Impact of DoS attacks on authoritative DNS servers

Internet Measurements

Wintersemester 2023/24

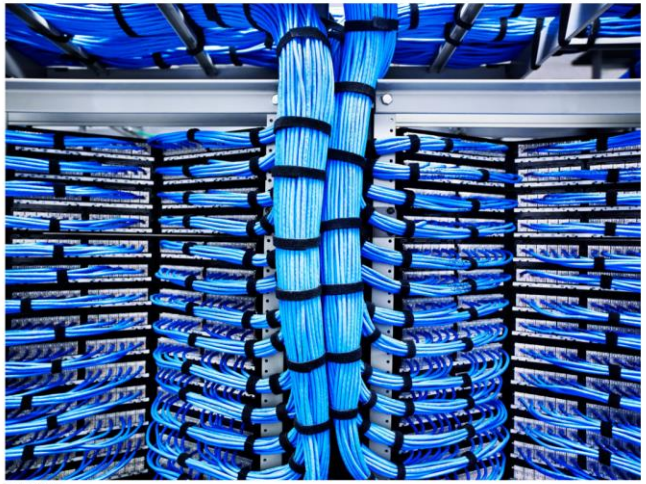
Overview

- Studie kombiniert bereits existierende Datensätze und erhebt eigene Messungen, um Einfluss von DoS-Angriffen gegen authoritative DNS-Server zu analysieren
- Zeitraum vom 1. November 2020 bis 31. März 2022
- Erlaubt Analyse von DoS-Angriffen als Third-Party

LILY HAY NEWMAN SECURITY OCT 21, 2016 1:04 PM

What We Know About Friday's Massive East Coast Internet Outage

DNS service Dyn faces DDoS attacks.

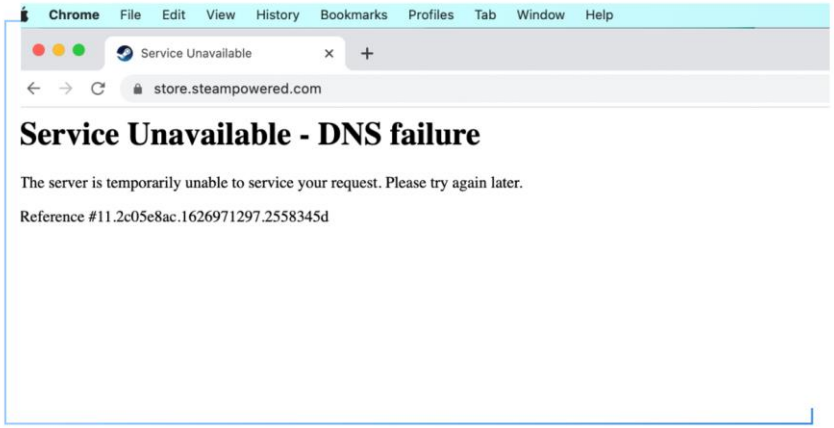


GETTY IMAGES

https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

Akamai DNS outage knocks many major websites and services offline: PSN, Steam, Fidelity, more [U]

Chance Miller | Jul 22 2021 - 9:29 am PT | 0 Comments



https://9to5mac.com/2021/07/22/dns-outage-akamai-steam-chase-and-more/

Cloudflare DNS goes down, taking a large piece of the internet with it

Devin Coldewey @techcrunch / 9:50 PM UTC • July 17, 2020 Comment

Image Credits: mith Collection/Gado / Getty Images

https://techcrunch.com/2020/07/17/cloudflare-dns-goes-down-taking-a-large-piece-of-the-internet-with-it/

BRIAN BARRETT SECURITY FEB 26, 2022 9:00 AM

Security News This Week: DDoS Attempts Hit Russia as Ukraine Conflict Intensifies

Plus: Hacker recruits, NFT thefts, and more of the week's top security news.

PHOTOGRAPH: FUTURE PUBLISHING/GETTY IMAGES

https://www.theregister.com/2023/04/27/microsoft_windows_rust/

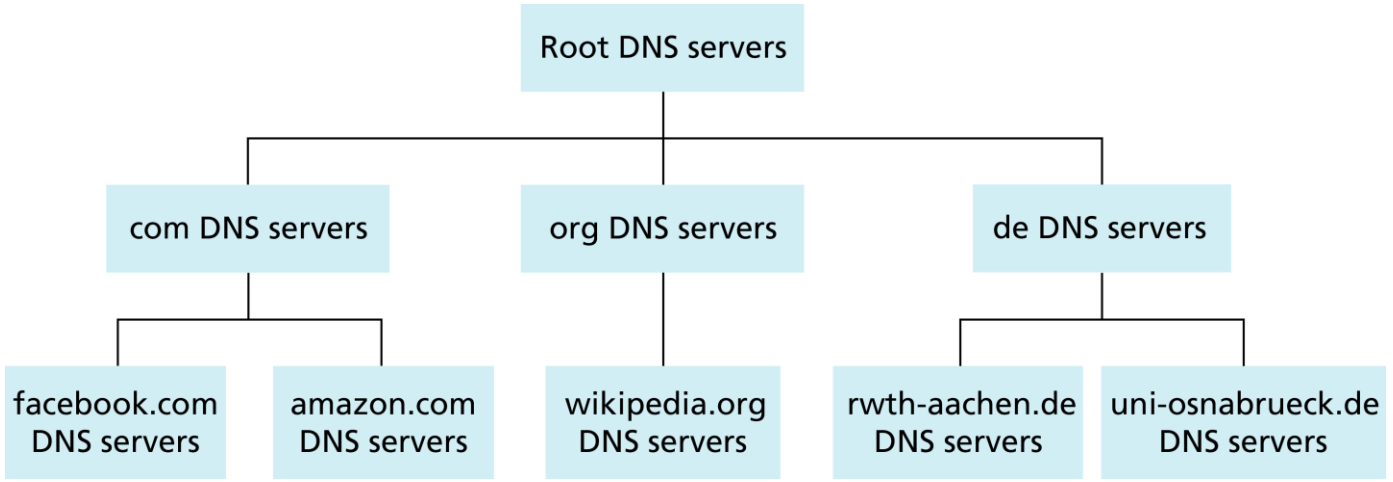
Inhalt

- Grundlagen
- Methodik und Datensätze
- Exemplarische Angriffe
- Überblick über Angriffe
- Best Practices

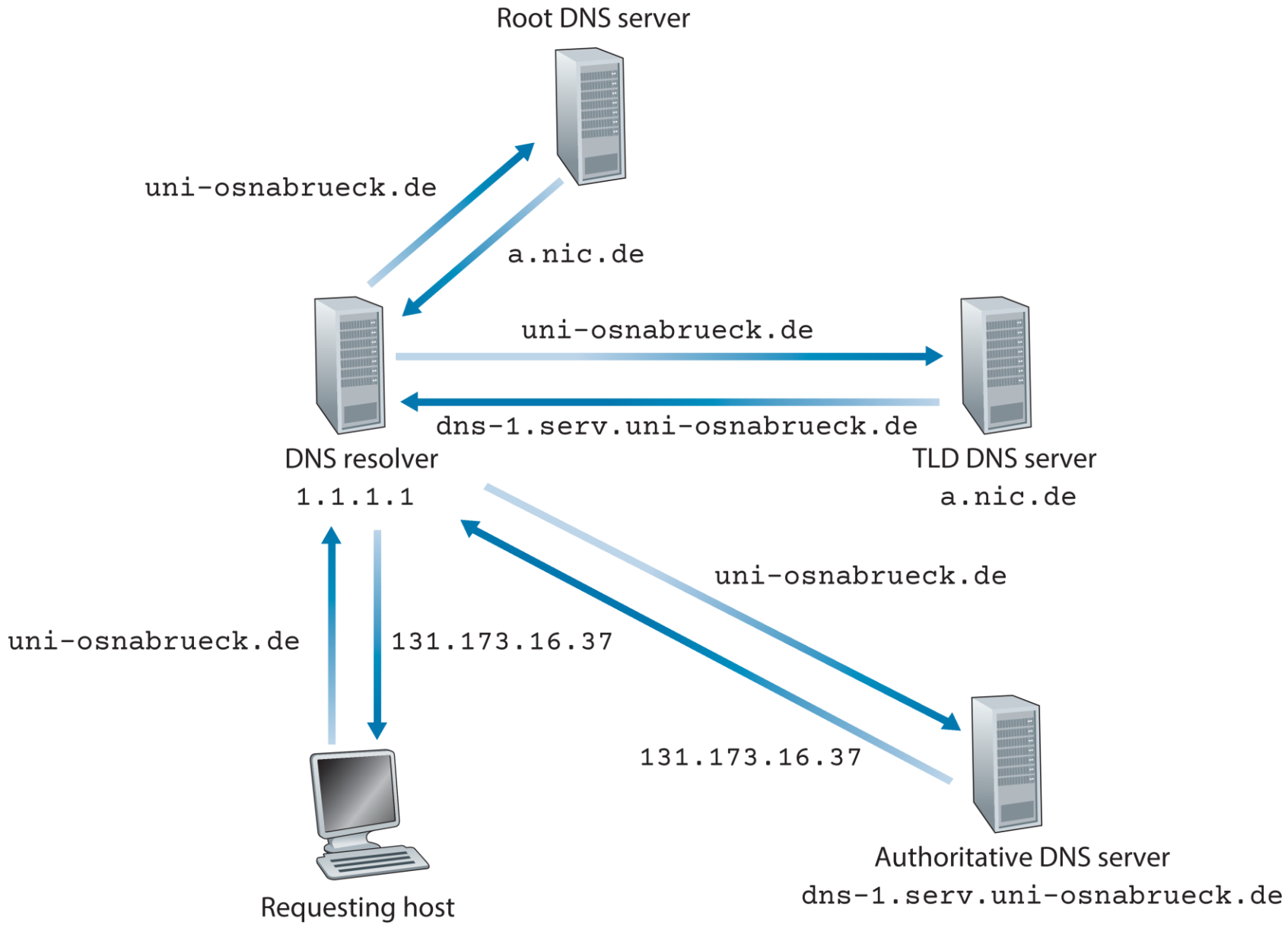
Grundlagen

Domain Name System

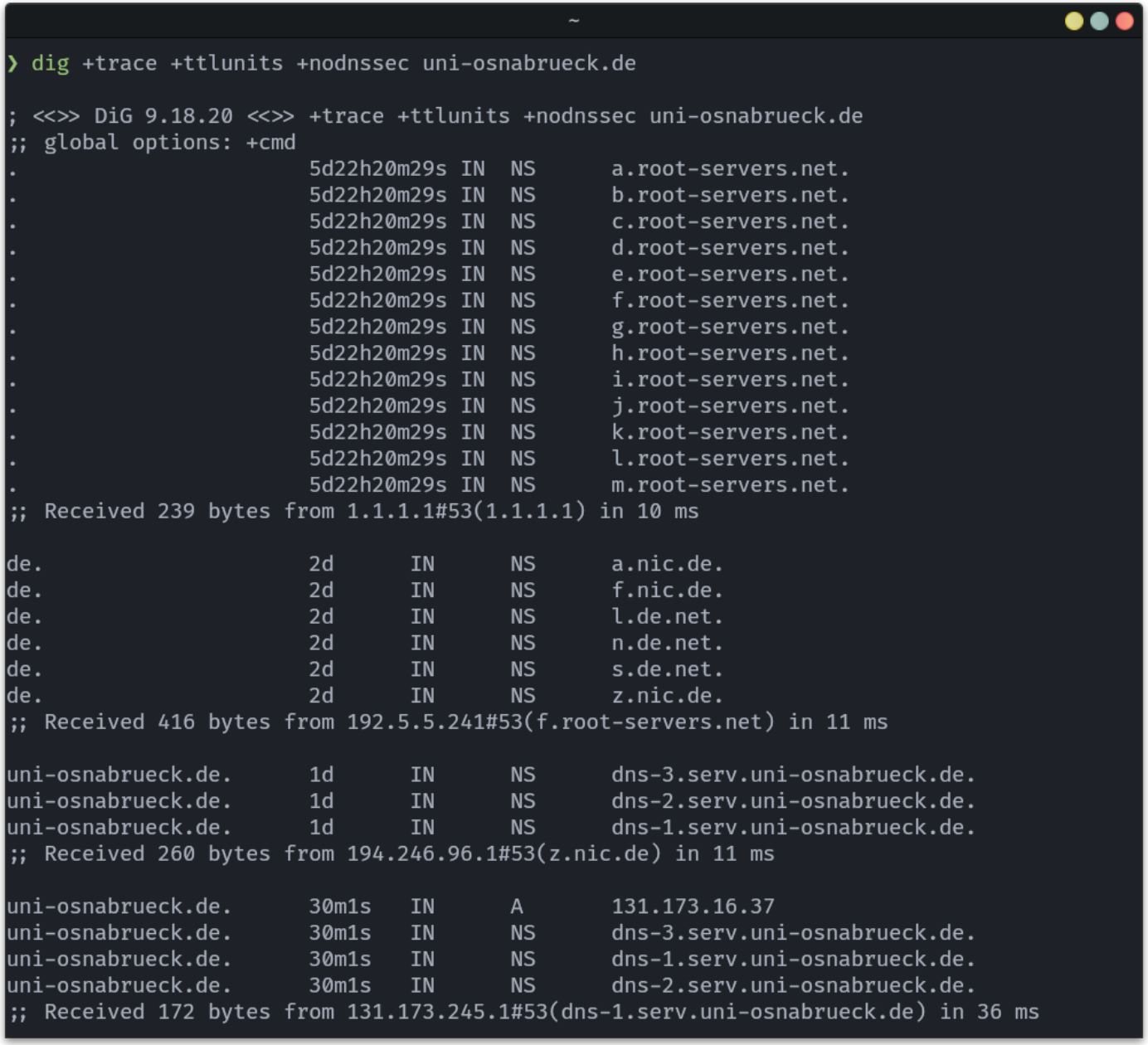
- Übersetzt Domainnamen in numerische IP-Adressen
- Verteilte Datenbank
- Hierarchische Anordnung



Vgl.: James F. Kurose und Keith W. Ross. Computer Networking - A Top-Down Approach. Pearson Addison Wesley, 2020. Seite 127



Vgl.: James F. Kurose und Keith W. Ross. Computer Networking - A Top-Down Approach. Pearson Addison Wesley, 2020. Seite 129


~
❯ dig +trace +ttlunits +nodnssec uni-osnabrueck.de
; <<>> DiG 9.18.20 <<>> +trace +ttlunits +nodnssec uni-osnabrueck.de
;; global options: +cmd
. 5d22h20m29s IN NS a.root-servers.net.
. 5d22h20m29s IN NS b.root-servers.net.
. 5d22h20m29s IN NS c.root-servers.net.
. 5d22h20m29s IN NS d.root-servers.net.
. 5d22h20m29s IN NS e.root-servers.net.
. 5d22h20m29s IN NS f.root-servers.net.
. 5d22h20m29s IN NS g.root-servers.net.
. 5d22h20m29s IN NS h.root-servers.net.
. 5d22h20m29s IN NS i.root-servers.net.
. 5d22h20m29s IN NS j.root-servers.net.
. 5d22h20m29s IN NS k.root-servers.net.
. 5d22h20m29s IN NS l.root-servers.net.
. 5d22h20m29s IN NS m.root-servers.net.
;; Received 239 bytes from 1.1.1.1#53(1.1.1.1) in 10 ms
de. 2d IN NS a.nic.de.
de. 2d IN NS f.nic.de.
de. 2d IN NS l.de.net.
de. 2d IN NS n.de.net.
de. 2d IN NS s.de.net.
de. 2d IN NS z.nic.de.
;; Received 416 bytes from 192.5.5.241#53(f.root-servers.net) in 11 ms
uni-osnabrueck.de. 1d IN NS dns-3.serv.uni-osnabrueck.de.
uni-osnabrueck.de. 1d IN NS dns-2.serv.uni-osnabrueck.de.
uni-osnabrueck.de. 1d IN NS dns-1.serv.uni-osnabrueck.de.
;; Received 260 bytes from 194.246.96.1#53(z.nic.de) in 11 ms
uni-osnabrueck.de. 30m1s IN A 131.173.16.37
uni-osnabrueck.de. 30m1s IN NS dns-3.serv.uni-osnabrueck.de.
uni-osnabrueck.de. 30m1s IN NS dns-1.serv.uni-osnabrueck.de.
uni-osnabrueck.de. 30m1s IN NS dns-2.serv.uni-osnabrueck.de.
;; Received 172 bytes from 131.173.245.1#53(dns-1.serv.uni-osnabrueck.de) in 36 ms

Anycast

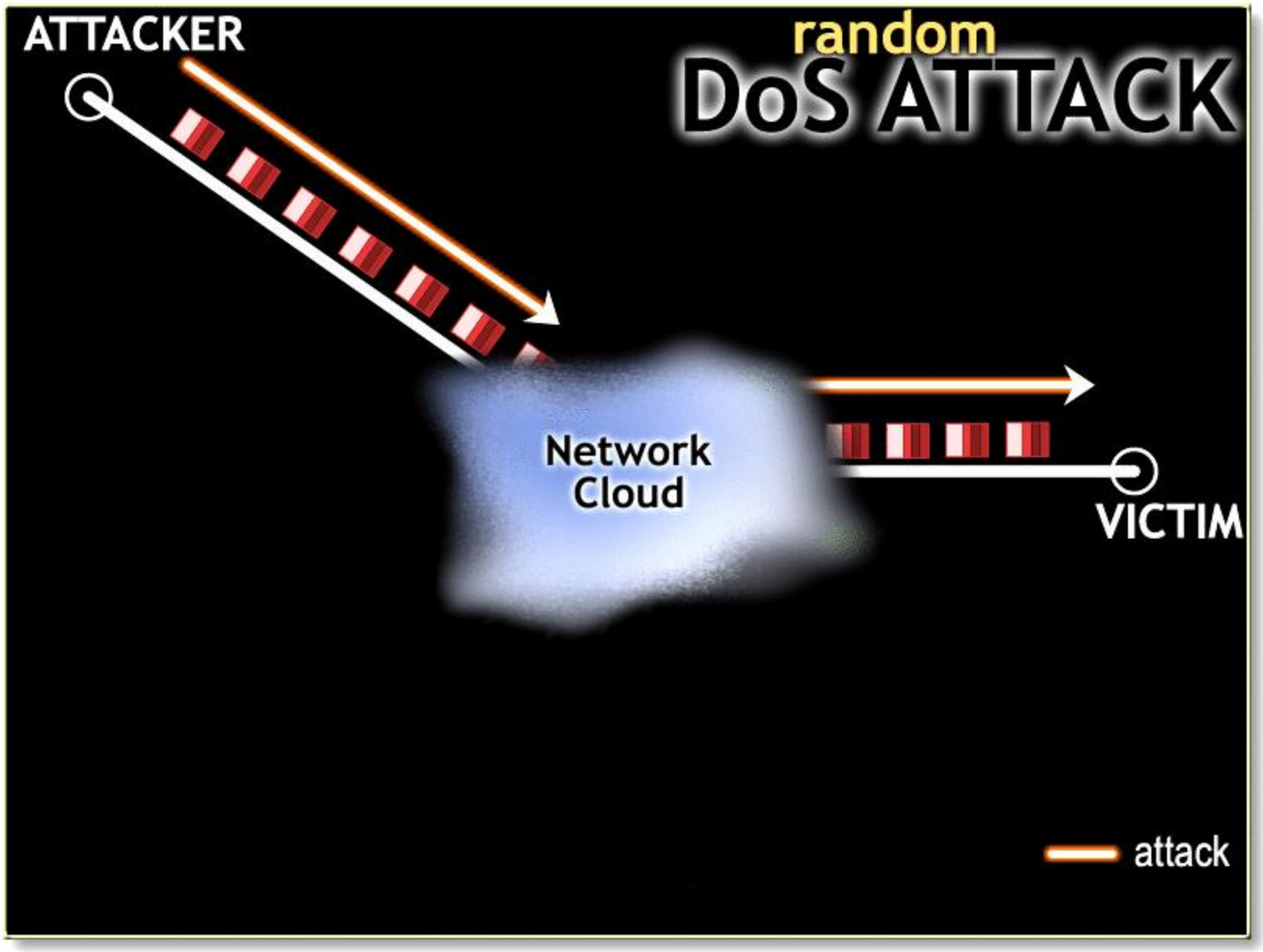
- DNS ist limitiert auf 13 Root-Server
- Gruppe an Hosts teilt gleiche IP-Adresse
  - Pakete werden an den nächsten Host aus der Gruppe geleitet
  - Erlaubt Verteilung der Last auf mehrere Server und Network-Links
- Alle Root-Server verwenden Anycast
- TLD- und andere DNS-Server können ebenfalls Anycast verwenden

Methodik und Datensätze

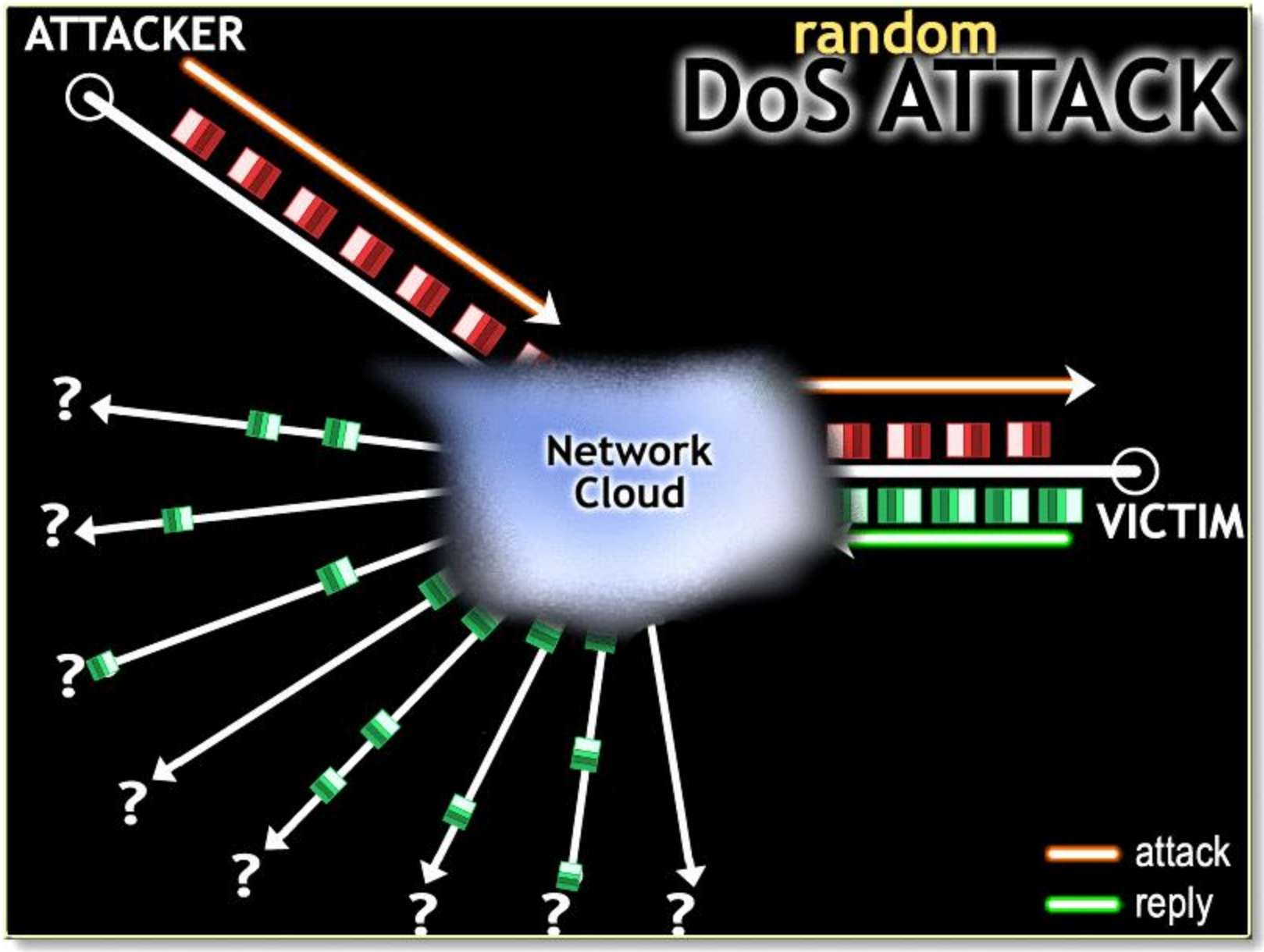
UCSD Network Telescope

- Passives Netzwerk-Monitoring von ungenutztem IP-Adressraum
- Randomly (and Uniformly) Spoofed Denial of Service (RSDoS) Attacks

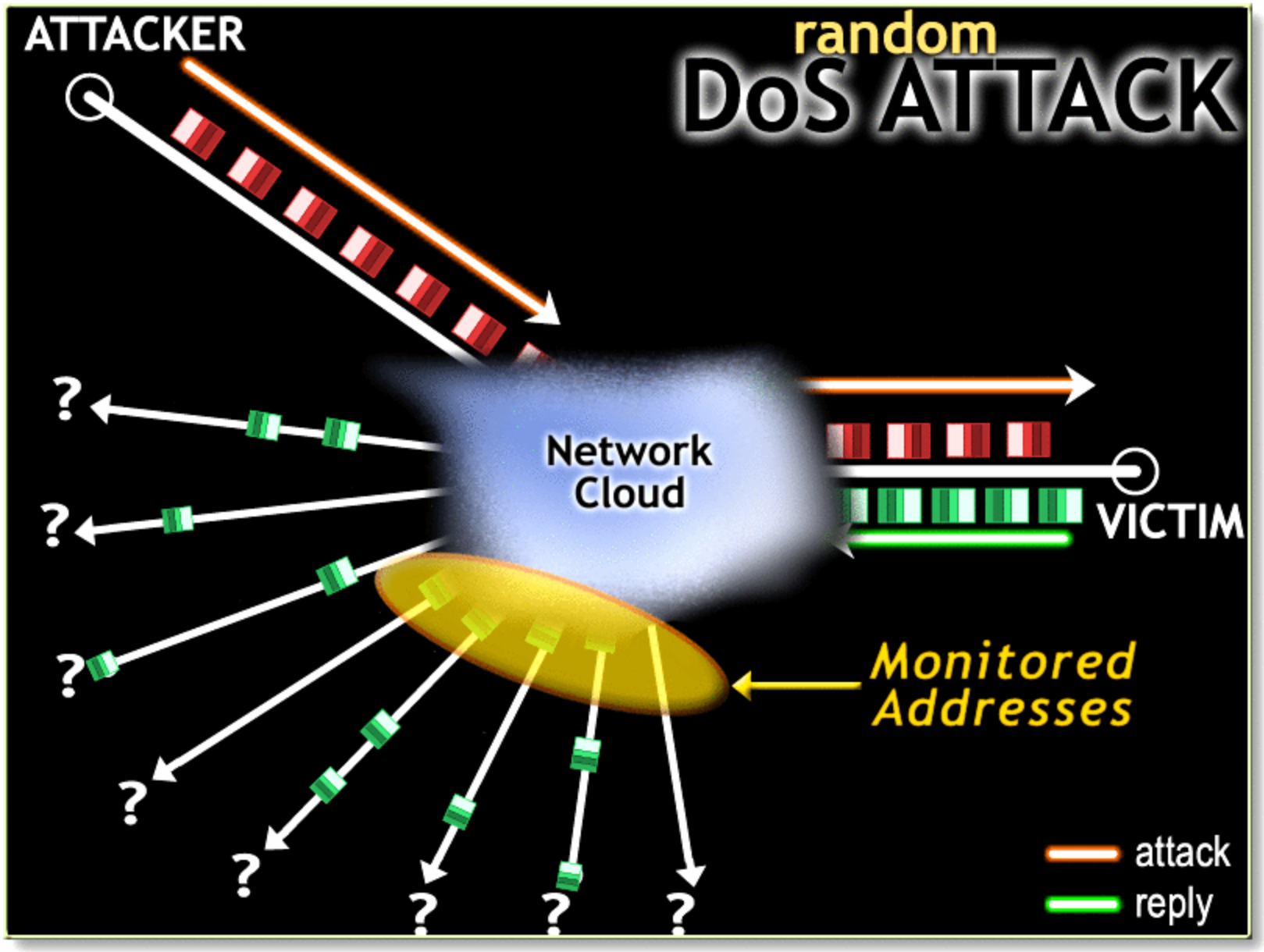
Image: https://www.caida.org/images/caida.png



https://www.caida.org/projects/network_telescope/



https://www.caida.org/projects/network_telescope/

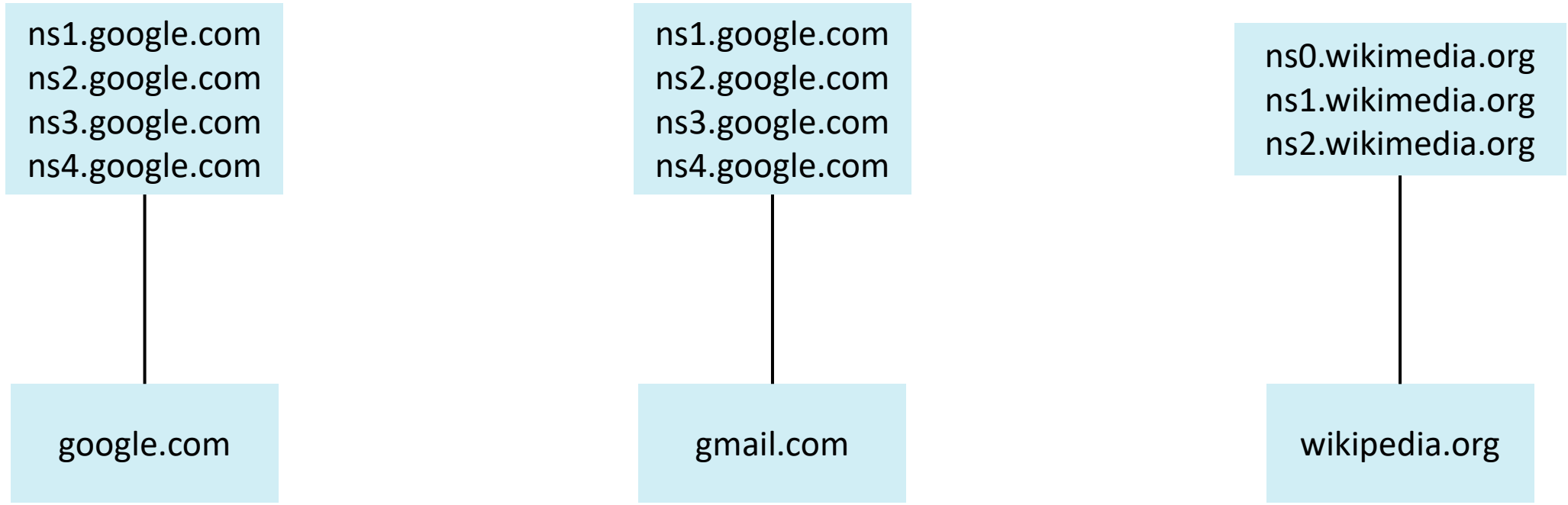


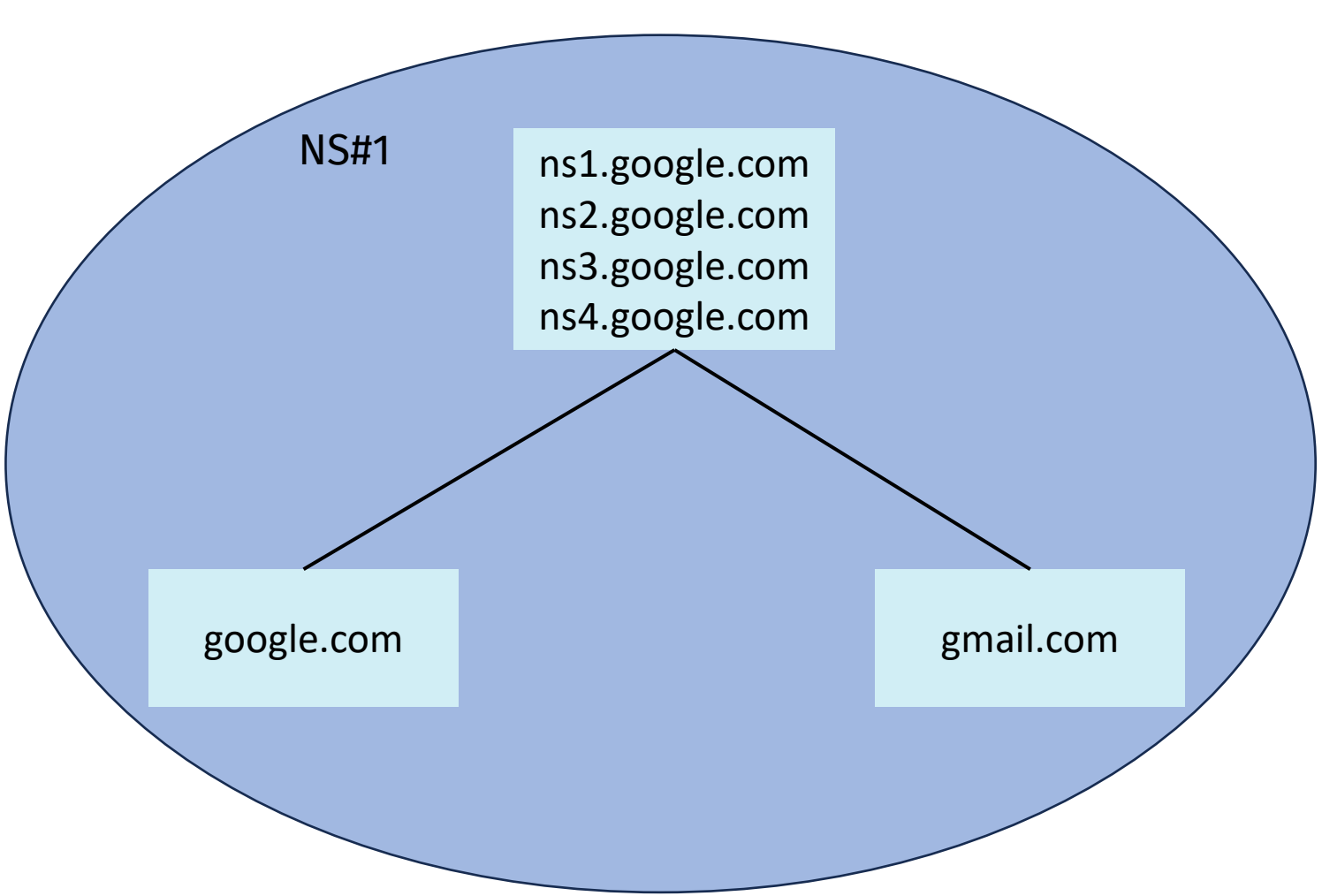
https://www.caida.org/projects/network_telescope/

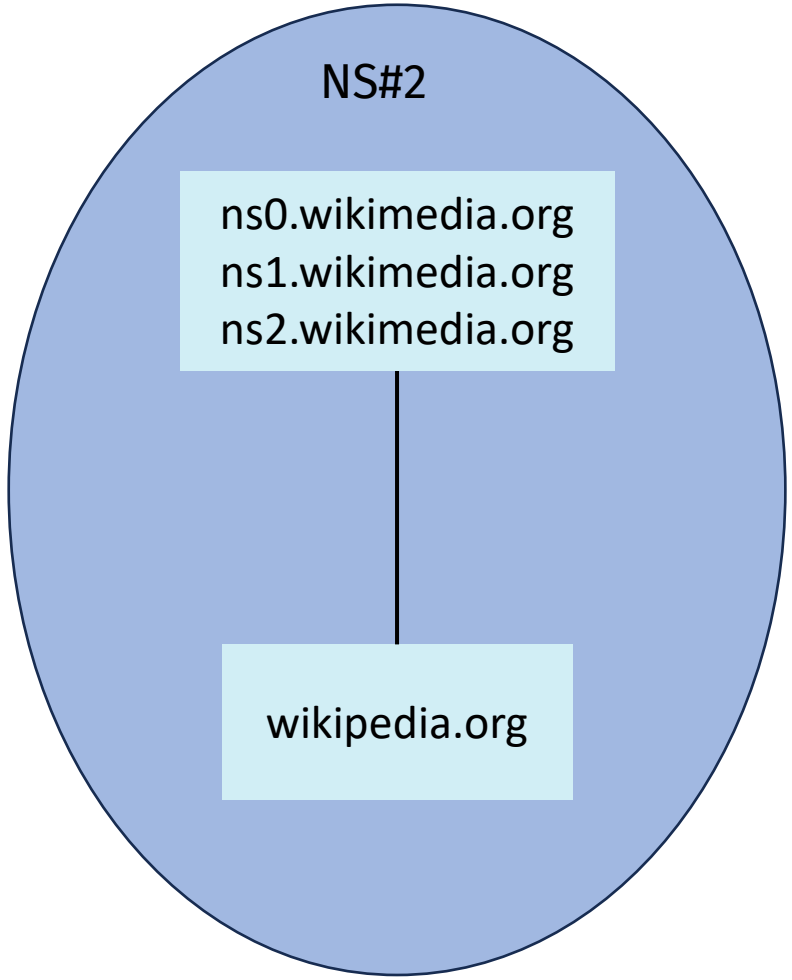
OpenINTEL

- Aktive Messungen zur Erfassung des Zustands großer Teile des globalen Domain Name Systems
- Stellt täglich DNS-Anfragen für ~70% aller Domains
- Misst Round-Trip Time von DNS-Queries

Image: https://www.openintel.nl/static/images/open-intel.svg


ns1.google.com
ns2.google.com
ns3.google.com
ns4.google.com
google.com
ns1.google.com
ns2.google.com
ns3.google.com
ns4.google.com
gmail.com
ns0.wikimedia.org
ns1.wikimedia.org
ns2.wikimedia.org
wikipedia.org

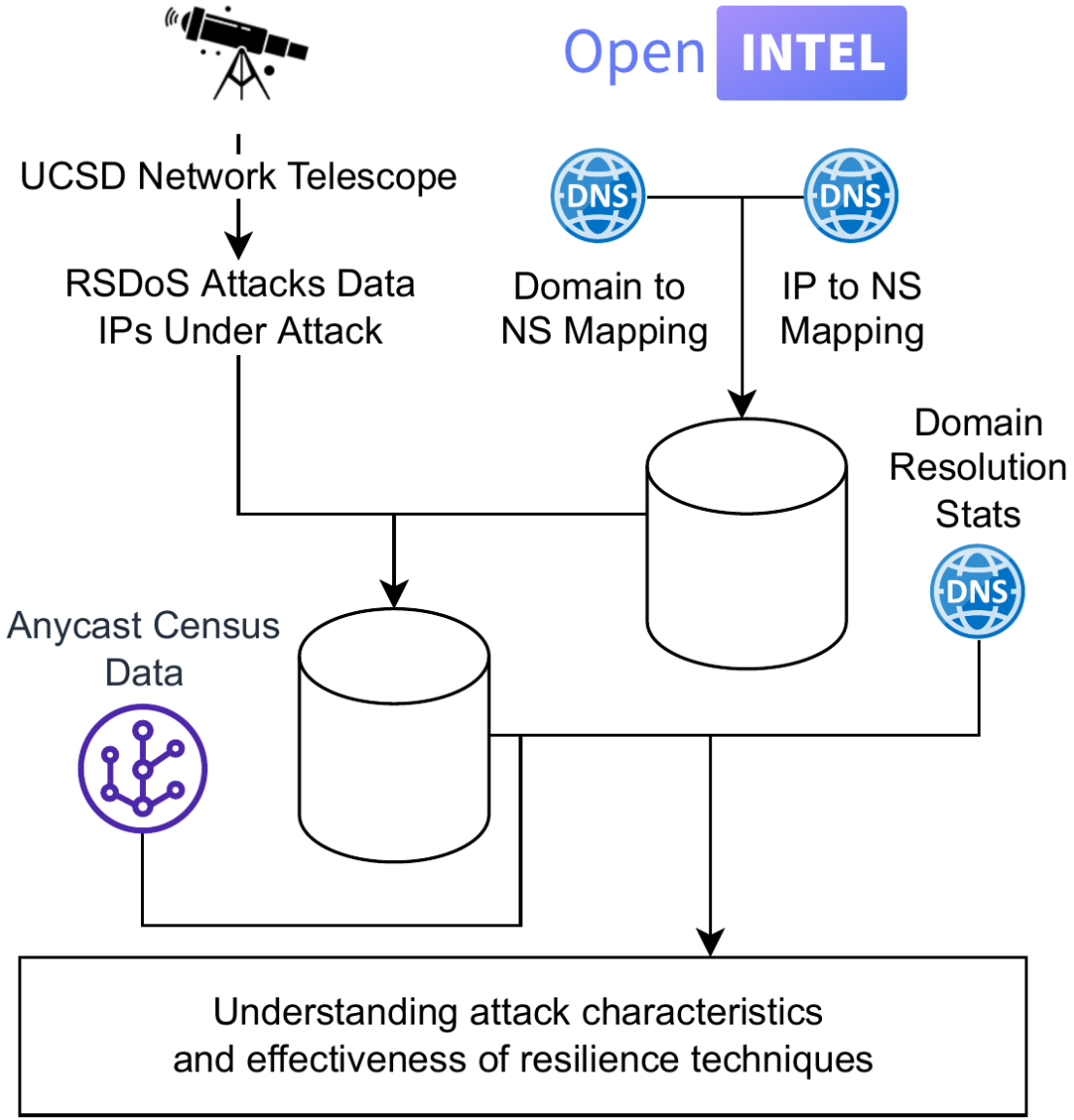

NS#1
ns1.google.com
ns2.google.com
ns3.google.com
ns4.google.com
google.com
gmail.com


NS#2
ns0.wikimedia.org
ns1.wikimedia.org
ns2.wikimedia.org
wikipedia.org

Reaktive Messungen

- Ab Januar 2022 zusätzlich reaktive Messungen
- Wird ein potentieller DoS-Angriff erkannt, so werden die Antwortzeiten aller Nameserver einzeln gemessen

Methodik


Open INTEL
UCSD Network Telescope
RSDoS Attacks Data
IPs Under Attack
DNS
DNS
Domain to
NS Mapping
IP to NS
Mapping
Domain
Resolution
Stats
DNS
Anycast Census
Data
Understanding attack characteristics
and effectiveness of resilience techniques

Exemplarische Angriffe

TransIP

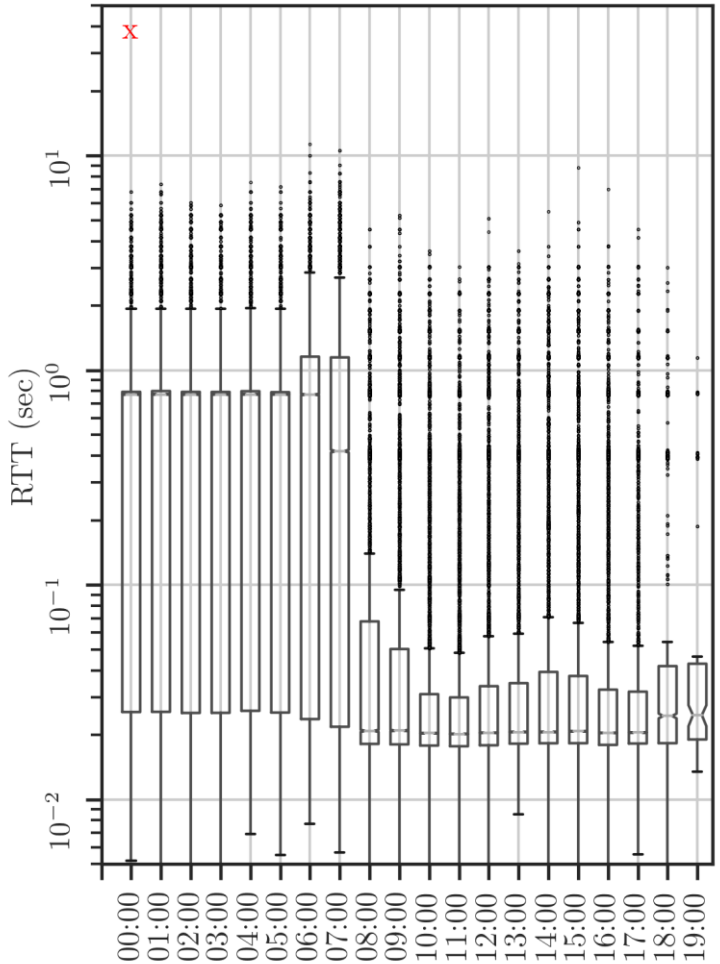
- Angriffe im Dezember 2020 und März 2021
- ~776‘000 Domains
- Drei Unicast Nameserver

Target Nameserver		A	B	C
December 2020 Attack	Observed Packer Rate (PPM)	21.8K	3.8K	2.9K
	Inferred Traffic Volume	1.4 Gbps	247 Mbps	188 Mbps
	Attacker IP Count	5.79M	1.57M	1.33M
March 2021 Attack	Observed Packer Rate (PPM)	125K	123K	13K
	Inferred Traffic Volume	8 Gbps	7.8 Gbps	845 Mbps
	Attacker IP Count	7M	6.19M	823K

TransIP

(Dezember 2020)

- Angriff nur gegen einen Nameserver
- 10x RTT



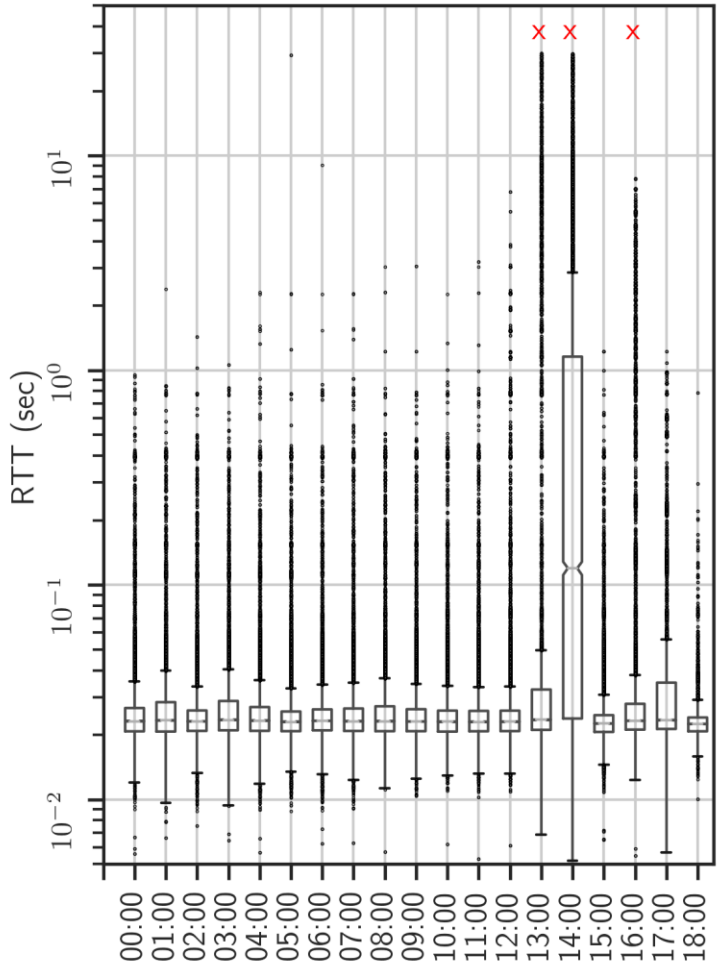
Target Nameserver		A	B	C
December 2020 Attack	Observed Packer Rate (PPM)	21.8K	3.8K	2.9K
	Inferred Traffic Volume	1.4 Gbps	247 Mbps	188 Mbps
	Attacker IP Count	5.79M	1.57M	1.33M
March 2021 Attack	Observed Packer Rate (PPM)	125K	123K	13K
	Inferred Traffic Volume	8 Gbps	7.8 Gbps	845 Mbps
	Attacker IP Count	7M	6.19M	823K

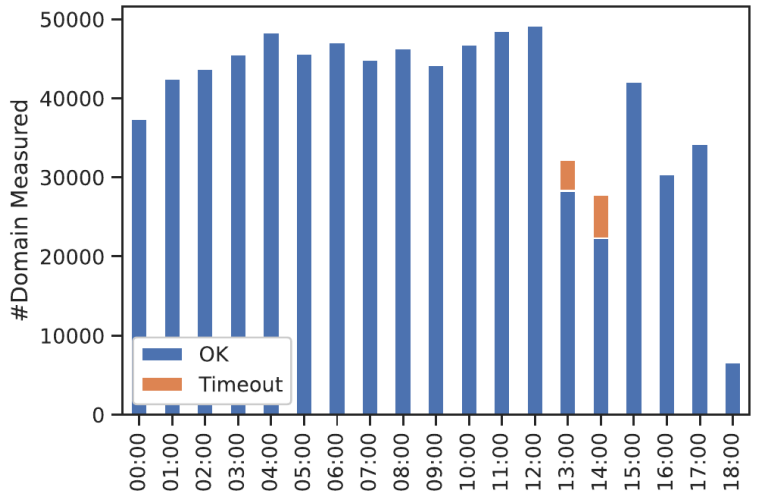
TransIP

(März 2021)

- Angriff gegen alle drei Nameserver
- 6x stärker
- ~20% Timeouts

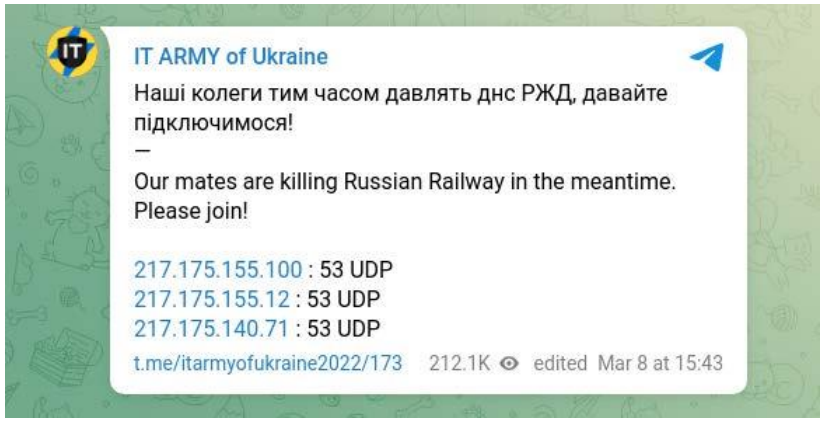
Target Nameserver		A	B	C
December 2020 Attack	Observed Packer Rate (PPM)	21.8K	3.8K	2.9K
	Inferred Traffic Volume	1.4 Gbps	247 Mbps	188 Mbps
	Attacker IP Count	5.79M	1.57M	1.33M
March 2021 Attack	Observed Packer Rate (PPM)	125K	123K	13K
	Inferred Traffic Volume	8 Gbps	7.8 Gbps	845 Mbps
	Attacker IP Count	7M	6.19M	823K





Angriffe gegen russische Server

- Potentiell politisch motiviert
- Angriff gegen `mil.ru`
  - Geringe Intensität
  - Konnte während des Angriffes nicht aufgelöst werden (8 Tage)
  - Drei Unicast Nameserver
  - Gleiches /24 Subnet
- Angriff gegen russische Eisenbahn
  - Erhöhte Antwortzeit und Timeouts
  - Drei Unicast Nameserver
  - Zwei verschiedene /24 Subnets



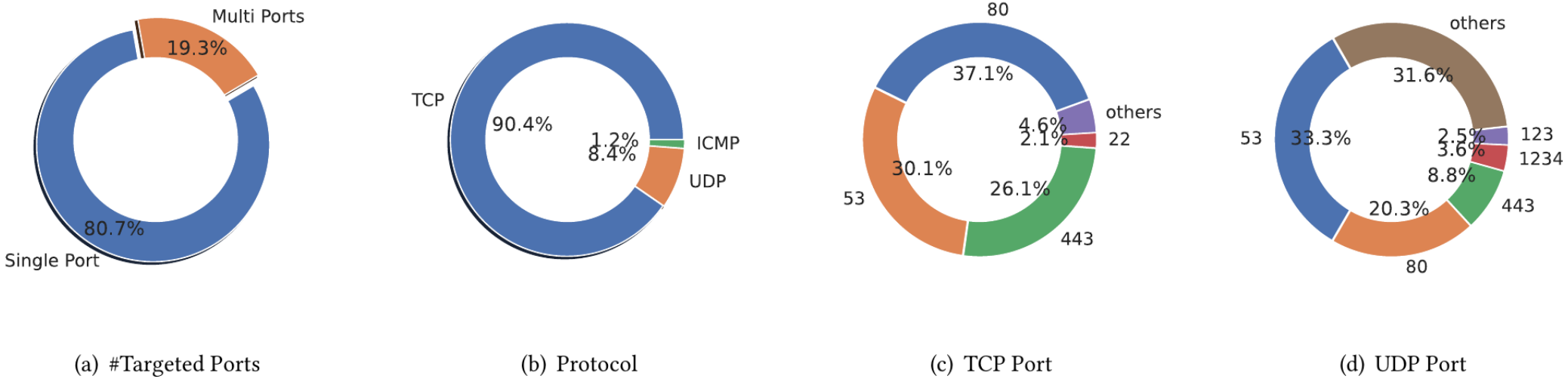
Überblick über Angriffe

Angriffsziele

Year	Month	#DNS Attacks	#Other Attacks	Total Attacks	DNS IPs	Other IPs	Total (Unique) IPs
2020	11	2,550 (1.63%)	156,884 (98.37%)	159,434	798 (1.64%)	47,839 (98.36%)	48,637
	12	3,876 (1.08%)	356,042 (98.92%)	359,918	1,070 (0.94%)	113,354 (99.06%)	114,424
2021	1	2,927 (1.68%)	171,089 (98.32%)	174,016	930 (1.43%)	63,971 (98.57%)	64,901
	2	2,873 (1.98%)	141,949 (98.02%)	144,822	827 (1.52%)	53,461 (98.48%)	54,288
	3	3,294 (1.18%)	276,503 (98.82%)	279,797	929 (0.52%)	177,514 (99.48%)	178,443
	4	3,522 (2.12%)	162,361 (97.88%)	165,883	802 (1.36%)	58,077 (98.64%)	58,879
	5	3,973 (1.99%)	195,540 (98.01%)	199,513	880 (1.19%)	72,899 (98.81%)	73,779
	6	2,244 (0.98%)	227,874 (99.02%)	230,118	821 (0.96%)	84,294 (99.04%)	85,115
	7	2,245 (0.66%)	335,948 (99.34%)	338,193	967 (0.91%)	105,917 (99.09%)	106,884
	8	4,473 (1.53%)	288,369 (98.47%)	292,842	1,055 (1.14%)	91,517 (98.86%)	92,572
	9	2,577 (1.05%)	242,713 (98.95%)	245,290	780 (1.12%)	68,561 (98.88%)	69,341
	10	1,968 (0.86%)	226,124 (99.14%)	228,092	624 (1.25%)	49,310 (98.75%)	49,934
	11	2,662 (0.94%)	281,907 (99.06%)	284,569	835 (1.06%)	77,942 (98.94%)	78,777
	12	2,984 (1.35%)	218,070 (98.65%)	221,054	706 (1.04%)	67,422 (98.96%)	68,128
2022	1	2,028 (0.86%)	232,999 (99.14%)	235,027	705 (1.23%)	56,616 (98.77%)	57,321
	2	1,368 (0.57%)	238,407 (99.43%)	239,775	572 (0.88%)	64,201 (99.12%)	64,773
	3	3,294 (1.37%)	237,848 (98.63%)	241,142	669 (0.94%)	70,778 (99.06%)	71,447
Total		48,858 (1.21%)	3,990,627 (98.79%)	4,039,485	8,864 (0.87%)	1,013,238 (99.13%)	1,022,102

#Attacks	Company
7,324	Google
2,841	Unified Layer
2,428	Cloudflare
2,192	OVH
2,172	Hetzner

Charakteristika



(a) #Targeted Ports (b) Protocol (c) TCP Port (d) UDP Port

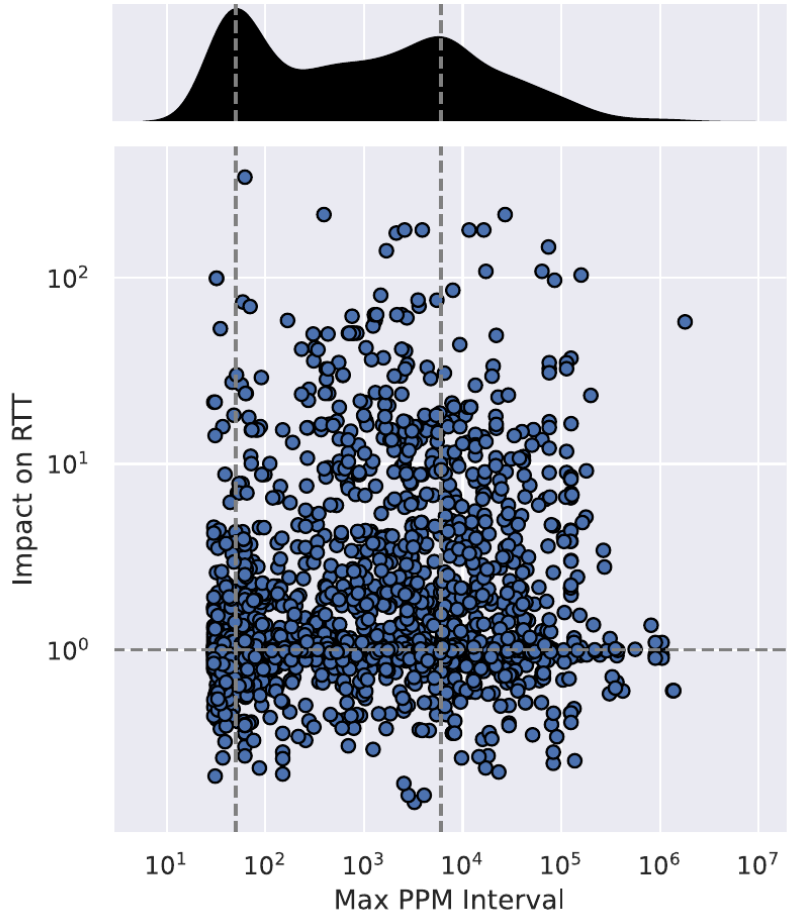
- Großteil der Angriffe nutzen TCP, obwohl DNS eigentlich ein UDP-Protokoll ist
  - SYN-Flooding?
- Die meisten Angriffe laufen nicht auf Port 53 (DNS)
- Angriffe können trotzdem DNS-Infrastruktur überlasten

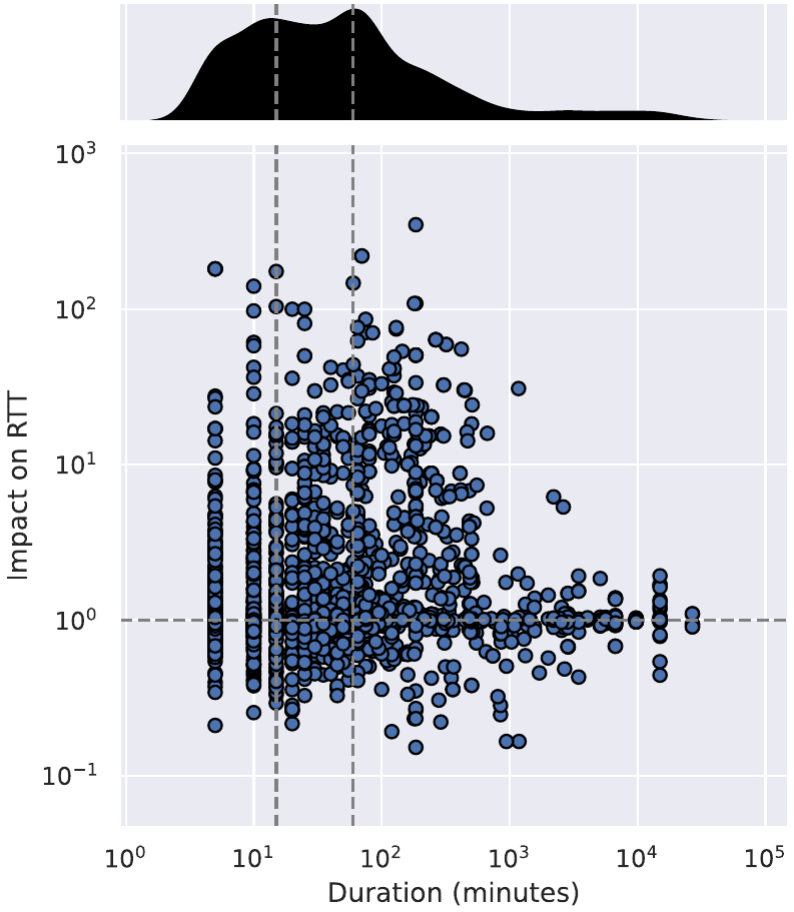
Auswirkungen

- 1% der Angriffe sorgten dafür, dass Domains nicht mehr aufgelöst werden konnten
- Kleinere Nameserver (100 – 10‘000 Domains) sind anfälliger
- 5% der Angriffe sorgten für Antwortzeit-Erhöhung von mehr als 10x
  - 2% sorgten für 100x
- Daten zeigen 2-3x für große Nameserver (10M Domains)
- Auswirkungen in der Praxis vermutlich geringer, da DNS-Resolver Ergebnisse cached

→ Die meisten Angriffe haben nur geringe Auswirkungen, ein erfolgreicher Angriff könnte jedoch potentiell sehr viele Services und Nutzer betreffen

Einfluss von Intensität und Dauer





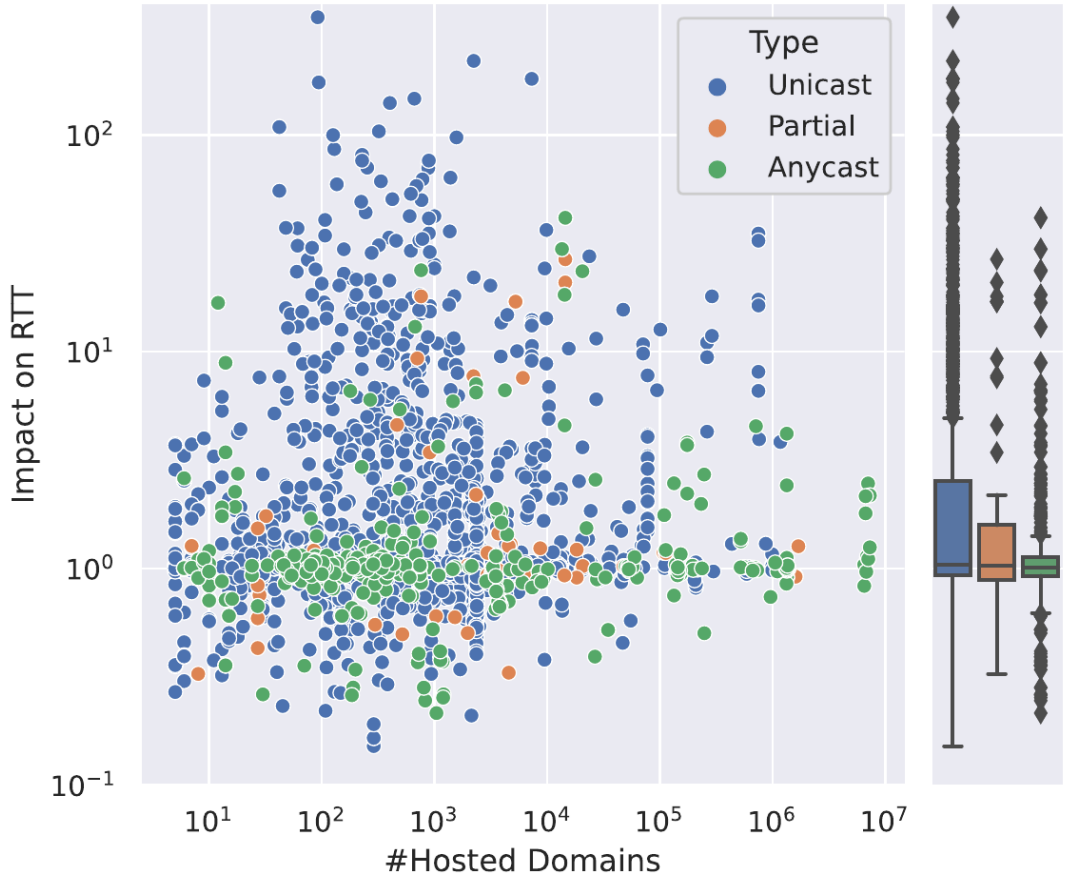
→ Keine aussagekräftige Korrelation zu erkennen

Einfluss von Intensität und Dauer

- Daten genügen nicht, um genaue Analyse des Angriffs aufzustellen
- Drei Annahmen[1]:
  - *Address uniformity:* attackers spoof source addresses at random.
  - *Reliable delivery:* attack traffic is delivered reliable to the victim and backscatter is delivered reliably to the monitor.
  - *Backscatter hypothesis:* unsolicited packets observed by the monitor represent backscatter.
- Backscatter Traffic könnte eingeschränkt sein, wenn Angriffsziel überlastest ist
- UCSD Network Telescope zeigt nur RSDoS und keine weiteren Attack Vectors

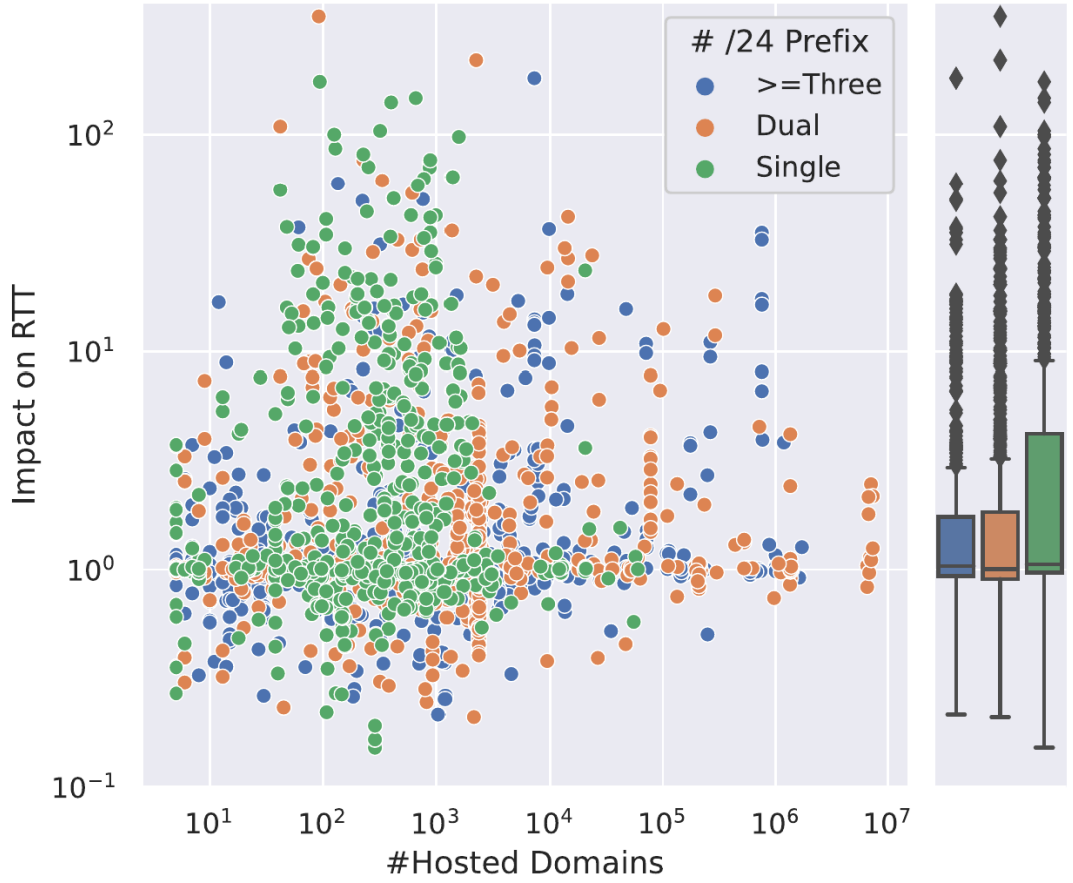
[1]: David Moore et al. “Inferring Internet Denial-of-Service Activity”. In: ACM Trans. Comput. Syst. 24.2 (2006), pp. 115–139. DOI: 10.1145/1132026.1132027

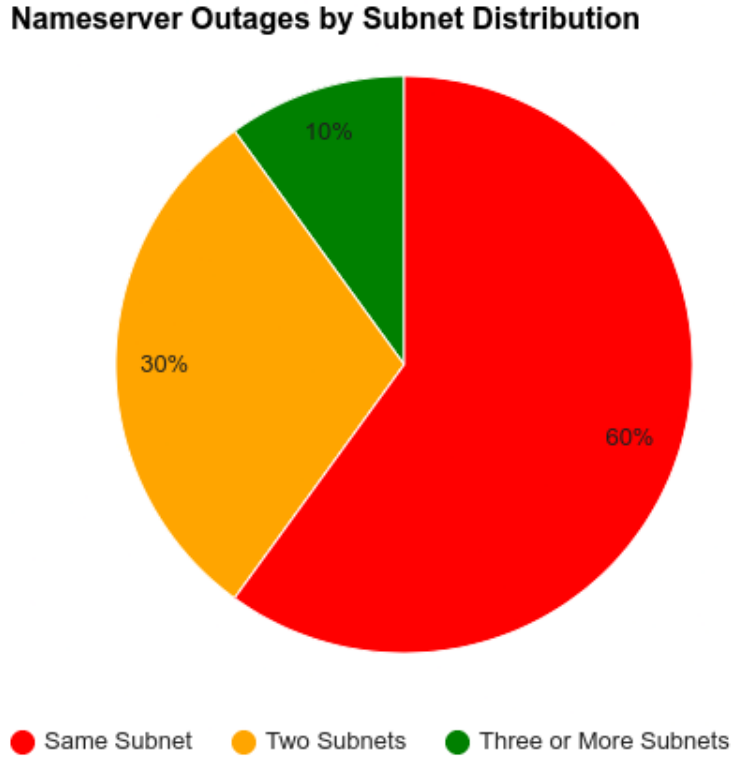
Einfluss von Anycast



- Anycast Konfigurationen halten Angriffen mehr stand als Unicast Server

Einfluss von Subnet-Diversifizierung





→ Subnet-Diversifizierung trägt positiv zur Widerstandsfähigkeit bei

Ethische Erwägungen

Ethische Erwägungen

- UCSD Network Telescope schreibt passiv mit → wenig bedenklich
- OpenINTEL stellt aktiv Anfragen
  - Relativ wenige Anfragen (11 – 12 Anfragen pro Domain pro Tag)
  - Opt-out
- Zusätzliche Messungen stellen aktiv Anfragen
  - Geringe und gleichmäßig verteilte Anzahl an Anfragen
- IP-Adressen in Daten nur veröffentlicht, falls öffentlich bekannt
- Veröffentlichung von Angriffen ggf. kritisch
  - Ebenfalls Gründe die dafür sprechen

→ Allgemein geringe ethische Bedenken

Best Practices

Best Practices

- Anycast
- Subnet-Diversifizierung
- Redundante Nameserver (≥ 3)
- Time-to-Live des DNS-Eintrages entsprechend anpassen
- Allgemeine Sicherheitsmaßnahmen (intrusion detection/prevention, firewalls, traffic filtering)

Zusammenfassung

Zusammenfassung

- Anzahl (erfolgreicher) Angriffe gegen authoritative DNS-Server ist vergleichsweise gering
- Erfolgreiche Angriffe können potentiell großen Schaden anrichten
- Anycast, Subnet-Diversifizierung und weitere Gegenmaßnahmen scheinen erfolgreich das Risiko zu vermindern

References

- Robert Beverly and Arthur Berger. 2015. Server Siblings: Identifying Shared IPv4/IPv6 Infrastructure Via Active Fingerprinting. In Passive and Active Measurement, 149–161.
- Dhruba Kumar Bhattacharyya and Jugal Kumar Kalita. 2016. DDoS attacks: evolution, detection, prevention, reaction, and tolerance. CRC Press.
- Brian Barrett. 2022. Security News This Week: DDoS Attempts Hit Russia as Ukraine Conflict Intensifies. Wired (February 2022). Retrieved November 15, 2023 from https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/
- CAIDA. RSDoS. Retrieved October 20, 2023 from https://www.caida.org/projects/stardust/docs/data/dos/
- CAIDA. The UCSD Network Telescope. Retrieved October 20, 2023 from https://www.caida.org/projects/network_telescope/
- Kimberly Claffy, Alberto Dainotti, Roalnd Jonker Mattijs Van Rijswijk-Deij, Raffaele Sommese, Anna Sperrotto, and Elena Yulaeva. 2022. Mapping DNS DDOS Vulnerability to Improve Protection and Prevention. University of California, San Diego. Retrieved from https://apps.dtic.mil/sti/citations/AD1165550
- Cloudflare. What is Anycast? | How does Anycast work? Retrieved October 17, 2023 from https://www.cloudflare.com/learning/cdn/glossary/anycast-network/
- Cloudflare. Cloudflare DDoS threat report for 2022 Q4. Retrieved October 24, 2023 from https://blog.cloudflare.com/ddos-threat-report-2022-q4/
- Cloudflare. DDoS threat report for 2023 Q1. Retrieved October 24, 2023 from https://blog.cloudflare.com/ddos-threat-report-2023-q1/
- Cloudflare. DDoS threat report for 2023 Q2. Retrieved October 24, 2023 from https://blog.cloudflare.com/ddos-threat-report-2023-q2/
- Domain Name Industry Brief. The Domain Name Industry Brief Quarterly Report - Q2 2023 Data and Analysis. Retrieved October 20, 2023 from https://dnib.com/articles/the-domain-name-industry-brief-q2-2023

References

- Gary Sockrider. 2022. Direct-Path Flooding Attacks Are on the Rise. NetScout (July 2022). Retrieved October 24, 2023 from https://www.netscout.com/blog/direct-path-flooding-attacks-are-rise
- Andy Greenberg. Anonymous Plans To Take Down The Internet? We're Being Trolled. Retrieved October 20, 2023 from https://www.forbes.com/sites/andygreenberg/2012/02/16/anonymous-plans-to-take-down-the-internet-were-being-trolled/
- James F. Kurose and Keith W. Ross. 2020. Computer Networking - A Top-Down Approach. Pearson Addison Wesley.
- Lily Hay Newman. 2016. What We Know About Friday's Massive East Coast Internet Outage. Wired (October 2016). Retrieved November 15, 2023 from https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/
- Jiarun Mao, Michael Rabinovich, and Kyle Schomp. 2022. Assessing Support for DNS-over-TCP in the Wild. In Passive and Active Measurement: 23rd International Conference, PAM 2022, Virtual Event, March 28–30, 2022, Proceedings, Springer-Verlag, 487–517. DOI:https://doi.org/10.1007/978-3-030-98785-5_22
- Mark Andrews. Reason for Limited number of Root DNS Servers. Retrieved October 20, 2023 from https://lists.isc.org/pipermail/bind-users/2011-November/085653.html
- Paul Mockapetris. 1987. Domain names - implementation and specification. IETF.
- David Moore, Colleen Shannon, Douglas J. Brown, Geoffrey M. Voelker, and Stefan Savage. 2006. Inferring Internet Denial-of-Service Activity. ACM Trans. Comput. Syst. 24, 2 (2006), 115–139. DOI:https://doi.org/10.1145/1132026.1132027
- David Moore, Colleen Shannon, Douglas J. Brown, Geoffrey M. Voelker, and Stefan Savage. 2006. Inferring Internet Denial-of-Service Activity. ACM Trans. Comput. Syst. 24, 2 (2006), 115–139. DOI:https://doi.org/10.1145/1132026.1132027
- Giovane C. M. Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker. 2019. Cache Me If You Can: Effects of DNS Time-to-Live. In Proceedings of the Internet Measurement Conference (IMC '19), Association for Computing Machinery, 101–115. DOI:https://doi.org/10.1145/3355369.3355568
- OpenINTEL. OpenINTEL: Active DNS Measurement Project. Retrieved October 20, 2023 from https://www.openintel.nl/

References

- Michael A. Patton, Scott O. Bradner, Robert Elz, and Randy Bush. 1997. Selection and Operation of Secondary DNS Servers. IETF.
- Root Server Technical Operations Association. Events of 2015-11-30. Retrieved October 20, 2023 from https://root-servers.org/media/news/events-of-20151130.txt
- Root Server Technical Operations Association. Retrieved October 19, 2023 from https://root-servers.org/
- Scott Hilton. 2016. Dyn Analysis Summary Of Friday October 21 Attack. Dyn (October 2016). Retrieved November 15, 2023 from https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
- Raffaele Sommese. 2023. Everything in Its Right Place: Improving DNS resilience. phdthesis. DOI:https://doi.org/10.3990/1.9789036556699
- Raffaele Sommese, Gautam Akiwate, Mattijs Jonker, Giovane Moura, Marco Davids, Roland Martijn van Rijswijk - Deij, Geoffrey M. Voelker, Stefan Savage, Kimberley Claffy, and Anna Sperotto. 2021. Characterization of Anycast Adoption in the DNS Authoritative Infrastructure. In TMA Conference 2021, IFIP.
- Raffaele Sommese, KC Claffy, Roland van Rijswijk-Deij, Arnab Chattopadhyay, Alberto Dainotti, Anna Sperotto, and Mattijs Jonker. 2022. Investigating the Impact of DDoS Attacks on DNS Infrastructure. In Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22), Association for Computing Machinery, 51–64. DOI:https://doi.org/10.1145/3517745.3561458
- William Stallings. 2022. Cryptography and Network Security: Principles and Practice, Global Ed. Pearson.
- Tijs Hofmans. 2020. Providers zijn maandag opnieuw getroffen door ddos-aanvallen. Tweakers (December 2020). Retrieved November 15, 2023 from https://tweakers.net/nieuws/175228/providers-zijn-maandag-opnieuw-getroffen-door-ddos-aanvallen.html
- TransIP. DDoS attack on March 22nd. Retrieved November 15, 2023 from https://transip.nl/img/cms/postmortem/ddos_post_mortem_english_march_22.pdf
- Paul A. Vixie. 1999. Extension Mechanisms for DNS (EDNS0). RFC Editor. DOI:https://doi.org/10.17487/RFC2671