CLOUDFLARE

How to launch and defend against a DDoS

John Graham-Cumming

October 9, 2013

The simplest way to a safer, faster and smarter website

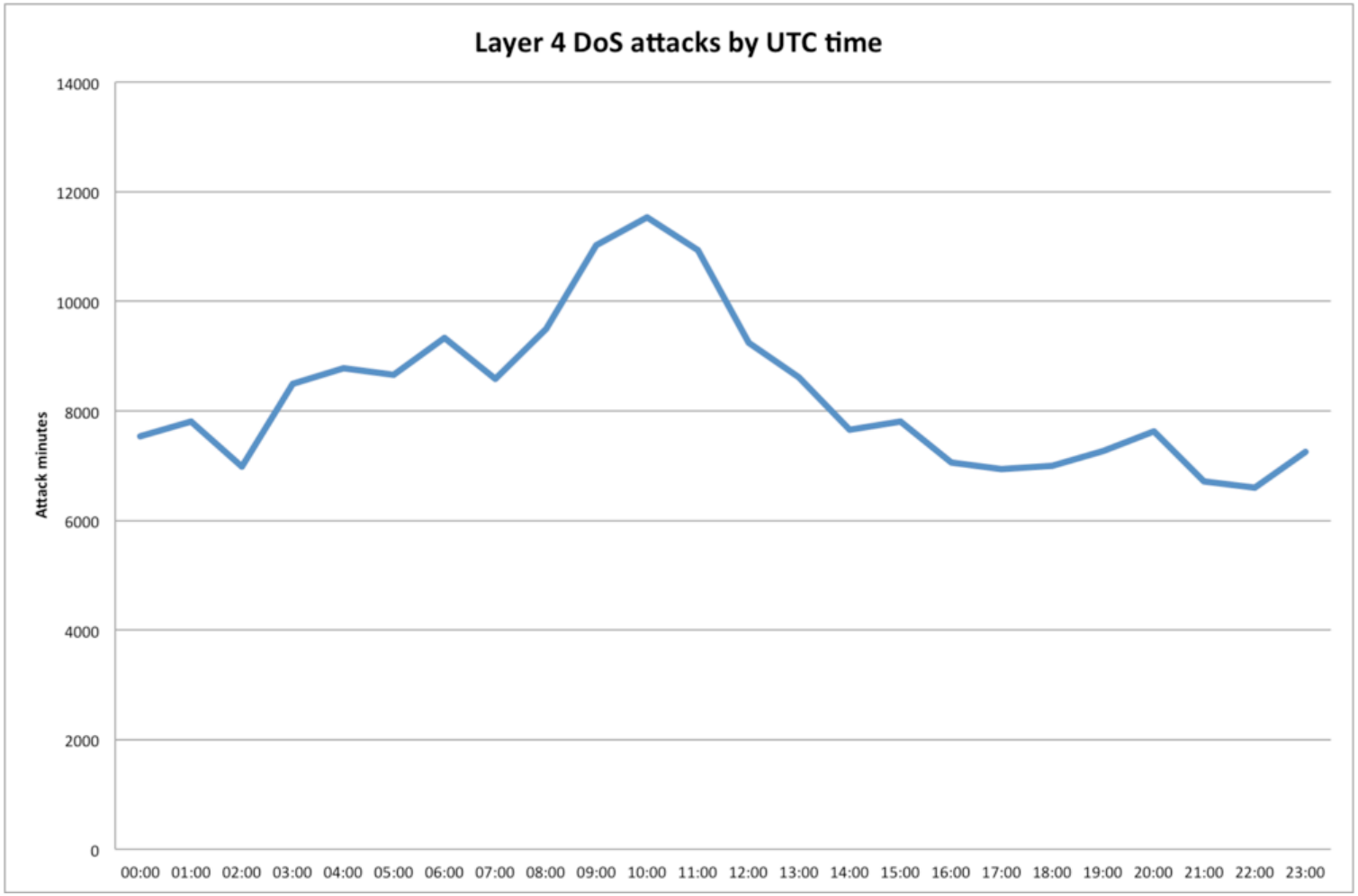
DDoSing web sites is... easy

- Motivated groups of non-technical individuals
  - Followers of Anonymous etc.
  - Simple tools like LOIC
- People with money to spend
  - Botnets
  - Online ‘booter’ services
- Anyone with a grudge

What gets attacked

- TCP
  - 92% against port 80
  - SYN flooding
- UDP
  - 97% against DNS
  - Reflection/amplification attacks
- Other significant attack ports
  - TCP port 53 (DNS)
  - UDP port 514 (syslog)

And when...



CLOUDFLARE

Three things make DDoS easy

- Fire and forget protocols
  - Anything based on UDP
  - ICMP
- No source IP authentication
  - Any machine can send a packet “from” any machine
- Internet Amplifiers
  - Authoritative DNS servers that don’t rate limit
  - Open DNS recursors
  - Open SNMP devices

DDoS Situation is Worsening

- Size and Frequency Growing
  - In 2012 the largest DDoS attack we saw was 65 Gbps
  - In 2013 it was 309 Gbps (almost 5x size increase)
  - DNS-based DDoS attacks grew in frequency by 200% in 2012

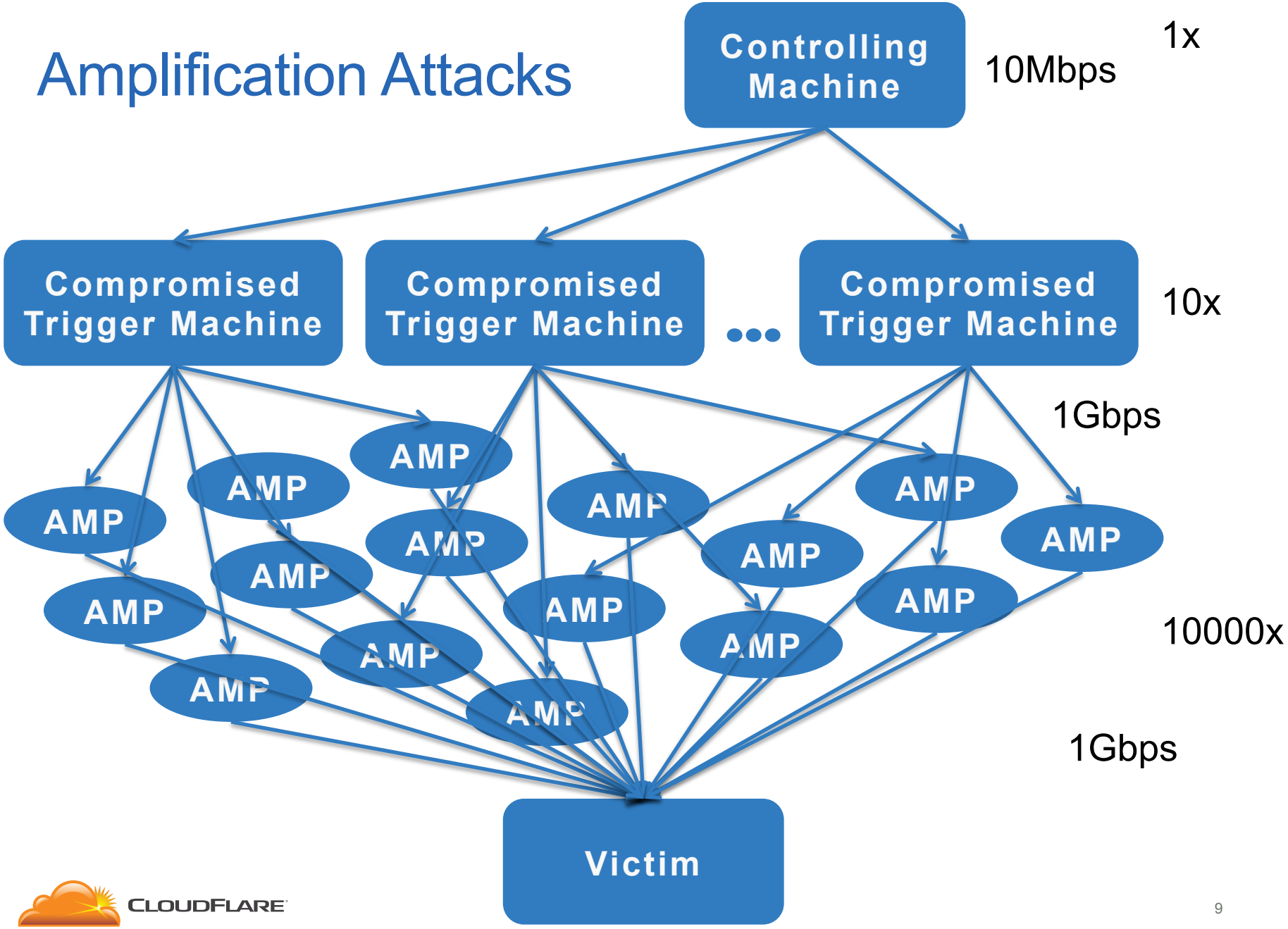
March 24, 2013

- 309 Gbps sustained for 28 minutes
- 30,956 open DNS resolvers
  - Each outputting 10 Mbps
- 3 networks that allowed spoofing

March 25, 2013

- 287 Gbps sustained for 72 minutes
- 32,154 open DNS resolvers
  - Each outputting 9 Mbps
- 3 networks that allowed spoofing

Amplification Attacks



DNS and SNMP Amplification

- Small request to DNS or SNMP server with spoofed source IP address
- DNS or SNMP server responds with large packet to ‘source’: the victim
  - DNS multiplier is 8x (Req: 64B; Resp: 512B)
  - EDNS multiplier is 53x (Req: 64B; Resp: 3,364B)
  - SNMP multiplier is 650x (Req: 100B; Resp: 65kB)

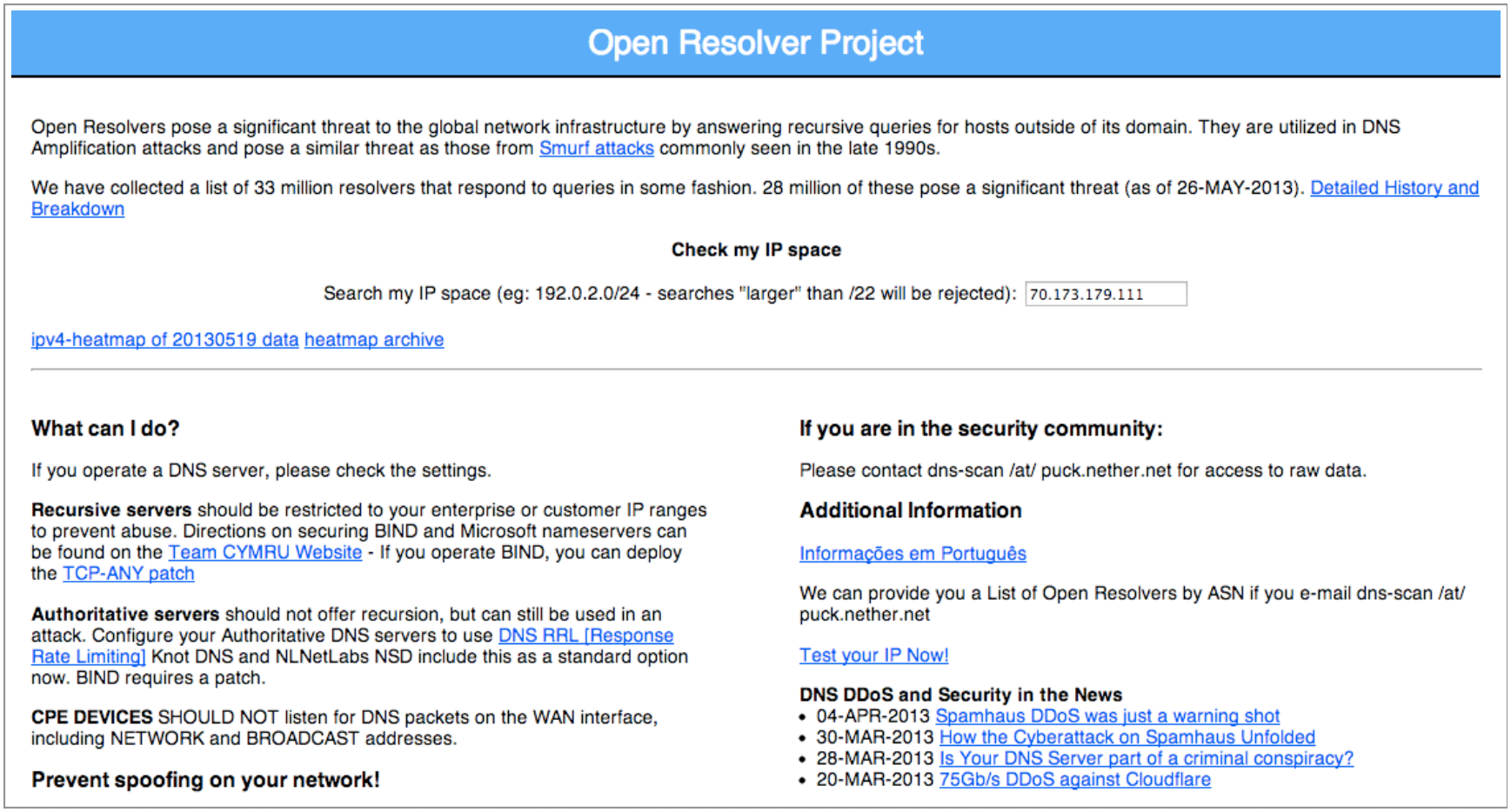
HOWTO: 1 Tbps DDoS

- Get a list of 10,000 open DNS recursors
  - Each machine will produce 1 Tbps / 10,000 = 100 Mbps
  - Use more machines if that's too high
- DNS amplification factor is 8x so need 1 Tbps / 8 = 125 Gbps trigger traffic
  - So 100 compromised servers with 1Gbps connections will do
- If DNS recursors support EDNS then only need 1 Tbps / 50 = 20 Gbps trigger traffic

SNMP etc.

- We have seen a 25 Gbps DDoS attack using SNMP amplification
  - Came from Comcast Broadband Modems
- NTP?

28 Million Open 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 33 million resolvers that respond to queries in some fashion. 28 million of these pose a significant threat (as of 26-MAY-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): 70.173.179.111

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!

If you are in the security community:

Please contact dns-scan /at/ 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 /at/ 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

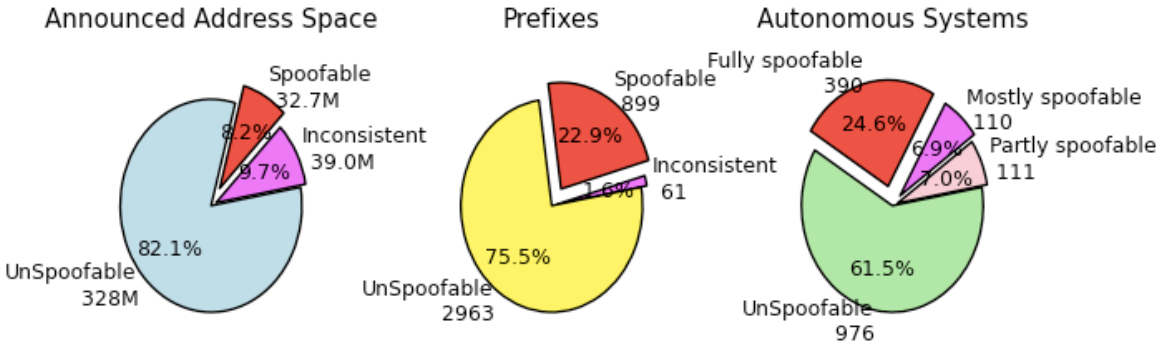
24.6% of networks allow spoofing

Spoofer Project: State of IP Spoofing

Home Stats Download News FAQ Papers Contact

Summary:

Data Range: *Fri Feb 11 08:16:52 EST 2005 to Wed Jul 3 12:27:56 EDT 2013*
Total Tests: *18299*
Unique IPs tested: *14423*
Unique Routed Prefixes tested from: *7829*
Unique ASes tested from: *2466*



Spamhaus DDoS Was Easy

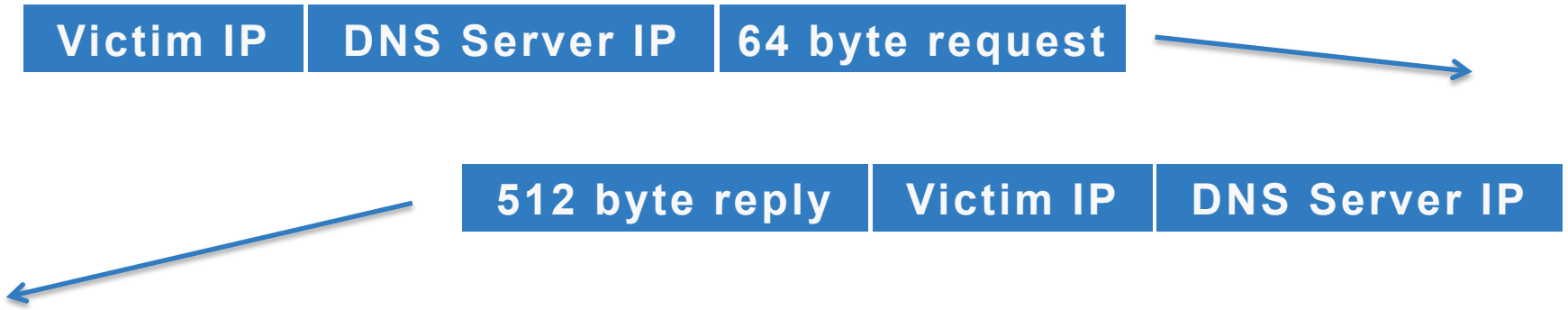
- 1 attacker's laptop controlling
  - 10 compromised servers on
  - 3 networks that allowed spoofing of
  - 9Gbps DNS requests to
  - 0.1% of open resolvers resulted in
- **300Gbps+** of DDoS attack traffic.

Solving This Problem

- Close Open DNS Recursors
  - Please do this!
- Stop IP Spoofing
  - Implement BCP38 and BCP84

IP Spoofing

- Used to ICMP attacks, TCP SYN floods and amplification attacks
  - Vast majority of attacks on CloudFlare are spoofed attacks



- Dealing with IP spoofing stops amplification, hurts botnets

Mars Attacks!

- 23% from Martian addresses
- 3.45% from China Telecom
- 2.14% from China Unicom
- 1.74% from Comcast
- 1.45% from Dreamhost
- 1.36% from WEBNX
- Larger point: spoofed packets come from everywhere

Ingress Filtering: BCP38 and BCP84

- BCP38 is RFC2827
  - Been around since 2000
  - http://www.bcp38.info/
  - https://en.wikipedia.org/wiki/Ingress_filtering
- BCP84 is RFC3704
  - Addresses problems with multi-homed networks

Why isn't BCP38 implemented widely?

- Simple: economic incentives are against it
  - IP-spoofing based DDoS attacks are an "externality": *like a polluting factory*
  - IP-spoofing based DDoS attacks are not launched by the networks themselves: *a factory that only pollutes on someone else's command*
  - Networks have a negative incentive to implement because of impact on their customers' networks
- Externalities get fixed by regulation
  - Better to fix this without government intervention
  - Governments will intervene when they are threatened (and they are!)

We've been here before

- SMTP Open Relays
  - Let's not get to the point that BL are created
  - Or that governments intervene

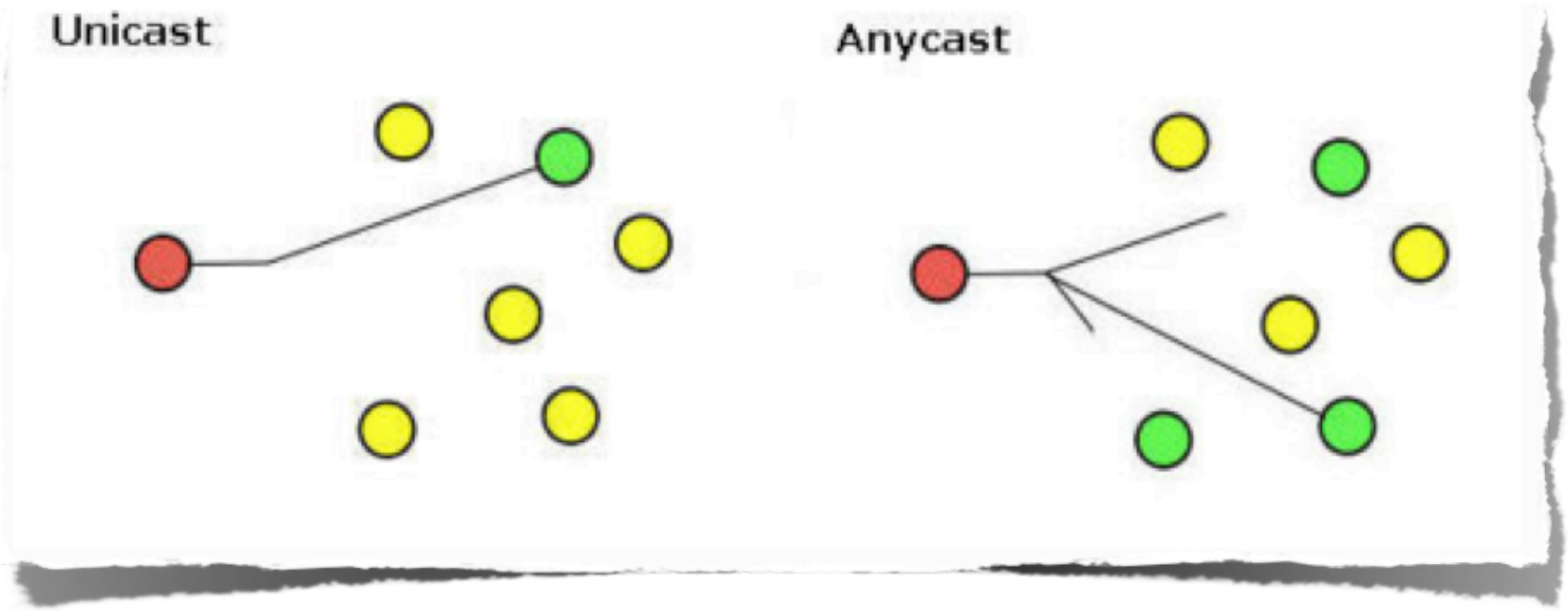
CLOUDFLARE

DDoS Defense

Start with a global network

CLOUDFLARE

Use Anycast



Anycast Attack Dilution

310 Gbps

/ 23 PoPs

= 14 Gbps per PoP

Hide Your Origin

- If you use a DDoS service make sure your origin IP is hidden
  - Change it when signing up
  - Make sure no DNS records (e.g. MX) leak the IP
- and make sure that IP only accepts packets from the service

Separate Protocols By IP

- For example, have separate IPs for HTTP and DNS
- Filter by IP and protocol
  - No UDP packets should be able to hit your HTTP server
  - No HTTP packets should be able to hit your SMTP server

Protect your infrastructure

- Separate IPs for infrastructure
  - Internal switches, routers
- Filters those IPs at the edge
  - No external access to internal infrastructure
- Otherwise attackers will attack your infrastructure

Work closely with your upstream

- Get to know who to call when trouble strikes
- Enable them to perform filtering in their infrastructure
- Share you IP/Protocol architecture with them