 3 networks which allow spoofing
  - + 9Gbps of DNS requests to
  - + 0.1% of all open resolvers
- 

= 300Gbps of DDoS attack traffic

# Attack #2 – The NTP Attack:

400Gbps

UDP

NTP

# Tweets report attack issues



Retweeted by Stéphane Bortzmeyer

**Octave Klab / Oles** @olesovhcom · Feb 12

We see today lot of new DDoS attacks from Internet to our network. Type: **NTP AMP** Size: >350Gbps. No issue. VAC is great :)

Expand

Reply Retweet Favorite More



**Brian Carpenter** @geeknik · Feb 14

This script will let you create a DDOS **attack** using **NTP** servers  
[buff.ly/1bwDTKH](http://buff.ly/1bwDTKH)

Expand

Reply Retweet Favorite More



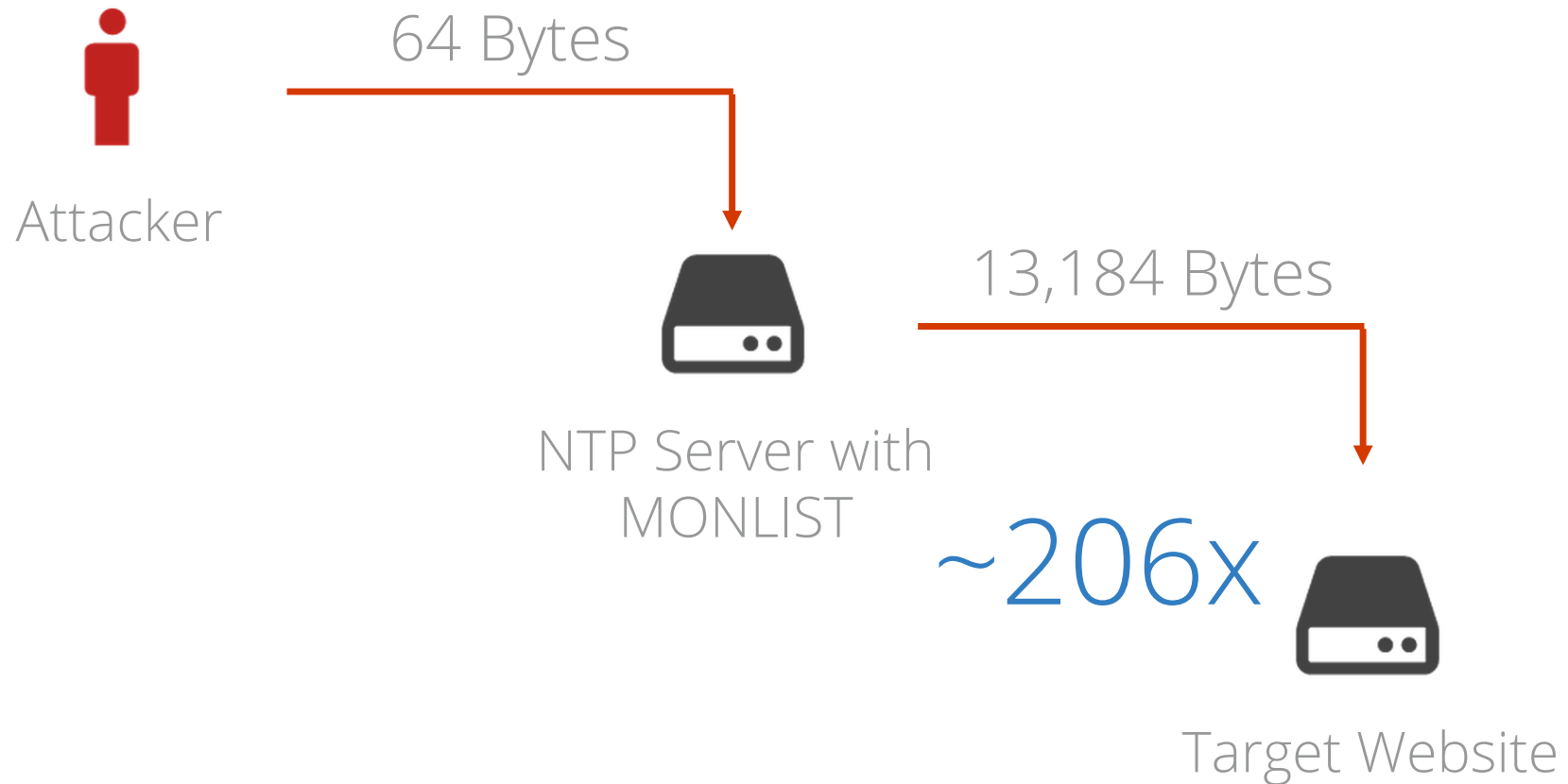
**Matthew Prince** @eastdakota · Mar 5

Encouraging: China Mobile reached out to clean up 231 vulnerable **NTP** servers on their network. ~5% those involved in 400Gbps DDoS **attack**.

Expand

Reply Retweet Favorite More

# An EVEN easier way: NTP Amplification



# 400Gbps+ of DDoS attack traffic

- 1 laptop
  - + 1 compromised server
  - + 1 network which allowed spoofing
  - + 1.94Gbps of MONLIST to
- 

= 400Gbps+ of DDoS attack traffic



# What's Next?

DNS → 8x

EDNS → ~50x

NTP → ~206x

SNMP → 650x

# Protecting your network

# 28 Million Open DNS Resolvers

## Open Resolver Project

Open Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from [Smurf attacks](#) commonly seen in the late 1990s.

We have collected a list of 32 million resolvers that respond to queries in some fashion. 28 million of these pose a significant threat (as of 27-OCT-2013). [Detailed History and Breakdown](#)

**Check my IP space**

Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /22 will be rejected):

[ipv4-heatmap of 20130519 data](#) [heatmap archive](#)

---

### What can I do?

If you operate a DNS server, please check the settings.

**Recursive servers** should be restricted to your enterprise or customer IP ranges to prevent abuse. Directions on securing BIND and Microsoft nameservers can be found on the [Team CYMRU Website](#) - If you operate BIND, you can deploy the [TCP-ANY patch](#)

**Authoritative servers** should not offer recursion, but can still be used in an attack. Configure your Authoritative DNS servers to use [DNS RRL \(Response Rate Limiting\)](#) Knot DNS and NLNetLabs NSD include this as a standard option now. BIND requires a patch.

**CPE DEVICES** SHOULD NOT listen for DNS packets on the WAN interface, including NETWORK and BROADCAST addresses.

**Prevent spoofing on your network!**

Configure Source Address Validation/uRPF/BCP-38 on all CPE and Datacenter equipment edges that have fixed IP ranges. This could be as simple as setting ip verify unicast source reachable-via rx on a router interface. Any statically routed customer should receive this setting by default.

### If you are in the security community:

Please contact [dns-scan@puck.nether.net](mailto:dns-scan@puck.nether.net) for access to raw data.

### Additional Information

[Informações em Português](#)

We can provide you a List of Open Resolvers by ASN if you e-mail [dns-scan@puck.nether.net](mailto:dns-scan@puck.nether.net)

[Test your IP Now!](#)

### DNS DDoS and Security in the News

- 04-APR-2013 [Spamhaus DDoS was just a warning shot](#)
- 30-MAR-2013 [How the Cyberattack on Spamhaus Unfolded](#)
- 28-MAR-2013 [Is Your DNS Server part of a criminal conspiracy?](#)
- 20-MAR-2013 [75Gb/s DDoS against Cloudflare](#)

### Presentations:

- DNS-OARC May 2013 - [slides](#)
- NANOG 58 June 2013 - [Lightning Talk](#)

<http://OpenResolverProject.org/>

Lock your DNS server (recursive & authoritative) down

# 28 Million Open DNS Resolvers

## UNIX bind configuration examples

```
options {  
    recursion no;  
    additional-from-cache no;  
};
```

```
acl "trusted" {  
    10.42.0.0/16;  
    192.0.2.0/24;  
    192.0.6.0/24;  
};  
options {  
    recursion no;  
    additional-from-cache no;  
    allow-query { none; };  
};  
view "trusted" in {  
    match-clients { trusted; };  
    allow-query { trusted; };  
    recursion yes;  
    additional-from-cache yes;  
};
```

<http://team-cymru.org/>

Confirm that the resolver is a closed resolver

# NTP Amplification Attacks

OpenNTPProject.org - NTP Scanning Project

Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /22 will be rejected):

**If you are a member of the general public:**

How can I check my server? - run the command `ntpd -n -c monlist 192.0.2.1 Of ntpq -c rv 192.0.2.1` - If you see a response, your server may be used in attacks.

How can I fix my server, router or other device? You should upgrade to NTP-4.2.7p26 or later. You can add `disable monitor` to your `ntp.conf` and restart your NTP process if on an earlier version. Also check out the [Team Cymru Secure NTP Template](#) - Also see [NTP Bug #1532](#)

The server should also not respond to `loopinfo` or `iostat` requests as well

We test the internet for NTP MODE 6 and MONLIST MODE 7 responses.

Cisco customers should ask about or open a case against [CSCum44673](#).

Recent News:

2014-02-22 - [Amplification Hell: Revisiting Network Protocols for DDoS Abuse](#)

2014-02-13 - [Technical Details behind 400Gb/s NTP attack](#)

2014-01-13 - [100Gb/s attacks using NTP](#)

2013-12-26 - [Christmas 2013 NTP Attacks](#)

**If you are a member of the security community:**

You can contact the `ntp-scan /at/ puck.nether.net` to obtain the raw data. It is available for re-use in your reporting.

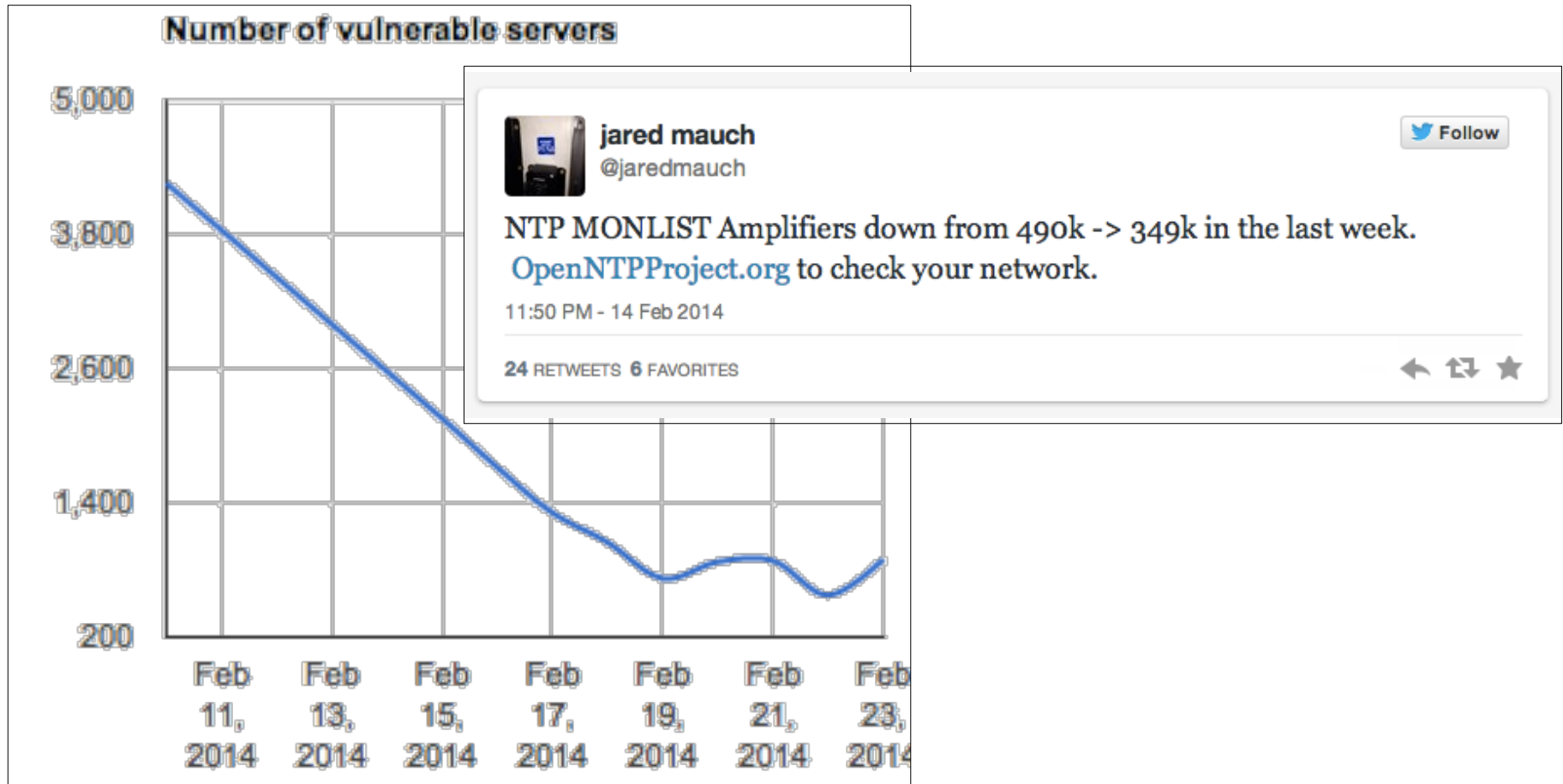
**About US:**

OpenNTPProject.org is operated in conjunction with [Network Time Foundation](#). If this service is valuable, please consider joining or donating to NTF.

http://OpenNTPProject.org/

## Turn off MONLIST on your NTP servers

# NTP Amplification Attacks



# NTP Amplification Attacks

## UNIX ntpd configuration example

```
# by default act only as a basic NTP client
restrict -4 default nomodify nopeer noquery notrap
restrict -6 default nomodify nopeer noquery notrap
# allow NTP messages from the loopback address, useful for debugging
restrict 127.0.0.1
restrict -6 ::1
# server(s) we time sync to
server 192.0.2.1
server 2001:db8::1
server time.example.net
```

<http://team-cymru.org/>

“noquery” is required to disable MONLIST

# Prevent IP Spoofing (network hygiene)

- BCP38 / RFC2827 (ingress filtering) – May, 2000:
  - <http://bcp38.info/>
  - <http://www.ietf.org/rfc/bcp/bcp38.txt>
  - <http://www.ietf.org/rfc/rfc2827.txt>
- BCP84 / RFC3704 (for multihomed) – March, 2004:
  - <http://www.ietf.org/rfc/bcp/bcp84.txt>
  - <http://www.ietf.org/rfc/rfc3704.txt>



# Securing CDN traffic at CloudFlare

# CloudFlare security

CloudFlare leverages the knowledge of a diverse community of websites to power a new type of security service. Online threats range from nuisances like comment spam and excessive bot crawling to malicious attacks like SQL Injection and denial of service (DOS) attacks. CloudFlare provides security protection against all of these types of threats and more to keep your website safe.

---



## Automatic learning of new attacks

CloudFlare's technology automatically detects new attacks that arise against any website on its network. Once CloudFlare identifies that there is a new attack, CloudFlare starts to block the attack for both the particular website and the entire community. This also means the longer you are on CloudFlare, the better the protection becomes. [See a customer case study at the CloudFlare blog.](#)

# CloudFlare – a global network



Attack traffic is global and hence a global edge is valuable

# Anycast Dilutes Attacks

300Gbps of attack traffic  
/ 29 locations

---

= ~10.3Gbps average per location

# Hide Origin IPs

- Use separate IPs for HTTP, DNS, SMTP, etc
- Public DNS should route to your EDGE's public IPs
- Keep actual/origin web device IPs protected

# Filter traffic by IP and protocol

- No UDP packets should be able to hit your HTTP server
  - UDP is IP protocol 17 vs. TCP for HTTP is IP protocol 6
- No HTTP packets should be able to hit your SMTP server
  - HTTP is TCP port 80 & 443 vs. SMTP is port 25 & 587

# Filter traffic by IP and protocol

## Simple Cisco filter configuration example

```
!  
hostname router-www  
!  
interface ethernet0  
    ip access-group 102 in  
!  
access-list 102 permit tcp any host 10.0.0.100 eq 80  
access-list 102 permit tcp any host 10.0.0.100 eq 443  
access-list 102 deny all  
!
```

<http://team-cymru.org/>

Allow only HTTP& HTTPS via TCP protocol to a specific IP

# Protect your infrastructure

- Internal switches, routers, and other devices should be locked down from any external access
- All traffic should flow through EDGE devices which handle attacks
  - CloudFlare Web Application Firewall (WAF) service



# Build relationships upstream

- Understand what your data center and bandwidth providers do about DDoS
- Know who to call when trouble strikes
- Share your IP/Protocol architecture with them

# Communicate about attacks

Enormous DNS DDoS attack originates from anti-DDoS service providers

SECURITY

NEWS

13 May 2014 by [Jamie Hinks](#)

[jamie.hinks@itproportal.co.uk](#)

**BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus**

**Plucky mail scrubbers battle internet carpet bombers**

By John Leyden, 27 Mar 2013

[Follow](#)

2,679 followers

## Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

Published on February 13, 2014 01:00AM by [Matthew Prince](#).

# Summary

# Summary

- First, make sure you're not part of the problem ...
- Second, practice good protocol hygiene ...
- Third, implement infrastructure ACLs ...
- Fourth, know your upstreams ...

# Questions?

AS13335 { Martin J. Levy, Network Strategy  
@mahtin  
@cloudflare  
<http://www.cloudflare.com/>