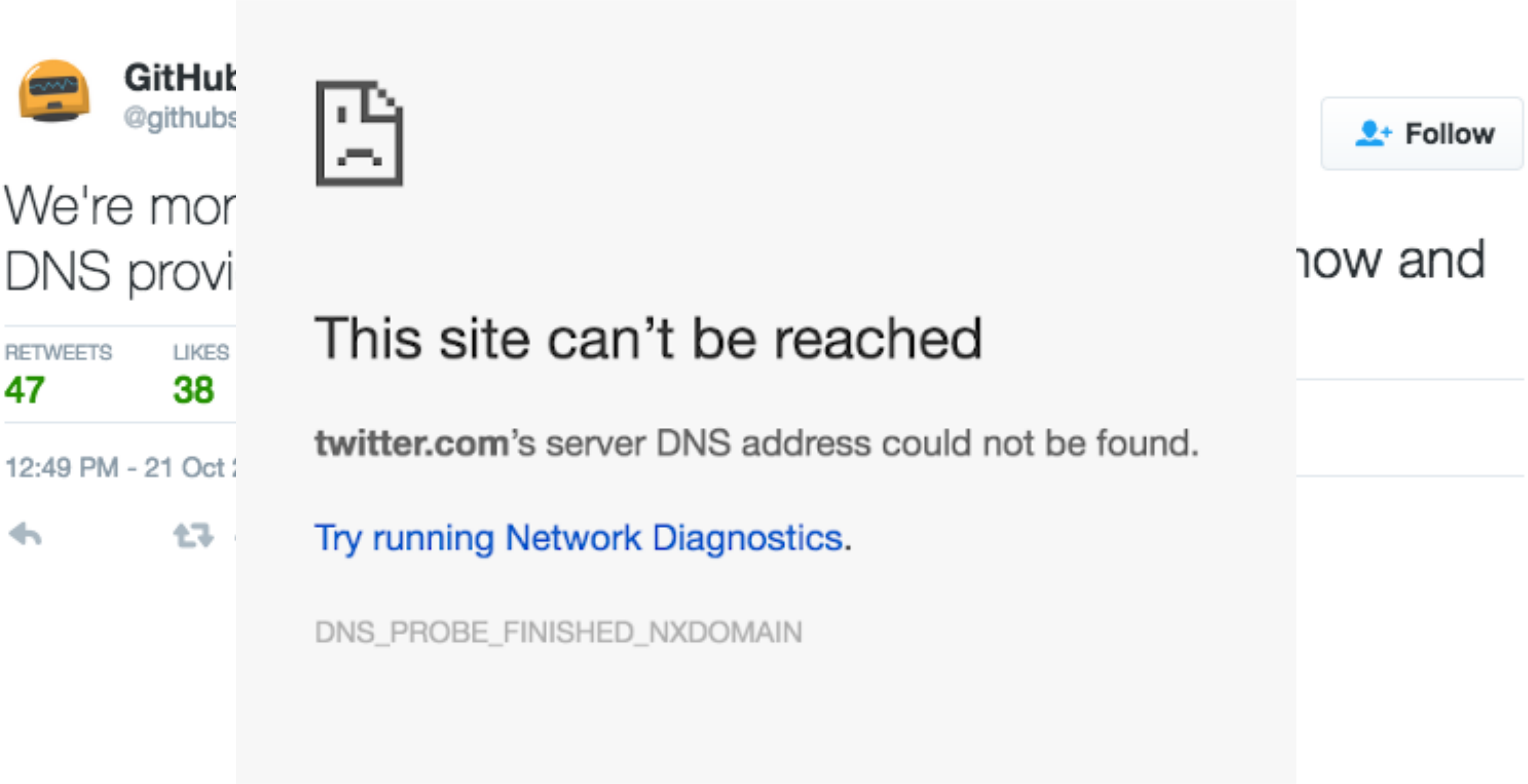
Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident?

Aqsa Kashaf, Vyas Sekar, Yuvraj Agarwal

Carnegie Mellon University

Mirai-Dyn Attack 2016



GitHub

@githubs

Follow

We're mor

DNS provi

now and

RETWEETS 47 LIKES 38

12:49 PM - 21 Oct

This site can’t be reached

twitter.com’s server DNS address could not be found.

Try running Network Diagnostics.

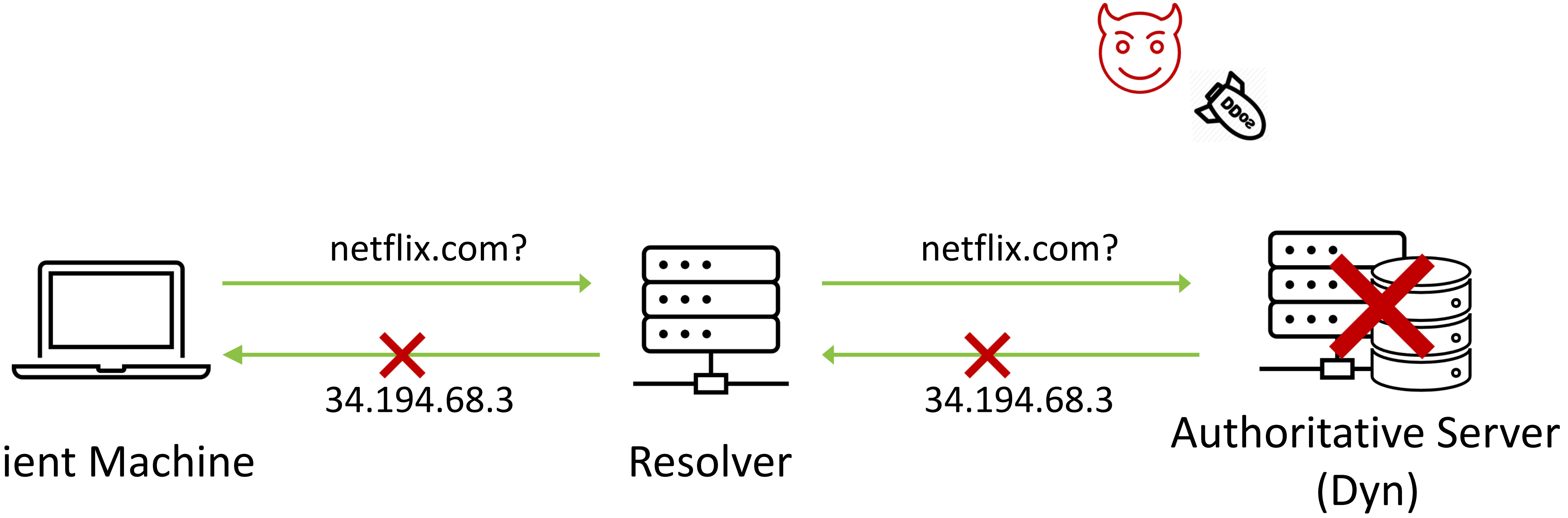
DNS_PROBE_FINISHED_NXDOMAIN

Mirai-Dyn Attack 2016

amazon.com
slack
yelp
BBC NEWS
VISA
SOUNDCLOUD
Quora
Etsy
imgur
tumblr.

How was it possible to take all of these websites down?

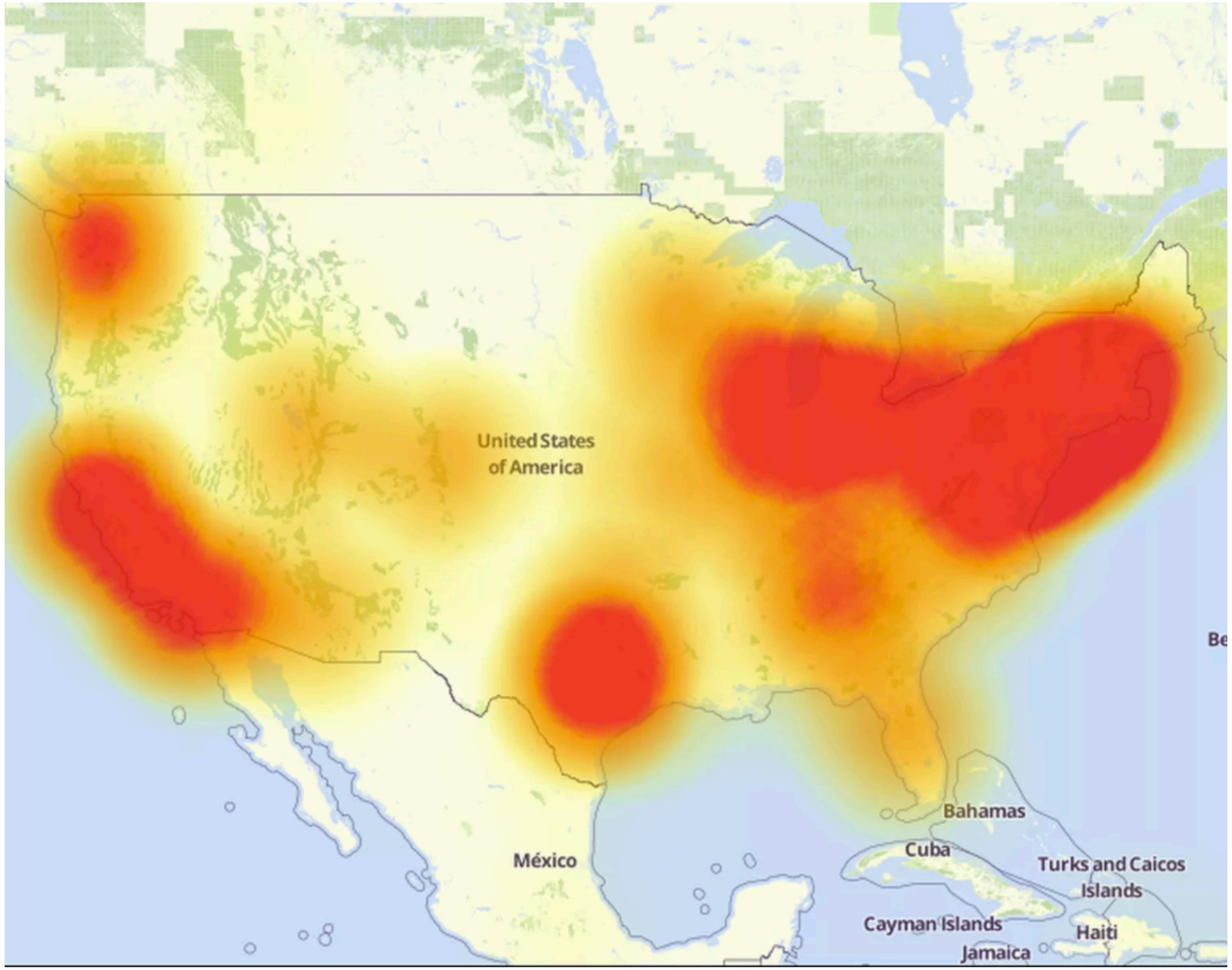
Mirai-Dyn Attack 2016



Insight: Many websites relied on the **same** 3rd Party DNS provider (Dyn)

Mirai-Dyn Attack 2016

- 178,000 domains affected in total
- Tens of millions of users affected



Motivating Questions for Our Work

- How prevalent are third party dependencies?

  Methodology: Analysis on Alexa Top 100K websites

- Are there any indirect dependencies between websites and third-party providers?

  Methodology: Analysis on inter-service dependencies

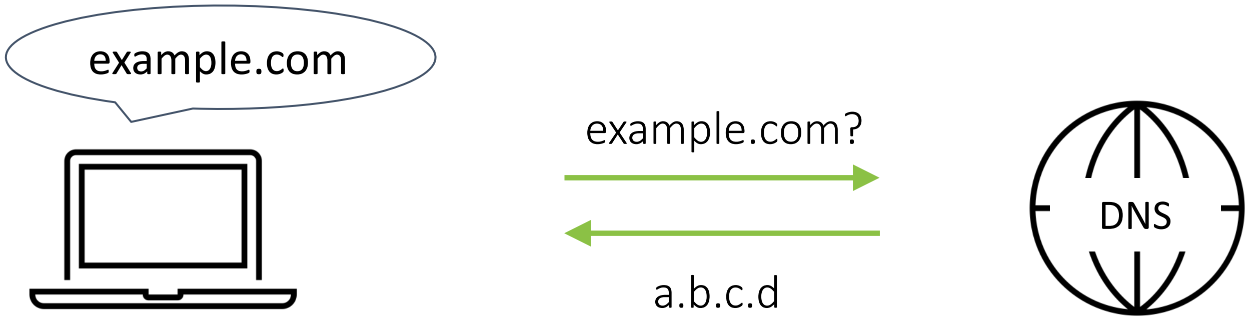
- How did the world change after the Dyn Incident?

  Methodology: Comparison analysis on Alexa Top 100K sites in 2016 vs. 2020

Life Cycle of a Web Request

- Domain Name System (DNS)

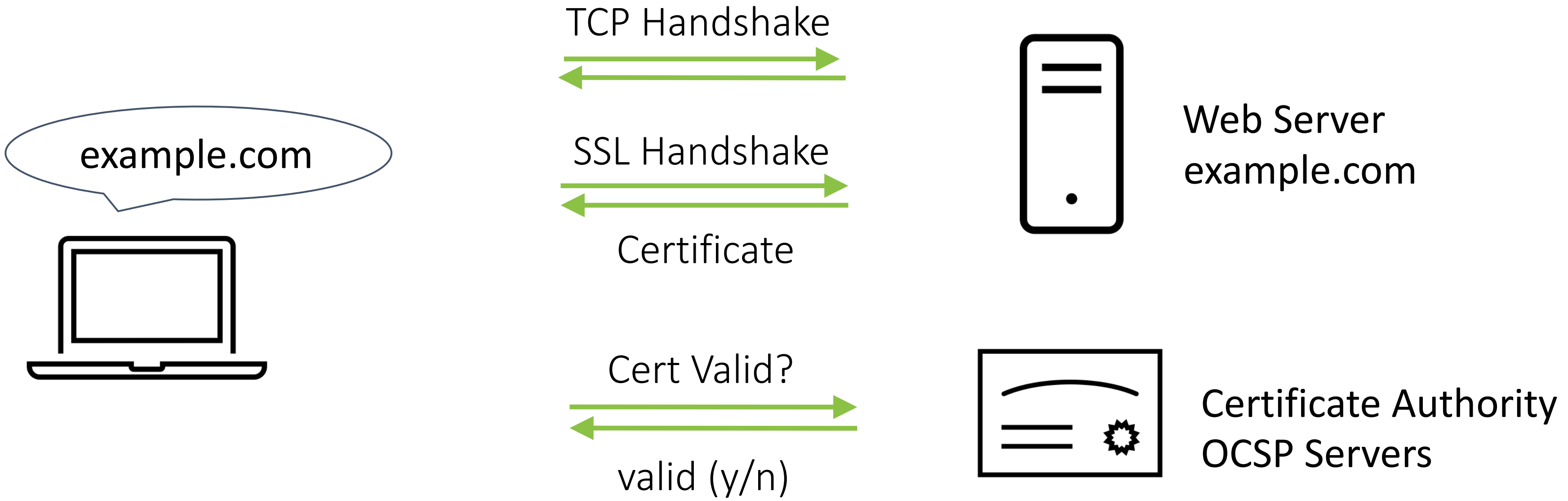
For example, AWS DNS, Dyn.



Life Cycle of a Web Request

- Domain Name System (DNS)
- Certificate Validation by CA

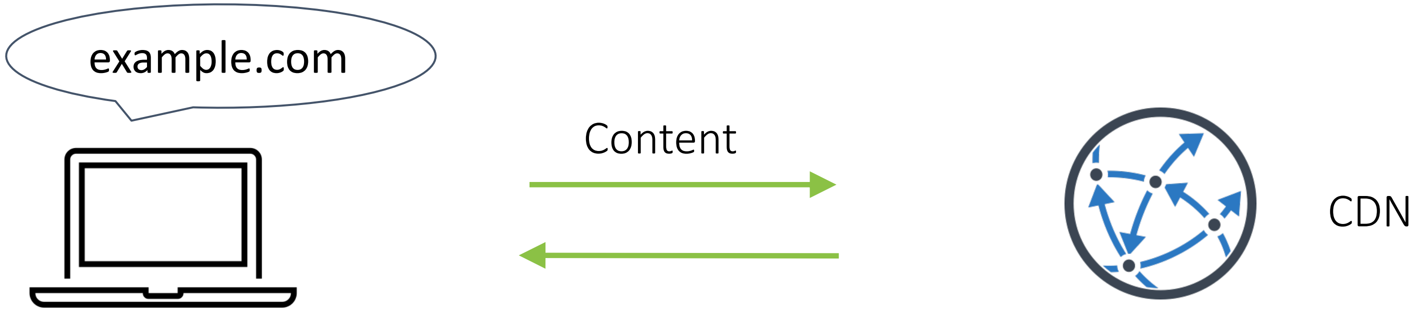
For example, DigiCert, Let’s Encrypt.



Life Cycle of a Web Request

- Domain Name System (DNS)
- Certificate Validation by CA
- Content Delivery Network (CDN)

For example, Akamai, CloudFlare



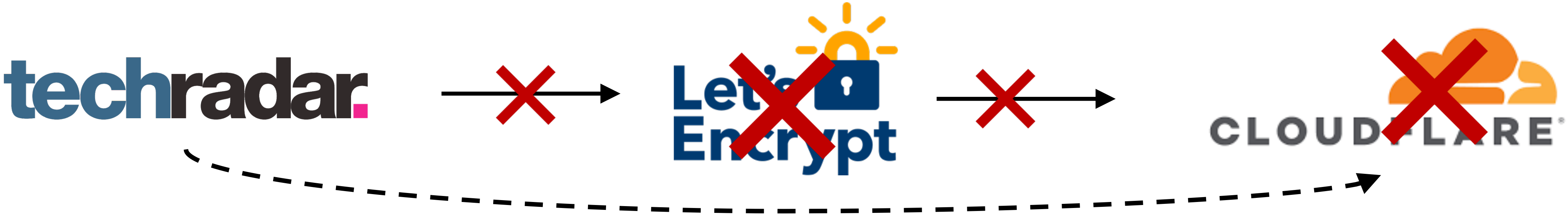
example.com

Content

CDN

Methodology: What to measure?

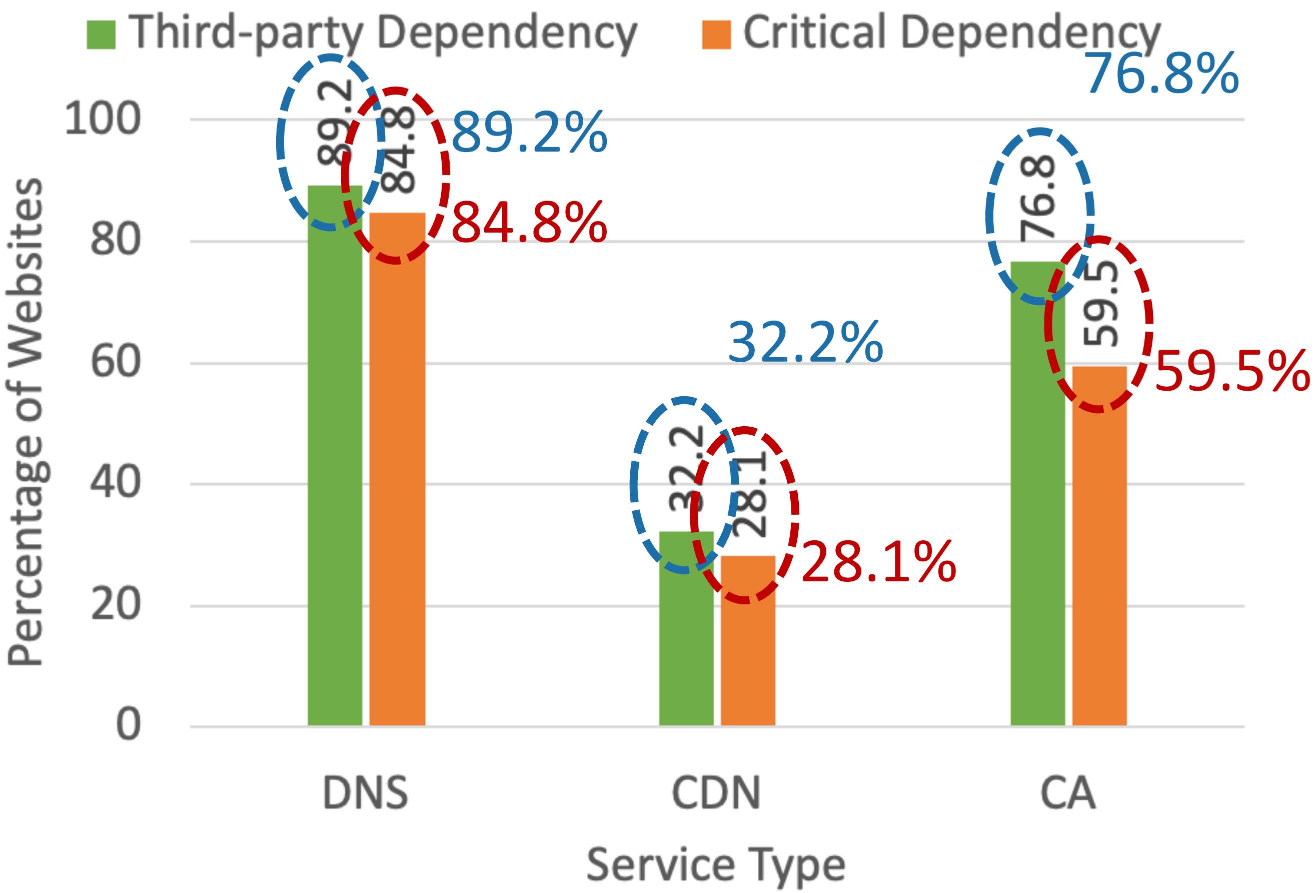
- Third Party Dependency
- Indirect Dependency
- Critical Dependency
  - No Redundancy in DNS and CDN provisioning
  - No OCSP stapling in certificate validation



Indirect Dependency

Q1: How prevalent are third-party dependencies?

Prevalence of Third-Party Dependencies



89.2%

84.8%

32.2%

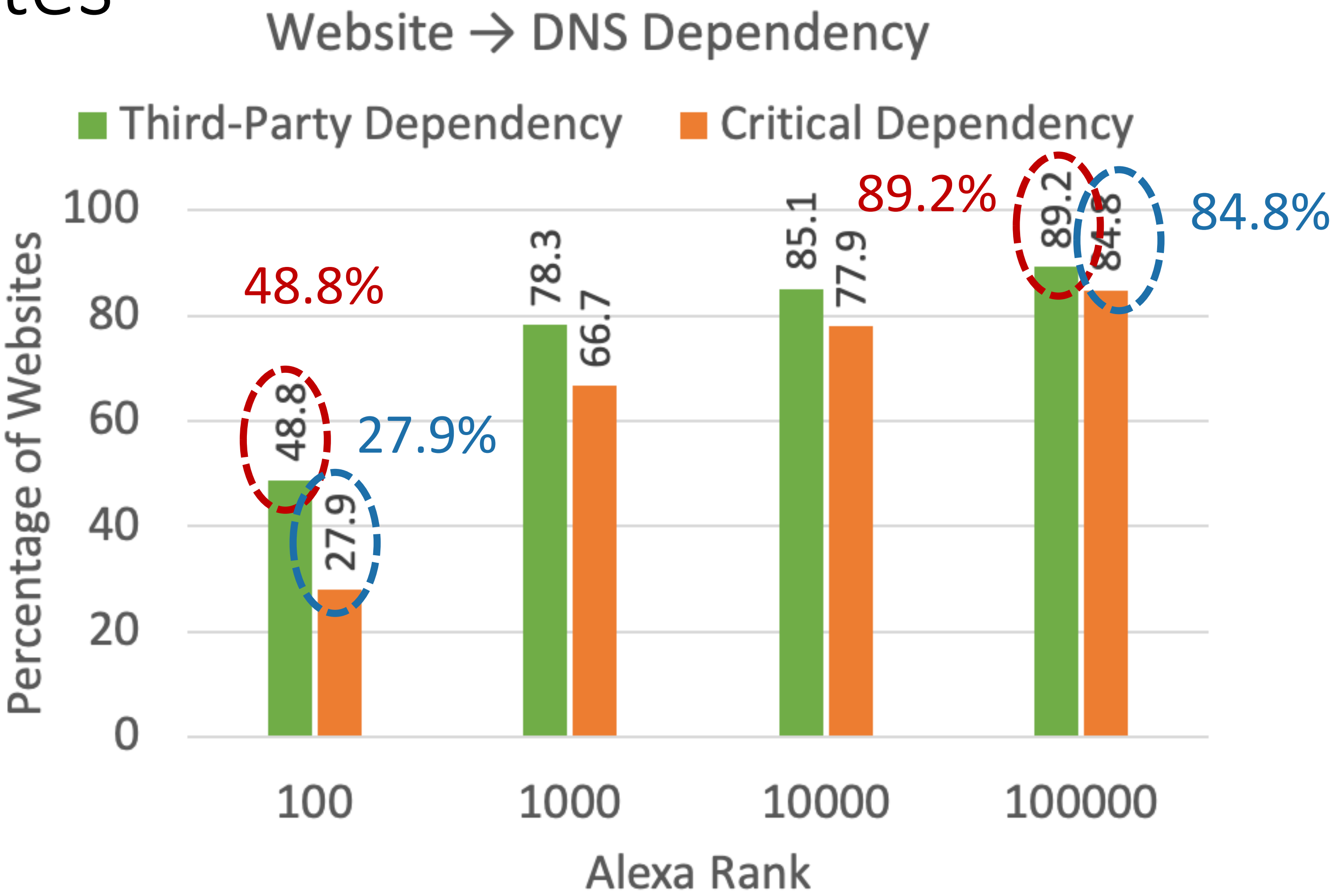
28.1%

76.8%

59.5%

89% of the top-100K websites critically depend on third-party DNS, CDN, or CA providers.

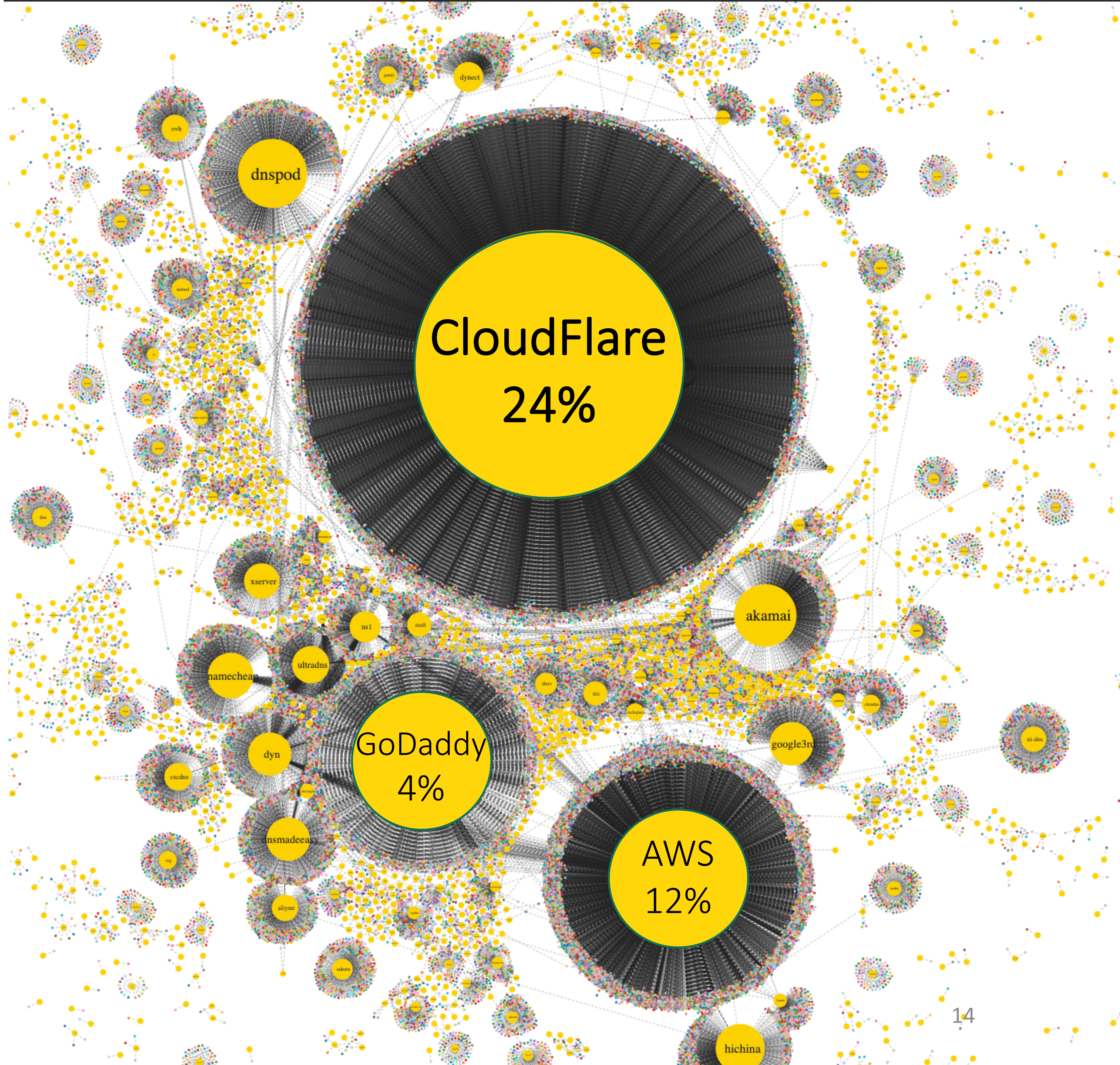
Third-Party Dependencies Higher for Less Popular Websites



Popular websites care more about availability.

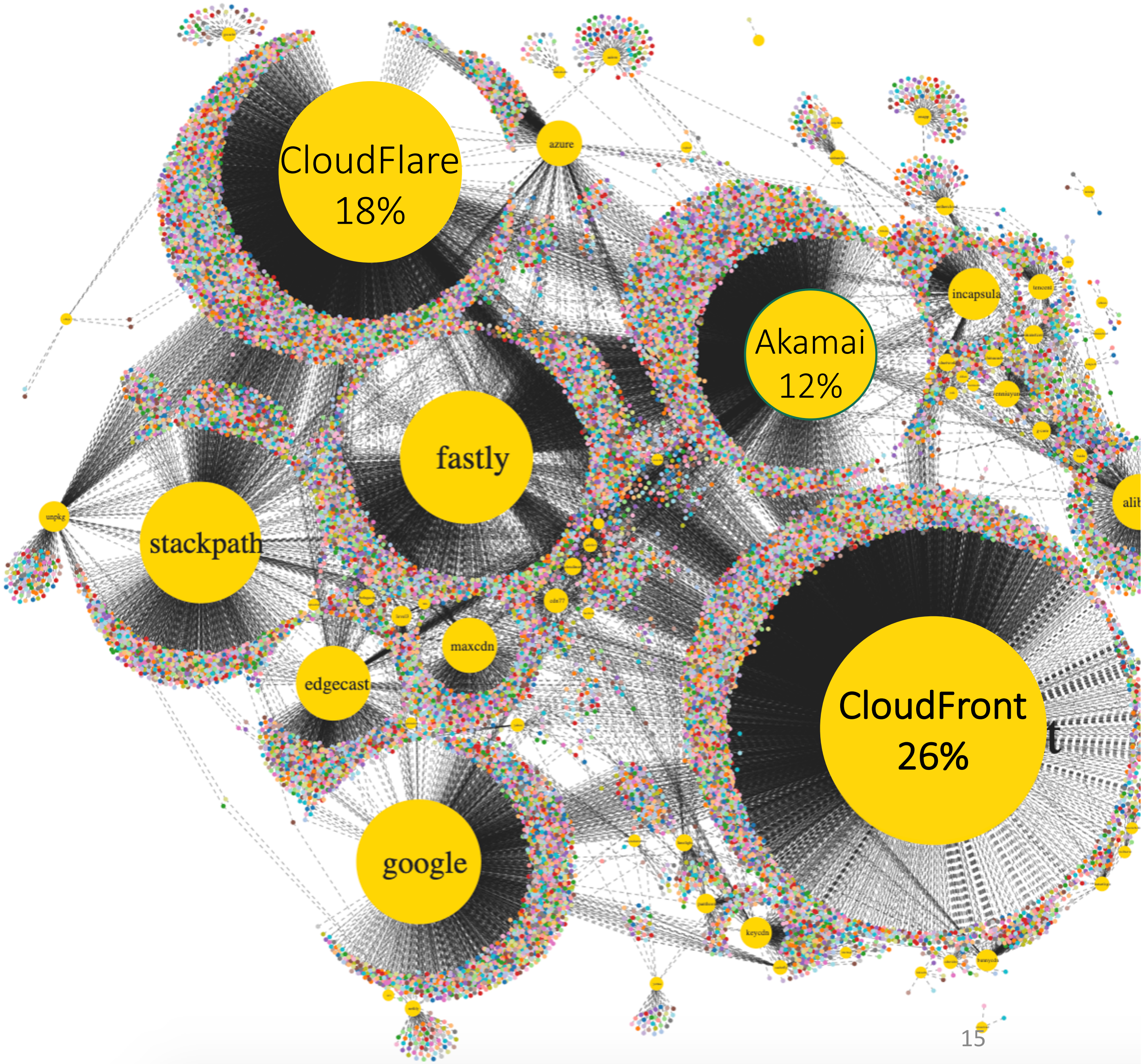
Concentration of DNS Providers

3 (out of 10K) DNS providers critically serve ~40% of the top-100K websites

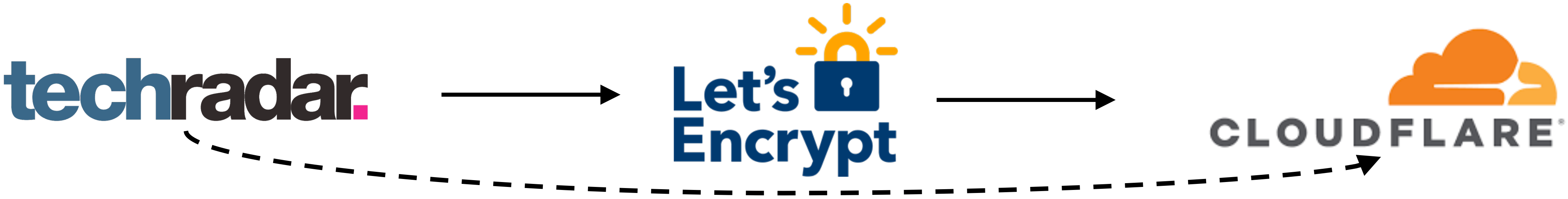


Concentration of CDN Providers

3 (out of 86) CDN providers critically serve ~60% of the top-100K websites using CDN



Q2: Are there any indirect dependencies between websites and their third-party providers?



Indirect Dependency

Inter-Service Third-Party Dependency

48%	36%	36%
CA → DNS	CA → CDN	CDN → DNS

Third-party dependencies are also prevalent among service providers

Inter-Service Critical Dependencies

31%

CA → DNS

36%

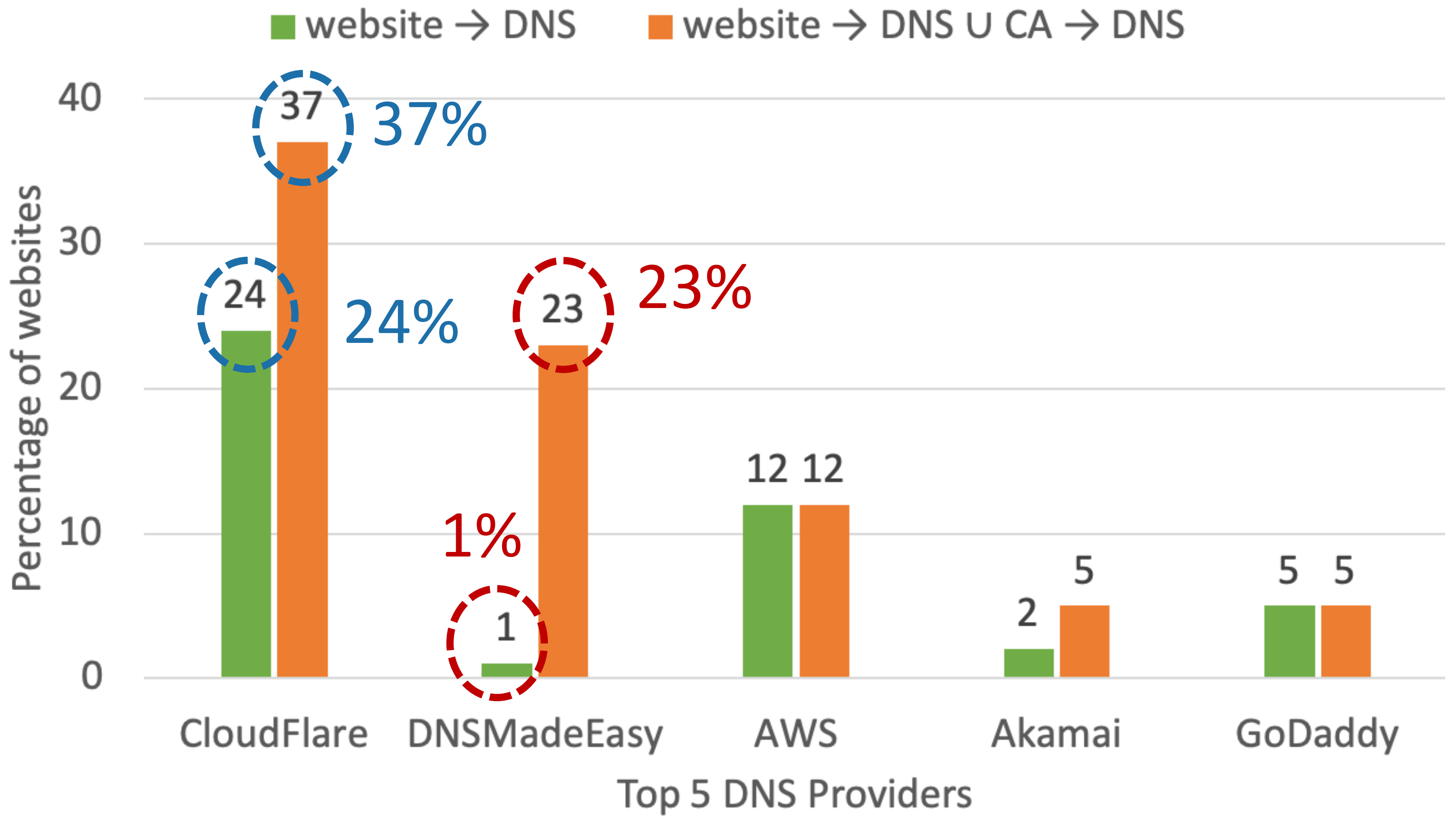
CA → CDN

17%

CDN → DNS

Due to inter-service **critical dependencies**, websites have indirect dependencies on service providers

Impact of Indirect Dependencies



Indirect Dependencies further amplify provider concentration

Q3: How did the world change after the Dyn incident in 2016?

Critical Dependency of Websites (2016 to 2020)

+4.7%	0%	-0.2%
website → DNS	website → CDN	website → CA

No improvement in the prevalence of third-party dependency. Critical dependency increased in DNS

Inter-Service Critical Dependency (2016 to 2020)

-8.6%

CA → DNS

0%

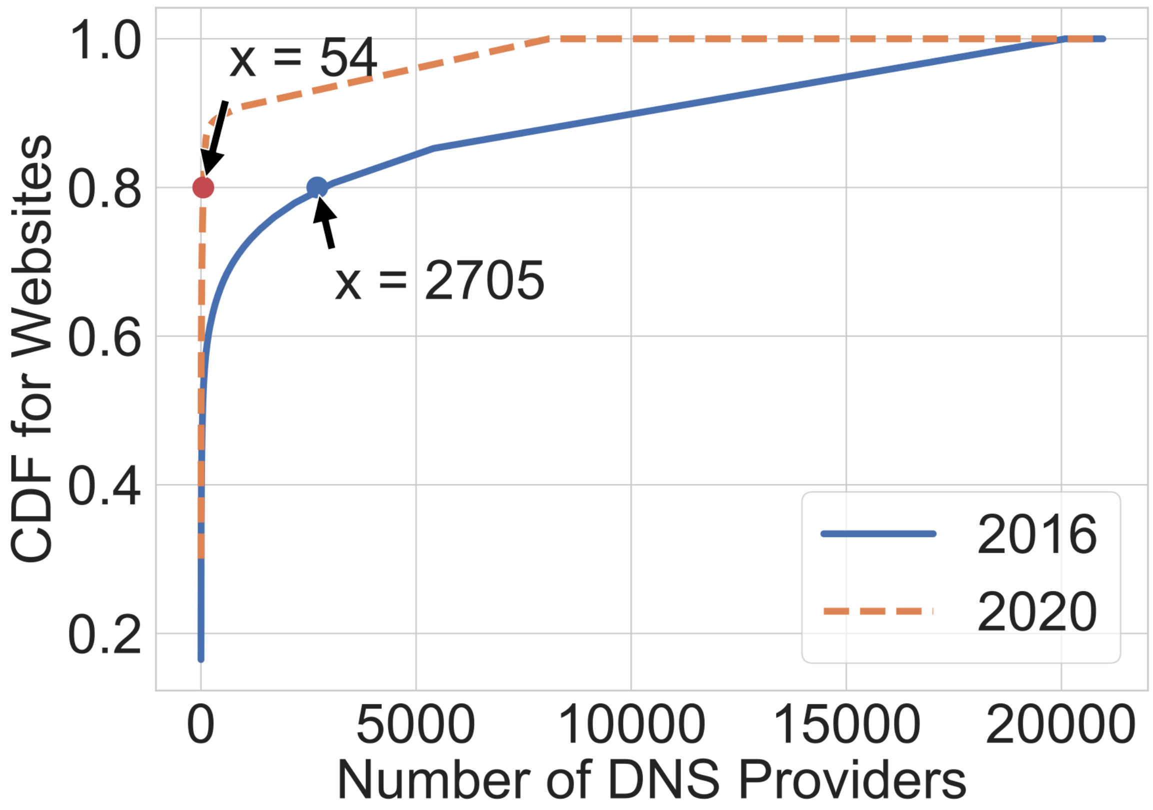
CA → CDN

-4.3%

CDN → DNS

Critical dependency decreased in service providers

Change in Concentration of DNS Providers



Single-points-of-failure got bigger in DNS and CA!

Limitations

- Measurements from a single vantage point
  - May miss region specific dependencies
- Analyze dependencies on landing pages only
  - May miss dependencies that manifest deeper
- Do not look at physical and network dependencies
  - For example, routing, hosting etc.

Our Recommendations

Websites

- Redundancy when using third party providers
- Understand their indirect dependencies

Service Providers

- Support and encourage redundancy
- Be careful about their inter-service dependencies
- Be more transparent about attacks

Conclusion

- DDoS attack on Dyn exposed the fragility of the Web due to dependencies
- Is this a one off? Are there more problems? Has the world changed?
- Our work: Analyze third-party and inter-service dependencies
- Our Key Findings:
  - **Prevalence of third-party dependency:**
    89% of top 100K websites are critically dependent
    An attack on a single provider can take down ~30% of the websites
  - **Impact of indirect dependencies:**
    Can cause ~23X amplification in provider concentration
  - **Change after the Dyn Incident:**
    No significant change in website dependencies
    Decrease in inter-service critical dependencies by up to 8%

Code: github.com/AqsaKashaf/Analyzing-Third-party-Dependencies.git