DNS DDoS
Challenges and Mitigations

Damian Menscher

Site Reliability Engineering

Presented at OARConline 35a

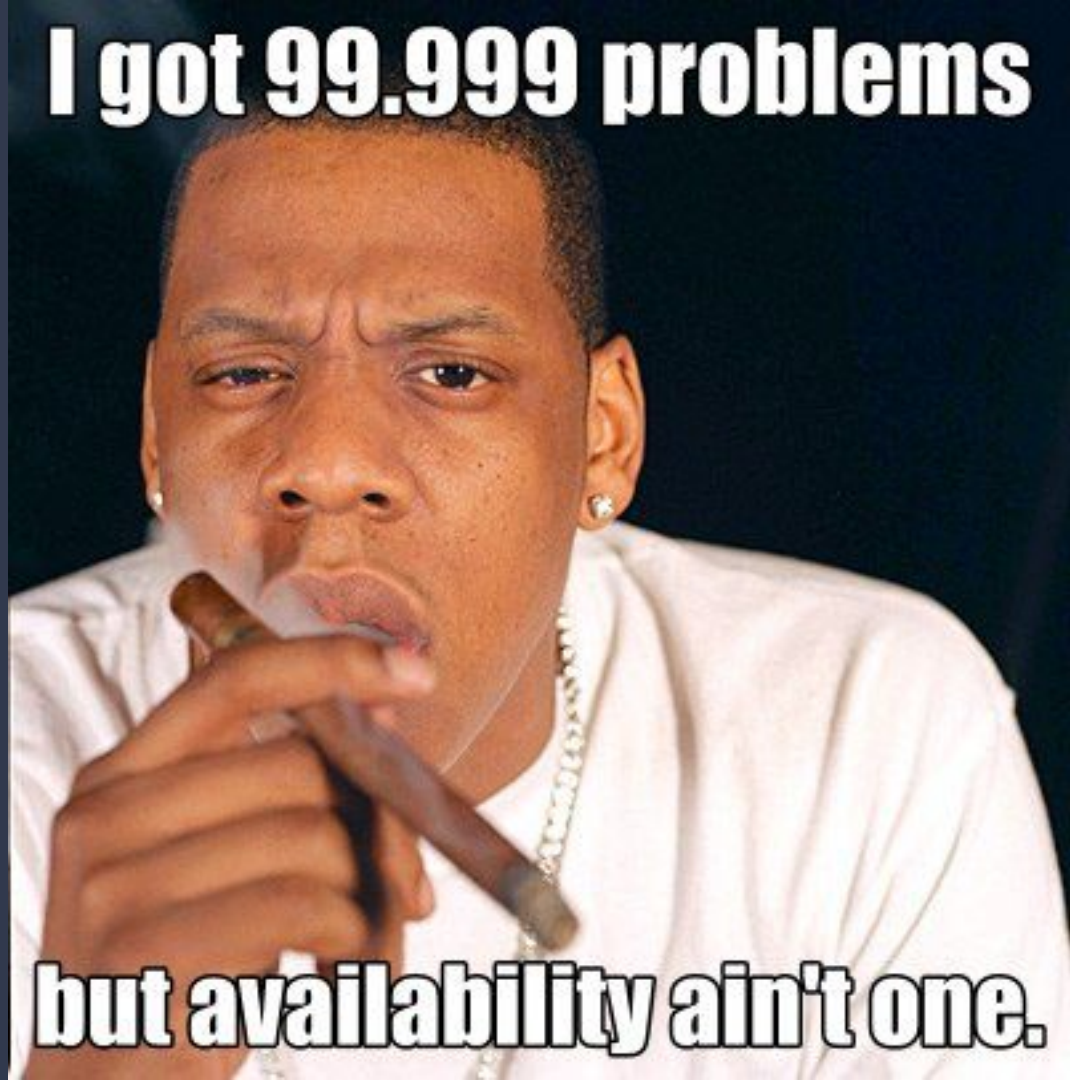
Google

$ whoami

Security Reliability Engineer

Focused on DDoS defense

Not a DNS expert



Agenda

Theory vs. practice
Non-attack escalations
Challenges for recursives
Auth server outages
Root cause analysis
DDoS mitigation
Incident reports
Main takeaways

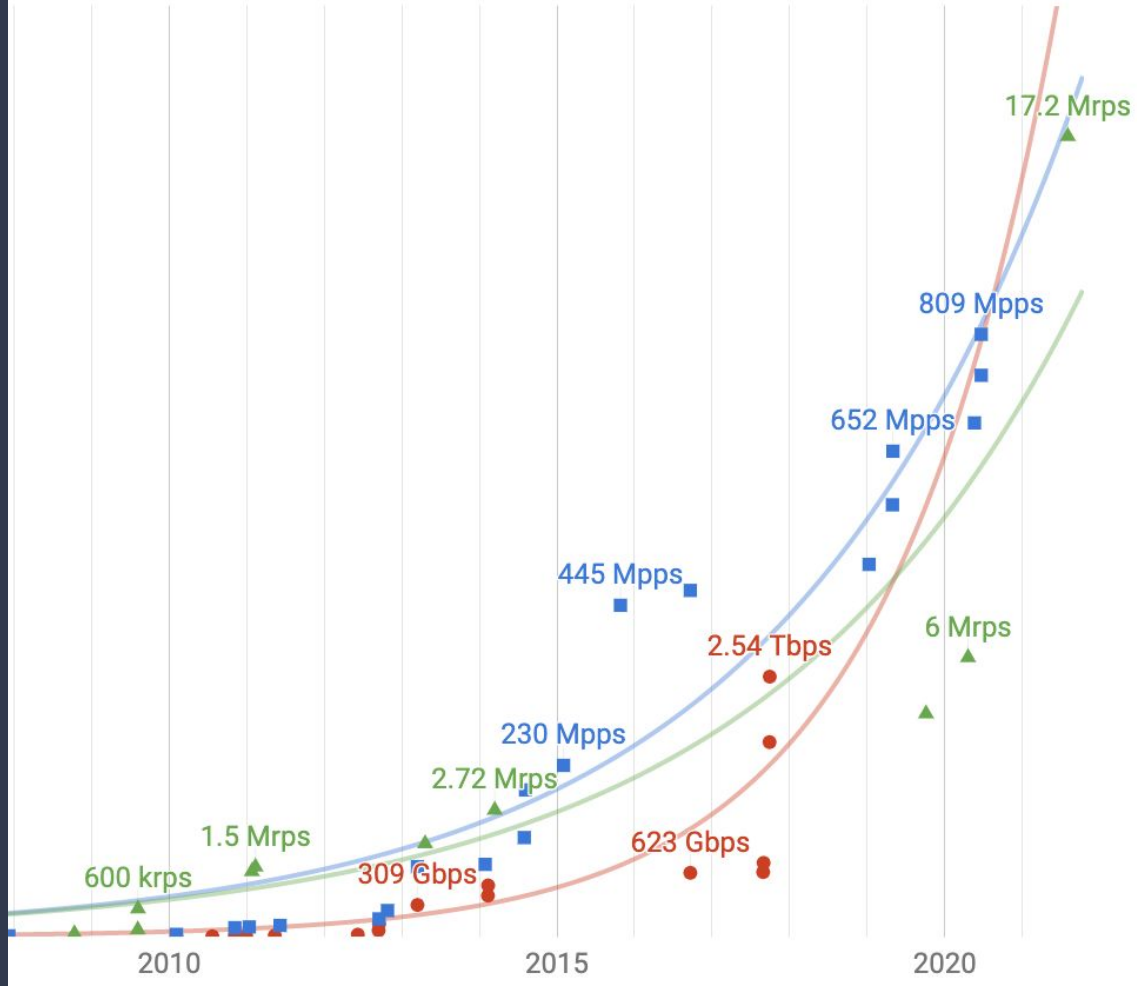
Theory

Largest attacks to date

2.5 Tbps (Google, 2017)

809 Mpps (Akamai, 2020)

17.2 Mrps (Cloudflare, 2021)



Theory *vs.* Practice

Companies that suffered DNS outages:

Akamai
Amazon
Cloudflare
Dyn
Google
Microsoft
Yahoo!
… ISP recursives, ccTLDs, etc.

TC

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Darrell Etherington, Kate Conger

/ 5:31 AM PDT • October 21, 2016

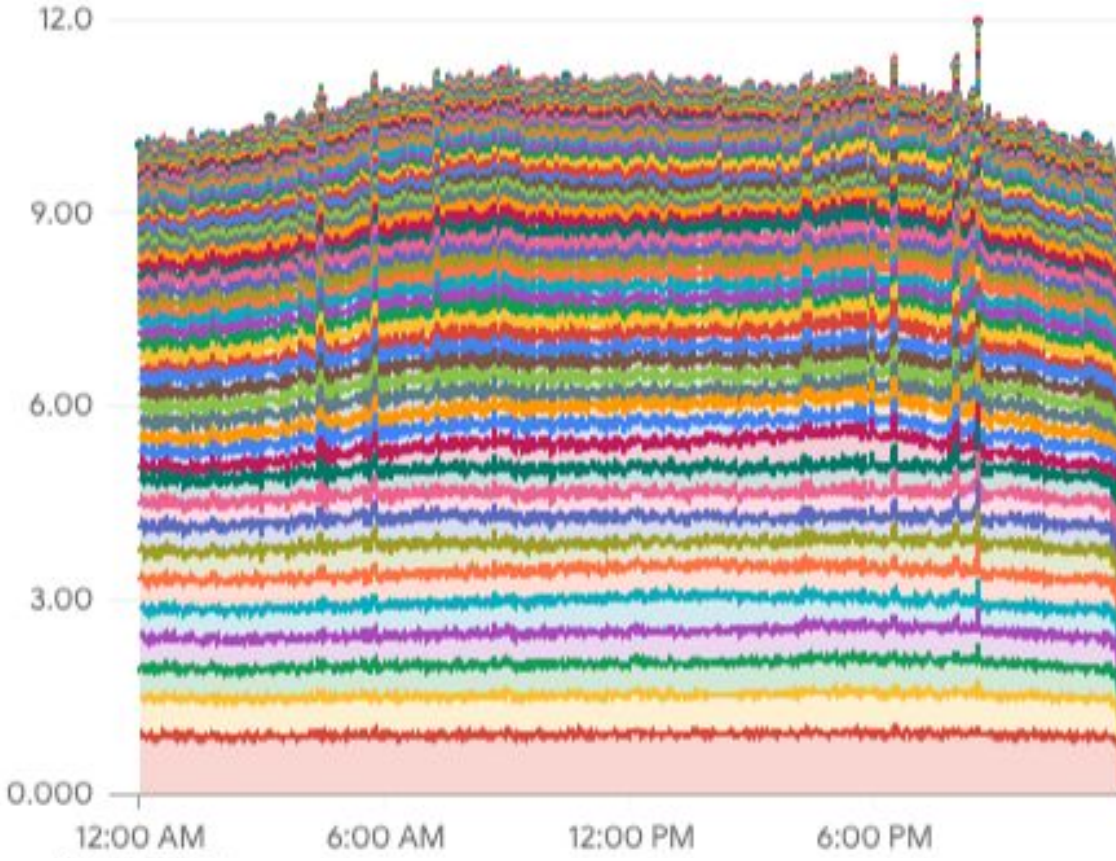
Comment

Non-attack escalations

Traffic characteristics?

Traffic volume?

Impact?



Challenges for recursives

Dealing with problem users

Spoofing

Repeated queries

Cache-busting (NXDOMAIN) attacks

peacecorps.gov.	421,295,842
sl.	294,092,992
hrsa.gov.	160,111,525
paypal.com.	139,793,620
.	129,737,705
isc.org.	52,448,135
census.gov.	38,714,553

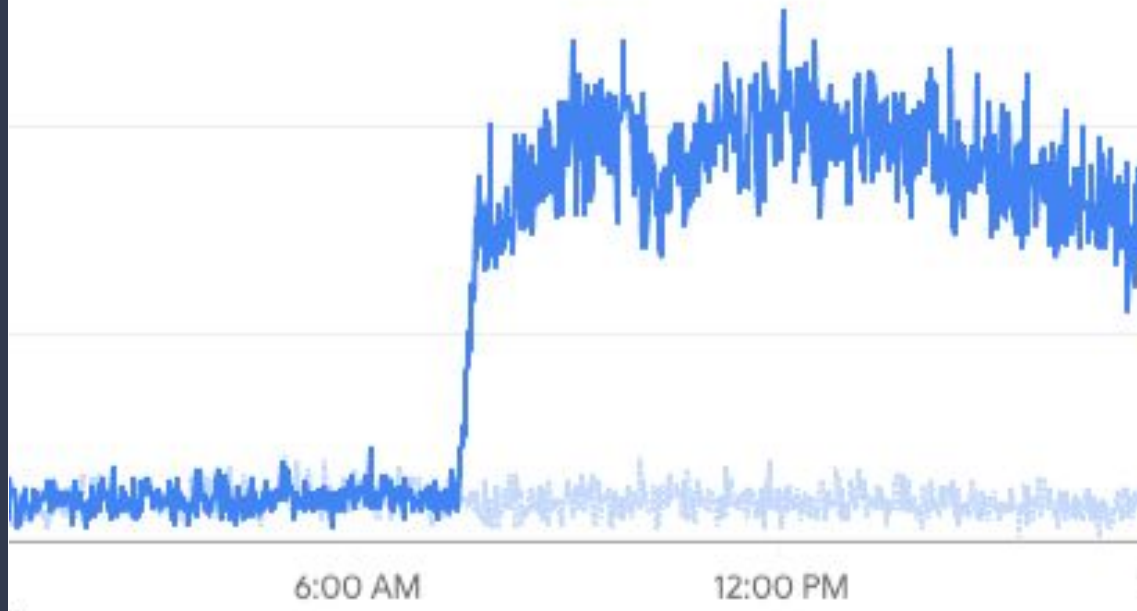
Challenges for recursives

Dealing with authoritative servers

Failures lead to retries

Benefits of throttling??

0-TTL responses



Auth server outages

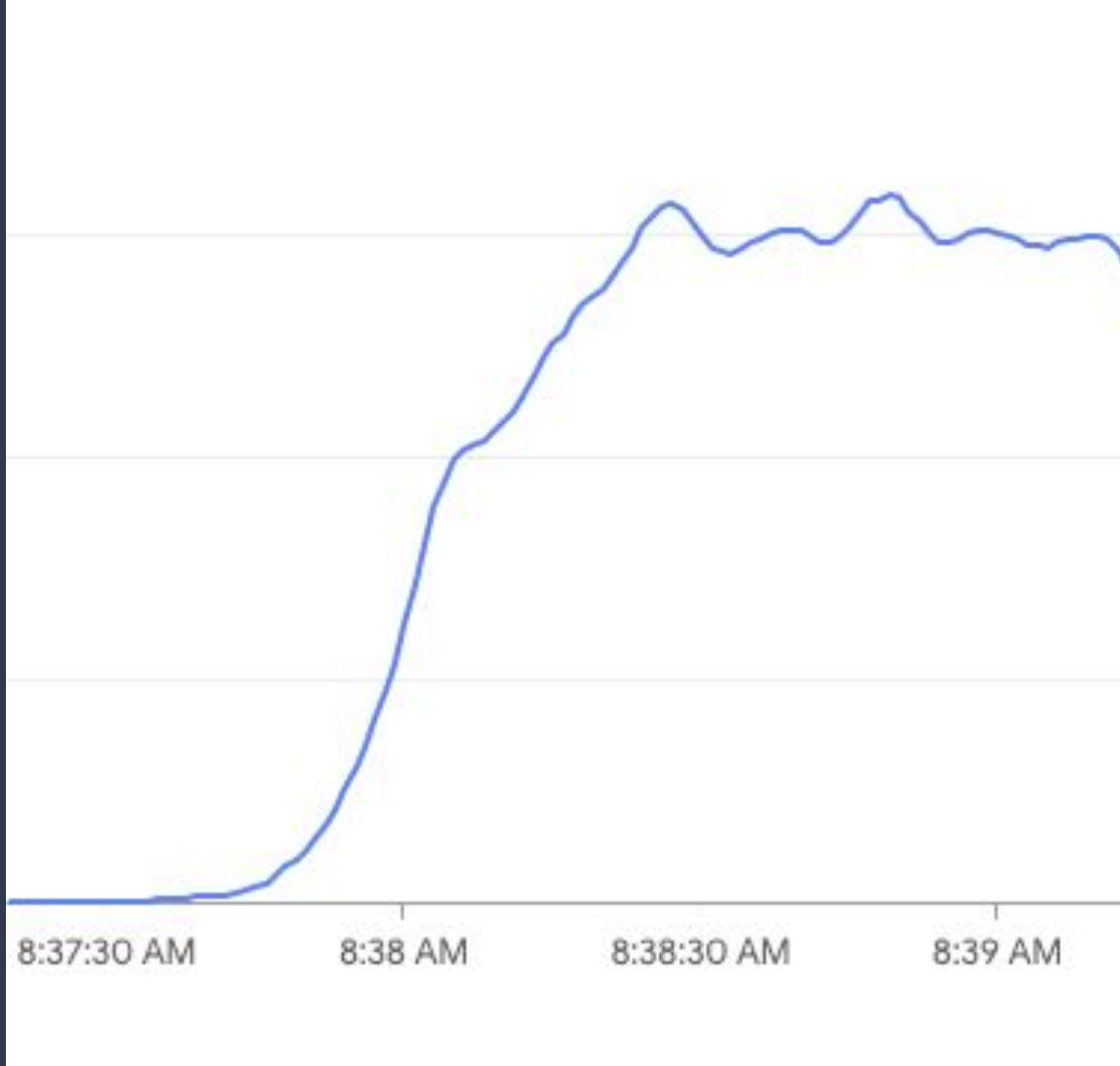
Common outage scenario

1. Outage → recursive caches expire
2. Lack of cache → recursion for every query + retries

Cache hit rates can be quite high — 30x increase not uncommon

30x sounds like a DDoS, but might not be…

Top talkers may be legitimate recursives



BGP

Hijack resistance

- announce /24s
- anycast w/ short AS-path

Return path?

DISRUPTIONS, INTERNET INTELLIGENCE | August 3, 2018

BGP / DNS Hijacks Target Payment Systems

Doug Madory

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 12:00 PM

TECH \ CYBERSECURITY \ CRYPTOCURRENCY \

Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

By Russell Brandom | Apr 24, 2018, 1:40pm EDT

RCA: Prerequisites

Know your baseline

- traffic volume
- query characteristics
- popular recursives

Internal dependencies?

Will you receive an alert? Can you VPN in?

RCA:
Common Causes

Rollout?

Traffic increase

- zone-file scraping?
- cache-busting attack?
- retries??

Think outside the DNS

Accept outside help

DDoS mitigation

Basic techniques

Best-effort response

Allow-list known recursives

Consider adversary response

Increase TTLs

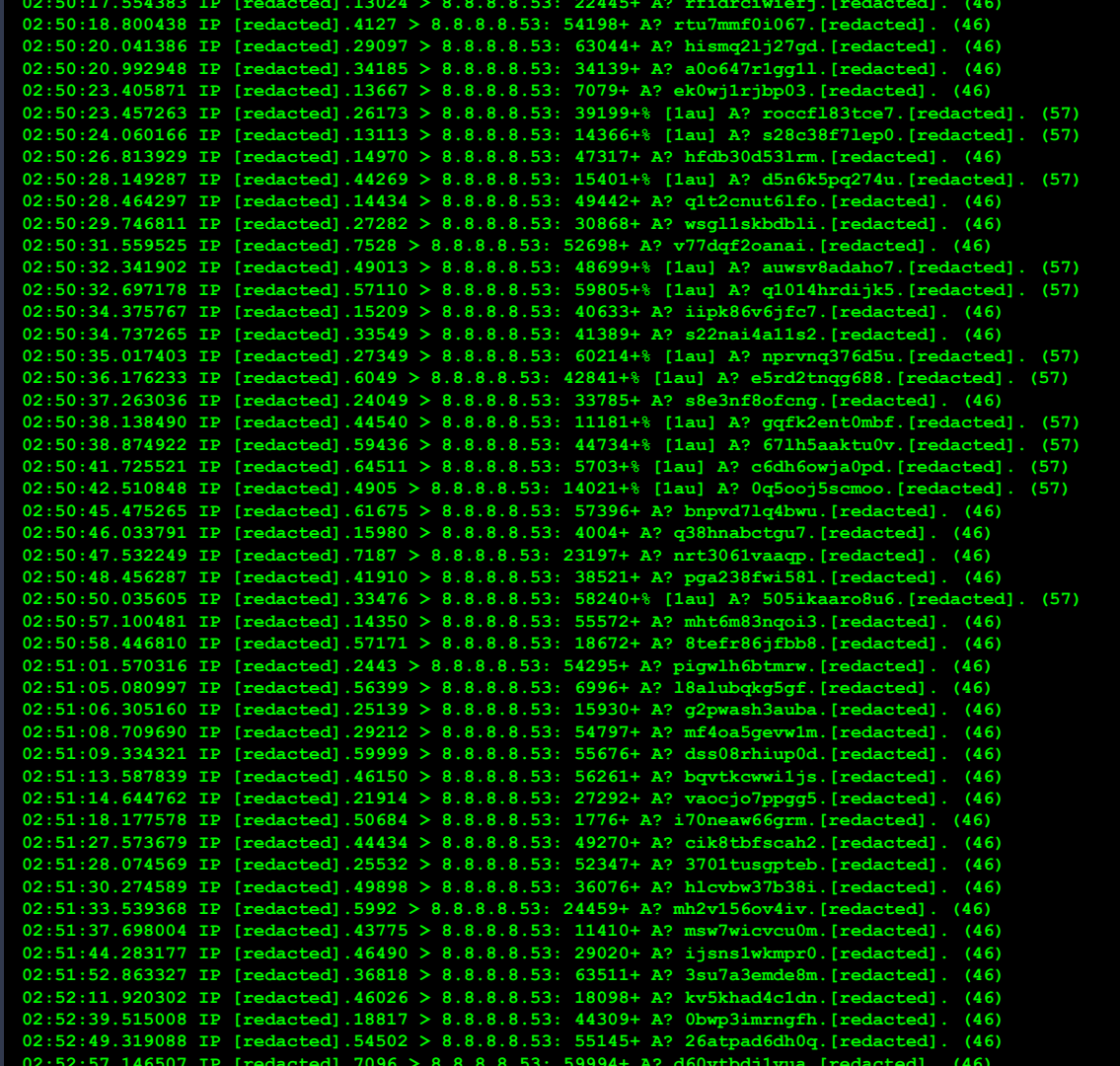
> We ended up enabling a DDoS policy in our firewall specifically target sources from the Google subnets above on port 53.
>
> Unfortunately, this is causing valid traffic from Google to be dropped. It is impacting us directly and all of our clients on our external DNS offering.

DDoS mitigation

Advanced strategies

NSEC/NSEC3 can mitigate cache-busting attacks

ECS (client-subnet): respond with the broadest CIDR possible



Incident reports

During event

Report early; Report often

Report facts, not guesses

Seek help from others in the community

Incident reports

After event

Community can help with timelines

Don't lie — including sins of omission

Main takeaways

Don't assume DNS outages are caused by DDoS *even if you see an increase in traffic*

Blocking the wrong queries can make the situation a lot worse

DNSSEC can benefit availability due to caching of NSEC/NSEC3 records

Consider the system as a whole, including recursives: TTL and ECS have a huge impact on the *effective* capacity of an authoritative server