

DNS DDoS Challenges and Mitigations

Damian Menscher



Site Reliability Engineering

Presented at OAROnline 35a



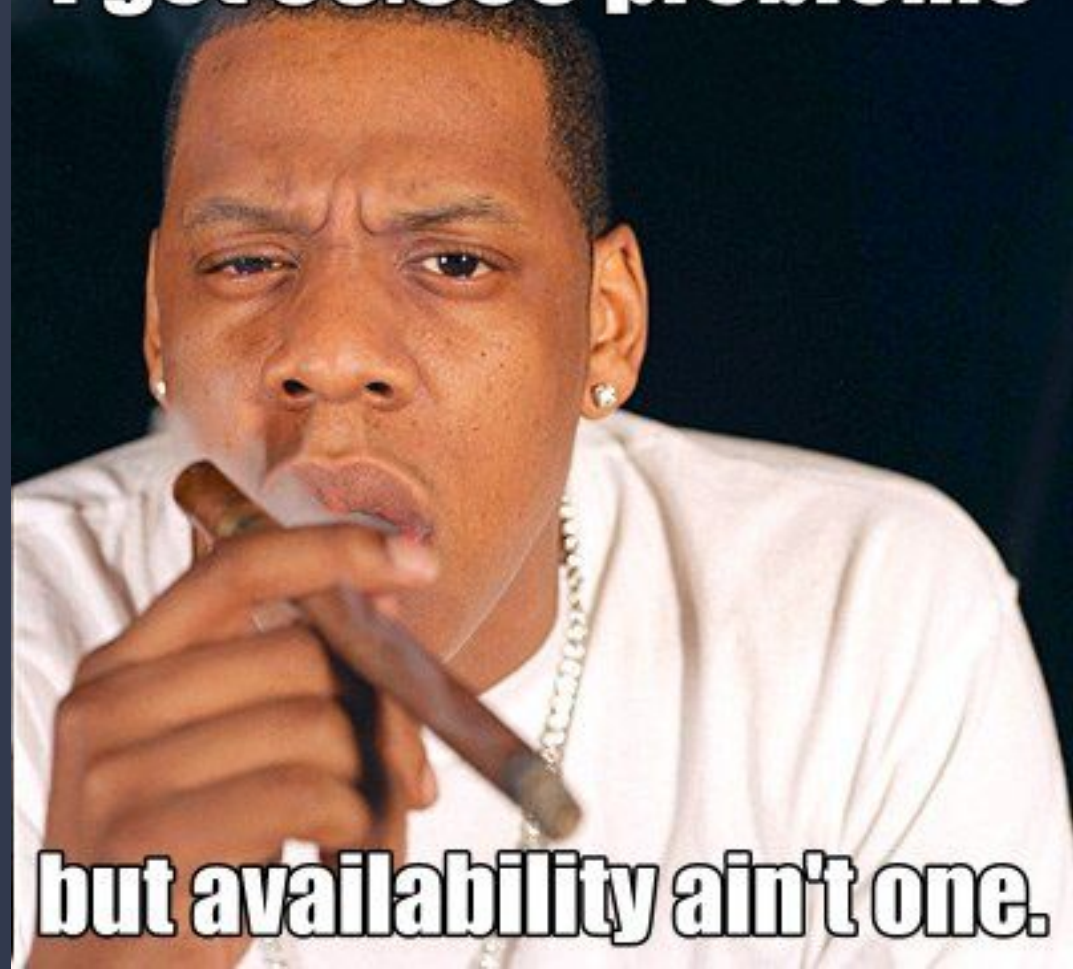
\$ whoami

Security Reliability Engineer

Focused on DDoS defense

Not a DNS expert

I got 99.999 problems



but availability ain't one.

Agenda

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

THE RUMORS ARE TRUE. GOOGLE
WILL BE SHUTTING DOWN PLUS—
ALONG WITH HANGOUTS, PHOTOS,
VOICE, DOCS, DRIVE, MAPS, GMAIL,
CHROME, ANDROID, AND SEARCH—
TO FOCUS ON OUR CORE PROJECT:
THE 8.8.8.8 DNS SERVER.



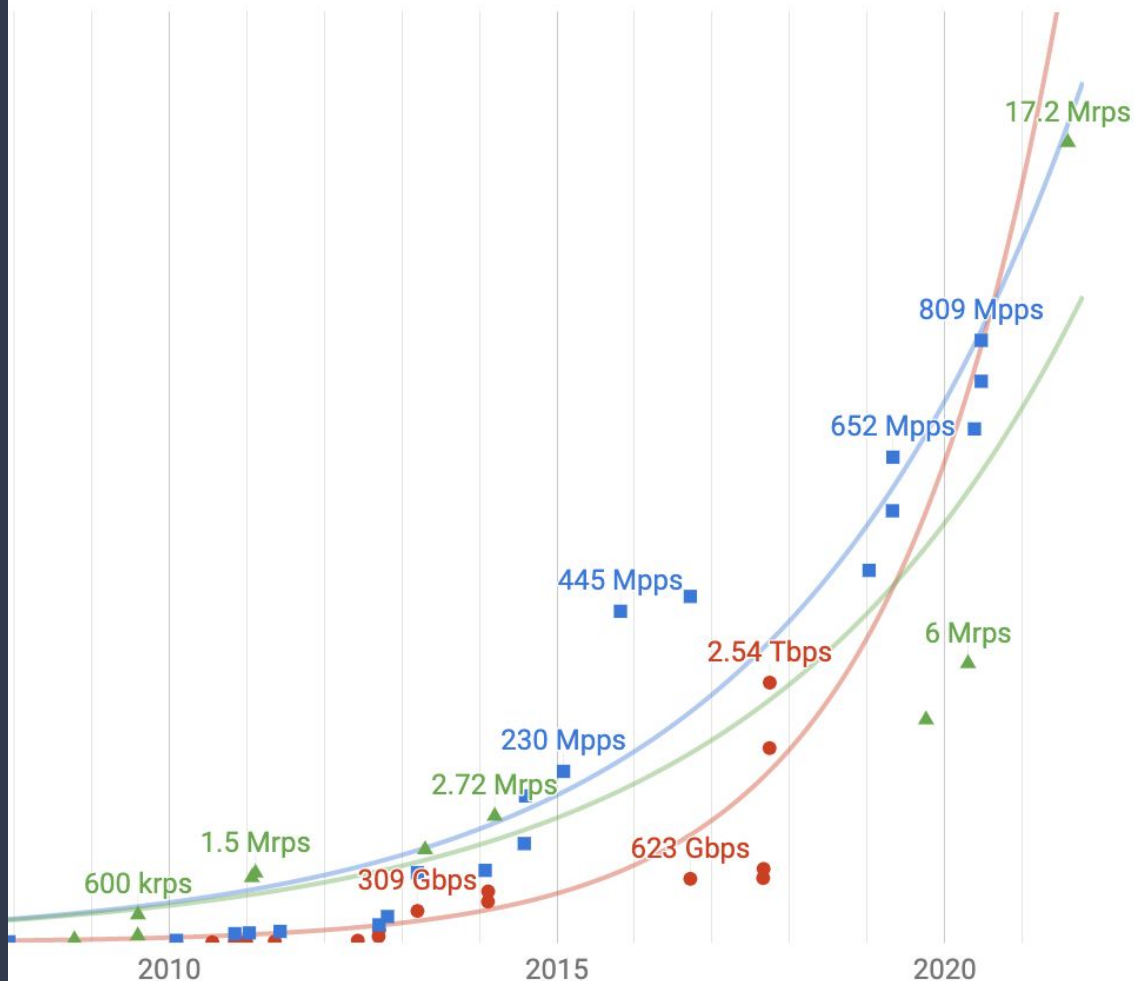
Theory

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.



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



Darrell Etherington, Kate Conger



/ 5:31 AM PDT • October 21, 2016

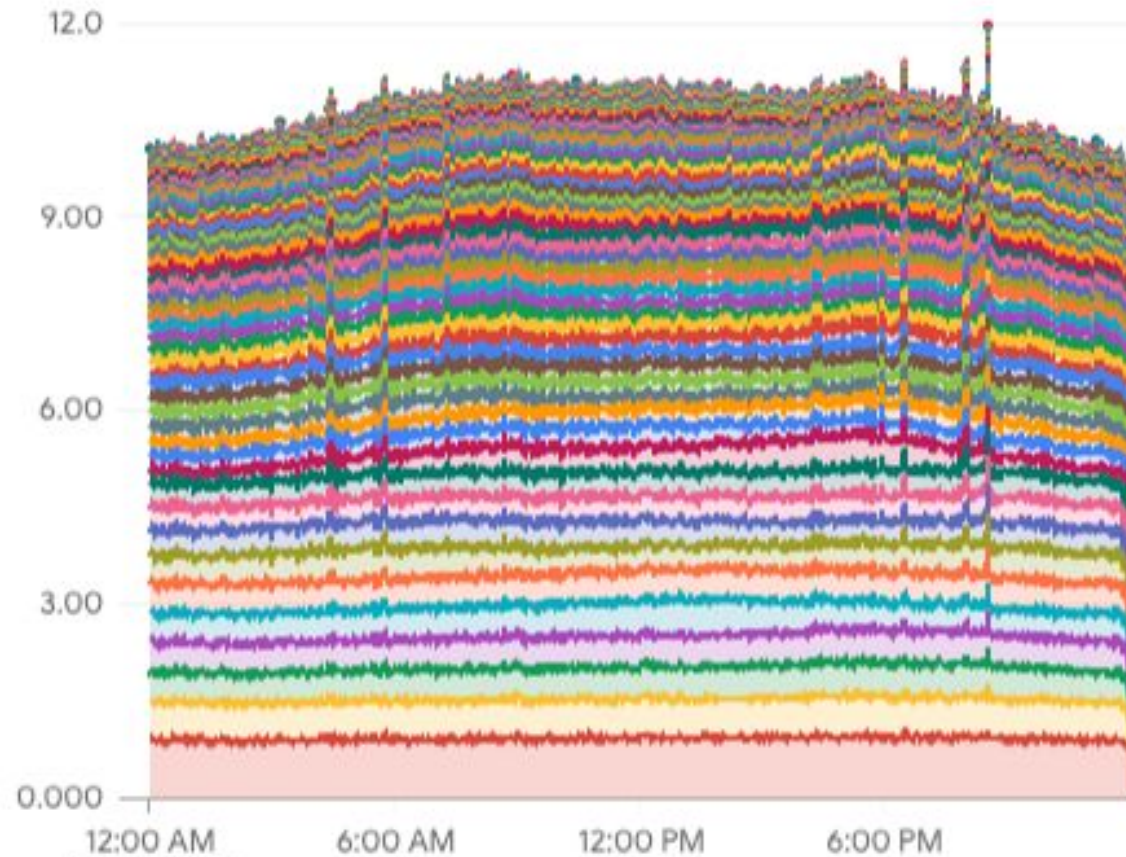
Comment

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

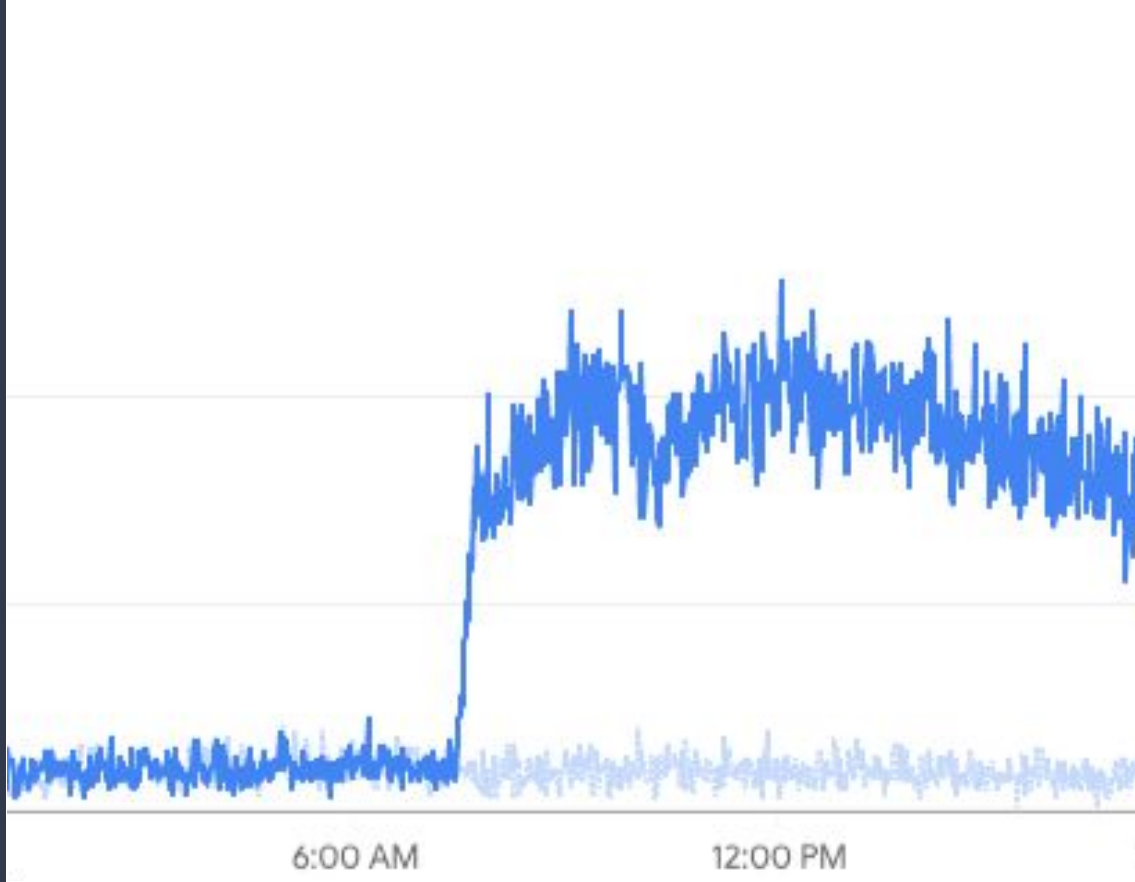
Challenges for recursives

Dealing with authoritative servers

Failures lead to retries

Benefits of throttling??

0-TTL responses



Auth server outages

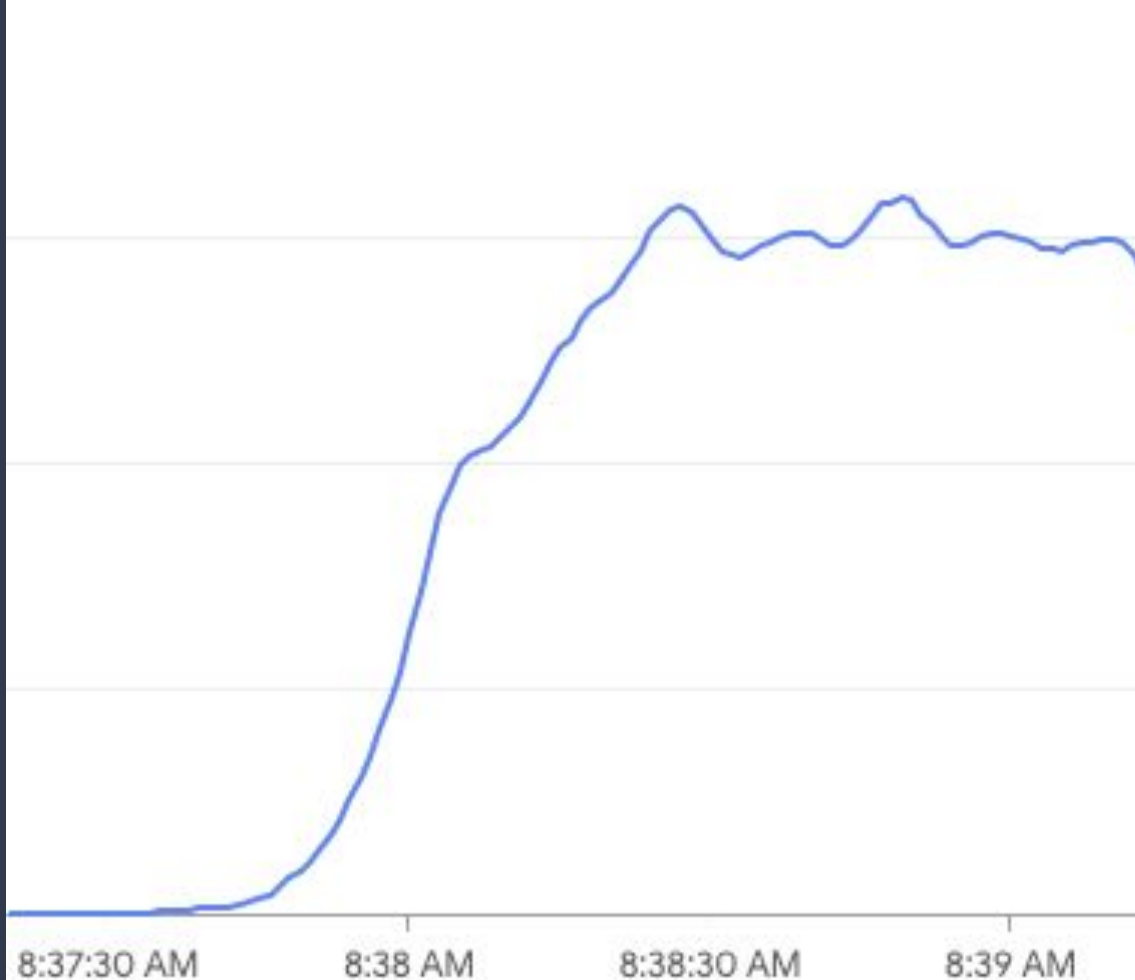
Common outage scenario

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 ST

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

```
02:50:17.554383 IP [redacted].13024 > 8.8.8.8.53: 22445+ A? rridrciwierrj.[redacted]. (46)
02:50:18.800438 IP [redacted].4127 > 8.8.8.8.53: 54198+ A? rtu7mmf0i067.[redacted]. (46)
02:50:20.041386 IP [redacted].29097 > 8.8.8.8.53: 63044+ A? hismq2lj27gd.[redacted]. (46)
02:50:20.992948 IP [redacted].34185 > 8.8.8.8.53: 34139+ A? a0o647rlgg1l.[redacted]. (46)
02:50:23.405871 IP [redacted].13667 > 8.8.8.8.53: 7079+ A? ek0wj1rjbp03.[redacted]. (46)
02:50:23.457263 IP [redacted].26173 > 8.8.8.8.53: 39199+ [1au] A? roccfl83tce7.[redacted]. (57)
02:50:24.060166 IP [redacted].13113 > 8.8.8.8.53: 14366+ [1au] A? s28c38f7lep0.[redacted]. (57)
02:50:26.813929 IP [redacted].14970 > 8.8.8.8.53: 47317+ A? hfdb30d53lrm.[redacted]. (46)
02:50:28.149287 IP [redacted].44269 > 8.8.8.8.53: 15401+ [1au] A? d5n6k5pq274u.[redacted]. (57)
02:50:28.464297 IP [redacted].14434 > 8.8.8.8.53: 49442+ A? qlt2cnut6lifo.[redacted]. (46)
02:50:29.746811 IP [redacted].27282 > 8.8.8.8.53: 30868+ A? wsgllskbdbli.[redacted]. (46)
02:50:31.559525 IP [redacted].7528 > 8.8.8.8.53: 52698+ A? v77dqf2oanai.[redacted]. (46)
02:50:32.341902 IP [redacted].49013 > 8.8.8.8.53: 48699+ [1au] A? auwsv8adaho7.[redacted]. (57)
02:50:32.697178 IP [redacted].57110 > 8.8.8.8.53: 59805+ [1au] A? ql014hrdijj5.[redacted]. (57)
02:50:34.375767 IP [redacted].15209 > 8.8.8.8.53: 40633+ A? iipk86v6jfc7.[redacted]. (46)
02:50:34.737265 IP [redacted].33549 > 8.8.8.8.53: 41389+ A? s22nai4all52.[redacted]. (46)
02:50:35.017403 IP [redacted].27349 > 8.8.8.8.53: 60214+ [1au] A? nprvng376d5u.[redacted]. (57)
02:50:36.176233 IP [redacted].6049 > 8.8.8.8.53: 42841+ [1au] A? e5rd2tnqg688.[redacted]. (57)
02:50:37.263036 IP [redacted].24049 > 8.8.8.8.53: 33785+ A? s8e3nf8ofcng.[redacted]. (46)
02:50:38.138490 IP [redacted].44540 > 8.8.8.8.53: 11181+ [1au] A? gqfk2ent0mbf.[redacted]. (57)
02:50:38.874922 IP [redacted].59436 > 8.8.8.8.53: 44734+ [1au] A? 671h5aaktu0v.[redacted]. (57)
02:50:41.725521 IP [redacted].64511 > 8.8.8.8.53: 5703+ [1au] A? c6dh6owja0pd.[redacted]. (57)
02:50:42.510848 IP [redacted].4905 > 8.8.8.8.53: 14021+ [1au] A? 0q5ooj5scmoo.[redacted]. (57)
02:50:45.475265 IP [redacted].61675 > 8.8.8.8.53: 57396+ A? bnpvd7lq4bwu.[redacted]. (46)
02:50:46.033791 IP [redacted].15980 > 8.8.8.8.53: 4004+ A? q38hnabctgu7.[redacted]. (46)
02:50:47.532249 IP [redacted].7187 > 8.8.8.8.53: 23197+ A? nrt306lvaagp.[redacted]. (46)
02:50:48.456287 IP [redacted].41910 > 8.8.8.8.53: 38521+ A? pga238fwi58l.[redacted]. (46)
02:50:50.035605 IP [redacted].33476 > 8.8.8.8.53: 58240+ [1au] A? 505ikaaro8u6.[redacted]. (57)
02:50:57.100481 IP [redacted].14350 > 8.8.8.8.53: 55572+ A? mht6m83nqoi3.[redacted]. (46)
02:50:58.446810 IP [redacted].57171 > 8.8.8.8.53: 18672+ A? 8tefr86jfb88.[redacted]. (46)
02:51:01.570316 IP [redacted].2443 > 8.8.8.8.53: 54295+ A? pigwlh6btmrw.[redacted]. (46)
02:51:05.080997 IP [redacted].56399 > 8.8.8.8.53: 6996+ A? l8alubqkg5gf.[redacted]. (46)
02:51:06.305160 IP [redacted].25139 > 8.8.8.8.53: 15930+ A? g2pwash3auba.[redacted]. (46)
02:51:08.709690 IP [redacted].29212 > 8.8.8.8.53: 54797+ A? mf4oa5gevv1m.[redacted]. (46)
02:51:09.334321 IP [redacted].59999 > 8.8.8.8.53: 55676+ A? dss08rhiup0d.[redacted]. (46)
02:51:13.587839 IP [redacted].46150 > 8.8.8.8.53: 56261+ A? bqvtkcwwiljs.[redacted]. (46)
02:51:14.644762 IP [redacted].21914 > 8.8.8.8.53: 27292+ A? vaocjo7ppgg5.[redacted]. (46)
02:51:18.177578 IP [redacted].50684 > 8.8.8.8.53: 1776+ A? i70neaw66grm.[redacted]. (46)
02:51:27.573679 IP [redacted].44434 > 8.8.8.8.53: 49270+ A? cik8tbfscah2.[redacted]. (46)
02:51:28.074569 IP [redacted].25532 > 8.8.8.8.53: 52347+ A? 3701tusgpteb.[redacted]. (46)
02:51:30.274589 IP [redacted].49898 > 8.8.8.8.53: 36076+ A? hlcvbw37b38i.[redacted]. (46)
02:51:33.539368 IP [redacted].5992 > 8.8.8.8.53: 24459+ A? mh2v156ov4iv.[redacted]. (46)
02:51:37.698004 IP [redacted].43775 > 8.8.8.8.53: 11410+ A? msw7wicvcu0m.[redacted]. (46)
02:51:44.283177 IP [redacted].46490 > 8.8.8.8.53: 29020+ A? ijsns1wkmp0.[redacted]. (46)
02:51:52.863327 IP [redacted].36818 > 8.8.8.8.53: 63511+ A? 3su7a3emde8m.[redacted]. (46)
02:52:11.920302 IP [redacted].46026 > 8.8.8.8.53: 18098+ A? kv5khad4cldn.[redacted]. (46)
02:52:39.515008 IP [redacted].18817 > 8.8.8.8.53: 44309+ A? 0bwp3imrngfh.[redacted]. (46)
02:52:49.319088 IP [redacted].54502 > 8.8.8.8.53: 55145+ A? 26atpad6dh0q.[redacted]. (46)
02:52:57.146507 IP [redacted].7096 > 8.8.8.8.53: 59994+ A? d60vrbdi1yua.[redacted]. (46)
```


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

ABOUT | RSS

cyberscoop

BROUGHT

T

TRANSPORTATION

HEALTHCARE

TECHNOLOGY

FINANCIAL

WATCH

LISTEN

EVEN

After Dyn cyberattack, lawmakers seek best path forward



(From left to right) Level 3 Communications' chief security officer Dale Drew, computer security luminary Bruce Schneier and university of Michigan's Dr. Kevin Fu / Credit: C-Span video

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

