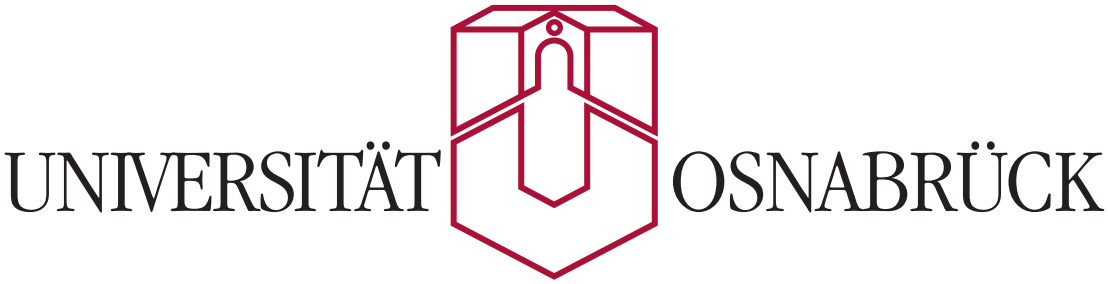

Institut für Informatik
Arbeitsgruppe Verteilte Systeme

Internet Measurements

Impact of DoS attacks on authoritative DNS servers

Wintersemester 2023/24

November 2023

Contents

1 Introduction

The Domain Name System (DNS) is a fundamental component of the Internet, translating domain names into numerical IP addresses, enabling users to access websites and a vast array of online resources. Its role is indispensable to the modern Internet, and a successful Denial of Service (DoS) attack targeting DNS nameservers can have a catastrophic impact on global connectivity. Without DNS, navigating the web, sending emails, or utilizing numerous online services would become impossible.
DoS attacks pose a significant threat to the DNS infrastructure [Sco16] [Lil16]. These attacks involve overwhelming DNS servers with a flood of traffic, rendering them unavailable to legitimate users. DNS DoS attacks are particularly effective due to the high volume of traffic typically handled by DNS servers.
The successful execution of a DNS DoS attack can have far-reaching consequences for the Internet. It can trigger widespread outages of websites, applications, and other online services. Moreover, DNS DoS attacks can be employed to target specific organizations or industries, causing targeted disruptions.
The threat of DNS DoS attacks underscores the critical need for DNS reliability.
This paper will discuss a study that analyzed the impact of DNS DoS attacks on authoritative nameservers. First, the fundamentals of DNS servers are laid out. Subsequently, the methodology employed and specific examples of DNS DoS attacks are presented, followed by a broader analysis of DNS DoS attacks. Finally, the paper explores the implications for DNS and domain operators, along with potential countermeasures.

2 Theoretical Background

To comprehend the impact of DoS attacks on the DNS infrastructure and its implications for evaluating mitigation techniques, a thorough understanding of DNS infrastructure management is essential.

2.1 Domain Name System

The Domain Name System (DNS) operates as a distributed database system, mapping domain names to their corresponding IP addresses. Each DNS nameserver maintains a repository of DNS records associated with a particular domain name, and upon receiving queries for that domain name, it utilizes these records to provide responses.
The DNS namespace is organized into a hierarchical structure resembling an inverted tree, comprising various levels of servers. These servers can be categorized into three primary groups: root DNS servers, Top-Level Domain (TLD) DNS servers, and authoritative DNS servers. There are thirteen logical root DNS servers, which are distributed around the world and managed by the Internet Assigned Numbers Authority (IANA).
When resolving a domain name, the DNS resolver initiates the process by querying a root DNS server for the requested domain name. Since root DNS servers typically lack

direct entries for specific domain names, they provide the record of a TLD DNS server, responsible for the TLD associated with the requested domain name. For instance, upon querying `uni-osnabrueck.de`, the root DNS server would direct the resolver to the TLD DNS server for the `.de` domain (e.g., `a.nic.de`), managed by DENIC.
The DNS resolver then queries the TLD DNS server for the requested domain name. This TLD DNS server, in turn, provides the record of an authoritative DNS server specifically responsible for the requested domain name. For the query `uni-osnabrueck.de`, the TLD DNS server would provide the entry for the authoritative DNS server for the domain (e.g., `dns-1.serv.uni-osnabrueck.de`). The DNS resolver subsequently queries this authoritative DNS server, which delivers the IP address corresponding to the domain name.
During the domain resolution process, an end user's client typically does not interact with all DNS servers in the hierarchy. Instead, it communicates with a DNS resolver, which subsequently queries the DNS servers in the hierarchy and relays the results back to the client.
To minimize the number of queries directed to DNS servers, most DNS resolvers employ a caching mechanism, temporarily storing DNS records for a specified duration [KR20, pp. 126–127].

2.2 Anycast

The original DNS protocol was designed to utilize the User Datagram Protocol (UDP) with a maximum packet length of 512 bytes [Moc87]. This limitation constrained the number of root DNS servers to thirteen, as a larger number would have exceeded the packet size limit [Mar]. With only thirteen root DNS servers, each operating under unique network conditions and server resource constraints, the system would be incapable of handling the sheer volume of DNS queries directed to them.
To address this challenge, all root DNS servers employ *anycast* [Roo], a network addressing and routing technique that enables a group of hosts to share the same IP address. Incoming packets are routed to the host within the group closest to the sender, typically in terms of network hops, and with the capacity to handle the request. This approach distributes the load, ensuring that even if one server becomes overwhelmed, requests can still be processed by other available hosts.
Moreover, an anycast network is not restricted to a single network link, allowing the distribution of hosts across different geographical locations and data centers. This technology is utilized not only by root DNS servers but also by TLD DNS servers and authoritative DNS servers to distribute the load across multiple servers, ensuring a more reliable and responsive DNS service [Som+21] [KR20, pp. 406–407].

3 Methodology and Datasets

To identify and analyze DoS attacks against authoritative DNS servers, an analysis was conducted on a combined dataset from the UCSD Network Telescope and OpenINTEL

measurement project. This analysis spanned a 17-month period, encompassing data from November 1, 2020, to March 31, 2022.

3.1 UCSD Network Telescope - Passive Network Monitoring

A Randomly (and Uniformly) Spoofed Denial of Service (RSDoS) attack utilizes randomly spoofed source IP addresses to obscure the attack's origin and hinder the victim's ability to filter out malicious traffic. Unable to distinguish between legitimate and spoofed traffic, the victim attempts to respond to all incoming requests. These outgoing packets, generated in response to spoofed requests, are known as *backscatter* traffic [CAIa].
The UCSD Network Telescope, a network comprising a large number of unused IP addresses (roughly 1/256th of all IPv4 addresses), passively collects traffic directed to these spaces. Since these IP addresses are unassigned, any traffic received is considered suspicious, enabling the capture of backscatter traffic. By analyzing this backscatter data, DoS attacks can be identified and insights into their scale, target, and methodology can be obtained [CAIb] [Moo+06a].

3.2 OpenINTEL - Active DNS Measurements

The OpenINTEL measurement project conducts daily DNS queries on approximately 70% of all registered domain names worldwide (as of Oct. 2023) [Ope] [Dom]. These measurements encompass resolution time, enabling the detection of anomalies in DNS latency and reachability. Since OpenINTEL does not provide information about the authoritative DNS server that answered the query, the IP addresses of nameservers associated with each domain are aggregated into a set.
Over a 5-minute interval, the number of domains resolved by OpenINTEL, the average, minimum, and maximum Round-Trip Time (RTT), and the number of errors are collected for each set by aggregating data across all domains within the same set. Identifying an impact on the nameservers is achieved by comparing the average RTT of the set to the average RTT of the same set on the previous day. This approach allows for a meaningful comparison within the same set and allows for swift adaptation if the DNS infrastructure, and consequently, the latency, undergoes changes [Som+22].

3.3 Methodology

The UCSD Network Telescope data can be leveraged to identify potential RSDoS attacks against IP addresses. By cross-referencing the IP addresses of nameservers with elevated RTT detected by OpenINTEL and the IP addresses identified by the UCSD Network Telescope data, potential RSDoS attacks targeting authoritative DNS servers can be pinpointed.
Utilizing the aggregated data from the OpenINTEL dataset enables the extraction of domain names served by the nameservers identified as potential targets. Measuring the RTT of these domains allows for an analysis of the impact of these attacks [Som+22].

3.4 Limitations

Gathering and identifying Denial of Service (DoS) attacks is a complex undertaking. While combining data from the UCSD Network Telescope and OpenINTEL facilitates the detection of potential DoS attacks, it falls short of providing a comprehensive analysis.
Specifically, the UCSD Network Telescope data only permits the identification of RSDoS attacks against IP addresses and is restricted to IPv4, excluding IPv6 addresses. Translating identified RSDoS attacks against IPv4 addresses to their IPv6 counterparts may be feasible, as IPv4 and IPv6 services often share network and server infrastructure [BB15].
One limitation of OpenINTEL's random nameserver selection approach is its inability to identify attacks targeting specific nameservers. However, this approach provides a measurement of the overall end-user experience of resolving a domain name, as a typical end user does not select a specific nameserver. Additionally, due to the inherent nature of the anycast infrastructure, it is possible that ongoing attacks in specific geographic regions may not be detected using the OpenINTEL dataset.
To address these limitations, an additional reactive measurement was implemented in conjunction with the dataset combination for attacks occurring after January 2022. Upon detecting a potential DoS attack, all nameservers belonging to a potentially attacked domain are queried iteratively. For each attack, 50 related domain names are queried evenly spread every 5 minutes during the attack and the following 24 hours. While this approach also has limitations, originating from a single network in the Netherlands, it does provide a more detailed analysis of the attack's impact [Som+22].

4 Exemplary Attacks and their Implications

The analyzed data reveals the impact of multiple attacks against different nameservers. The following section will delve into publicly acknowledged or reported attacks and their repercussions.

4.1 Attacks against TransIP's Nameservers

TransIP, a European domain and web hosting company, experienced two attacks that impaired the DNS resolution performance of its nameservers: one in December 2020 and the other in March 2021. Both attacks were acknowledged by TransIP [Tij20] [Tra]. TransIP utilized three nameservers hosted in a unicast deployment.
The December 2020 attack appears to have primarily targeted only one of the three nameservers, yet OpenINTEL recorded a 10-fold increase in resolution time due to the randomized querying of nameservers.
The March 2021 attack was more severe and targeted all three nameservers. While the nameservers' resolution time was also negatively impacted, the attack also caused approximately one-fifth of queries to time out, amplifying the attack's noticeable impact [Som+22].

4.2 Attacks against Russian Nameservers

The TransIP example illustrates an attack targeting a commercial entity, while attacks against Russian assets are suggested to be politically motivated. In March 2022, an attack targeted `mil.ru`, the domain of the Russian Ministry of Defense [Bri22]. The domain was managed by three unicast nameservers on the same `/24` subnet. During the attack, both OpenINTEL and the reactive measurements failed to resolve the domain, and it was reported that the domain was geo-fenced, allowing only requests from within Russia.
In the same month, another attack targeting the nameservers of the state-owned Russian Railway company was observed. The three nameservers were hosted on two different `/24` subnets and used unicast. All three servers were targeted by the attack, and degradations in resolution time and timeouts were measured [Som+22].

4.3 Implications

In an attempt to filter out malicious traffic, TransIP implemented a traffic scrubbing technique. However, despite this measure, the attacks still had a significant impact on their servers and a substantial portion of their customers. Their servers were deployed in a unicast configuration across three different subnets in two distinct geographical locations. This deployment renders the infrastructure heavily reliant on these three physical servers and their corresponding network links.
Similarly, the `mil.ru` nameservers were hosted on the same subnet, implying that they shared the same network link. In such configurations, targeting the network links of the servers can be sufficient to execute a successful DoS attack.
The Russian Railway nameservers were hosted on two different subnets, but all three nameservers employed unicast and were individually targeted by the attack. In a unicast configuration, overwhelming the physical server can lead to a successful attack.
A more diverse infrastructure with more physical servers using anycast and distributed across different networks would allow for the distribution of the load and reduce the point of failure [Som+22].

5 Scope of Attacks against Authoritative DNS Servers

The preceding examples highlight the impact of specific attacks targeting authoritative DNS servers. However, the goal of the study is to infer a more general overview of the scope of these attacks. The following section delves into the insights that can be extracted from the data and the implications of these findings.

5.1 Attack Targets

The UCSD Network Telescope data indicates that approximately 0.5% to 2% of all potential attacks are directed at the DNS infrastructure. While the absolute number of attacks is relatively low, a successful attack on a nameserver could have a significant impact on

millions of domains and their users. On average, each attack potentially affects a small number of domains. However, the measurements show eight peaks that impacted 10 million domains, or approximately 4% of the domains covered by OpenINTEL. These attacks had negligible impacts on resolution time. Most attacks target large hosting companies such as Google, Unified Layer, and Cloudflare, with very little impact on the overall infrastructure [Som+22].

5.2 Attack Characteristics

The analysis of DoS attack characteristics shows that a significant majority (80.7%) of attacks targeted a single port and protocol. The most common protocol used is TCP (90.4%), followed by UDP (8.4%) and ICMP (1.2%).
While DNS originated as a UDP-based protocol, the use of TCP has increased over the years, and many authoritative nameservers have adopted TCP as a protocol [MRS22].
The most common ports targeted by TCP attacks were port 80 (HTTP), port 53 (DNS), and port 443 (HTTPS), accounting for 37.1%, 30.1%, and 26.1% of attacks, respectively. UDP attacks targeted a more diverse set of ports, with one-third of attacks targeting port 53 (DNS).
The persistent popularity of TCP SYN flooding attacks [Cloa] [Gar22], even when overtaken by other attack vectors [Clob] [Cloc], may be the reason for the high number of TCP-based attacks. TCP SYN flooding attacks work by sending a large number of SYN packets to a target server, exploiting the TCP three-way handshake, and leaving the target with half-open connections that consume resources [Sta22, pp. 688–690].
Notably, the majority of attacks targeting DNS nameservers did not target port 53, the port used by DNS.
Without knowing the attackers' goals and motivations, it is difficult to infer the reasons for this behavior and the chosen attack vectors. However, even attacks not targeting port 53 can still have an impact on the DNS infrastructure, as the network and server resources can still be overwhelmed by the attack traffic [Som+22].

5.3 Attack Impacts

Most identified DoS attacks have no impact on the ability to resolve domain names, with only 1% of attacks resulting in a resolution failure. However, smaller nameservers (10-10,000 domains) are more vulnerable, even if they use an anycast configuration.
Similarly, the majority of attacks have no impact on the resolution time. In approximately only 5% of cases, the resolution time increases by more than 10-fold, and in fewer than 2% of cases, the resolution time increases by more than 100-fold. These attacks also primarily target smaller nameservers. Attacks targeting larger nameservers are less effective, but can still lead to a 2- to 3-fold increase in resolution time [Som+22].
Overall, most DoS attacks on DNS authoritative servers are ineffective, but some can have a significant impact. The real-world impact of these attacks will vary depending on the end user's DNS resolver. Most DNS resolvers cache query results for a certain amount of

time, so an increase in resolution time or failure of resolution will only be noticeable if the cached result expires during the attack.

5.4 Effect of Intensity and Duration on the Attack Impact

Determining the severity of an attack from the UCSD Network Telescope data is a complex task. As noted in Section 3.4, the data only permits the identification of RSDoS attacks. If an attacker employs alternative attack vectors, the data will only reflect the RSDoS component, making it challenging to assess the true intensity. Furthermore, even when the Telescope indicates a high-intensity attack, determining the impact proves difficult as it hinges on the target's infrastructure. Overall, while the data enables the identification of potential attacks, it does not facilitate a detailed analysis of all attack vectors or a correlation with the impact [Moo+06b].
Most effective attacks were short-lived, ranging from 15 to 60 minutes. Given that the Telescope only detects RSDoS attacks, a successful attack may appear as a short-lived event, even if it persisted for an extended period, as backscatter traffic may be hindered if the victim cannot respond to the incoming traffic.
In summary, the UCSD Network Telescope data is valuable for identifying potential attacks, but it falls short of providing a comprehensive assessment of their impact [Som+22].

5.5 Effect of Anycast Deployment and Network Diversification on the Attack Impact

Consistent with the findings in Section 4, the broader data indicates that anycast deployments exhibit greater resilience, experiencing only a 1- to 1.5-fold increase in RTT while under attack. Partial anycast deployments, where only a portion of nameservers employ anycast, demonstrated reduced resilience compared to anycast-only deployments. Unicast-only deployments proved to be the most susceptible to attacks.
Furthermore, the data suggests that dispersing nameservers across multiple subnets enhances resilience. Nameservers residing on the same `/24` subnet likely share the same network link. Sixty percent of the nameserver sets that experienced outages were hosted on the same `/24` subnet. Distributing nameservers across two subnets improves resilience, as only 30% of nameserver sets that experienced outages spanned two `/24` subnets. Spreading nameservers across three subnets further strengthens resilience, with nameserver sets encompassing three or more subnets accounting for only 10% of those that experienced outages [Som+22].

6 Ethical Considerations

The release of information indicating that specific companies have been subjected to attacks raises ethical concerns. Companies often hesitate to disclose attack details due to factors like reputational damage and legal liabilities. However, there are also ethical justifications

for disclosing attack information, such as raising awareness of attack vectors and facilitating the development of countermeasures.
In the context of the data collection methods utilized for this study, the ethical concerns are relatively minor. The UCSD Network Telescope data is gathered through passive network monitoring and does not send any packets to the target systems. OpenINTEL is an active network monitoring project, but its impact is negligible as it only sends a limited number of queries to each target system [Ope]. The reactive measurements conducted also have a minimal impact, as they only involve sending a small and evenly distributed number of queries.
Furthermore, IP addresses were removed from the published data, with only the associated companies being disclosed. Exceptions were made only in instances where the data was already publicly available.
Overall, the ethical concerns stemming from the data collection methods employed in this study are minimal.

7 Best Practices

Anycast deployment plays a crucial role in mitigating the effects of DoS attacks, as discussed in Section 4.3 and Section 5.5. With an adoption rate of 97% for TLD and 62% for SLD DNS servers in 2021 [Som+21], anycast has become a widely used technique for enhancing the availability of DNS services. However, even with an anycast deployment, the risk of DoS attacks is not entirely eliminated. Employing additional unicast servers as a redundancy fallback can further mitigate the impact of DoS attacks, but it also increases the complexity and costs associated with the infrastructure [Som+21].
DNS records contain a Time-to-Live (TTL) value that determines the maximum duration for which the record can be cached by a resolver. DNS caching is a widely used technique that reduces the load on authoritative nameservers and enhances the performance of the DNS resolution process. Moreover, cached records remain accessible in the event of a DoS attack against the authoritative DNS servers, enabling quick resolution of queries even if the authoritative nameservers are affected or unreachable. The appropriate TTL value depends on various factors, and different values have different trade-offs. Longer TTL values, such as 8, 12, or 24 hours, allow for cached responses during authoritative nameserver disruptions, while also permitting changes to propagate through the DNS system in a timely manner [Mou+19] [Som23, pp. 140–141].
Domain operators can improve the resilience of the resolution process by supplying multiple nameservers that store the same records redundantly. The DNS specification mandates the use of at least two nameservers [Moc87]. If one nameserver falls victim to an attack and the other becomes unreachable due to other factors, the domain becomes inaccessible. Therefore, it is recommended to utilize at least three nameservers, dispersed across different geographical locations and networks, to further diversify the infrastructure and mitigate the risk of overloading server resources and network links. Increasing the number of nameservers further improves the infrastructure's resilience but also adds complexity

and cost, raising the likelihood of misconfigured servers and increasing the packet size of DNS responses [Pat+97]. Additional infrastructure diversification can be achieved by providing nameservers from different TLD servers (e.g., `.com` and `.net`). This enables domain resolution even if one of the TLD servers falls victim to an attack [Som23, pp. 133–140].
In addition to DNS infrastructure-specific measures, implementing more general security measures such as intrusion detection and prevention systems, firewalls, and traffic filtering can further enhance the resilience of the DNS infrastructure [BK16, pp. 145–159].

8 Conclusion

This study delves into an analysis of DoS attacks targeting authoritative nameservers, drawing upon data from the UCSD Network Telescope and OpenINTEL datasets alongside additional measurements.
The frequency of DNS attacks is relatively low, with the majority of attacks failing to disrupt DNS resolution for the vast majority of end users. However, certain attacks can have a substantial impact on smaller nameservers and pose real-world threats to service availability.
Anycast configurations exhibit greater resilience to attacks compared to unicast configurations. Diversifying the network infrastructure further by deploying nameservers on multiple subnets can also enhance resilience. Therefore, DNS operators should consider implementing anycast nameservers and dispersing them across multiple subnets.
The combined datasets offer a unique perspective on DNS attacks, providing insights from both passive and active network monitoring. The findings reveal that attackers employ a diverse range of ports and protocols to target authoritative DNS servers, with many attacks targeting ports other than port 53, the standard port for DNS.
Overall, the study's findings highlight that DNS attacks pose a genuine threat. However, by implementing the countermeasures discussed in this paper, DNS operators can effectively mitigate the impact of attacks and strengthen the resilience of their DNS infrastructure.

References

[Sco16] Scott Hilton. "Dyn Analysis Summary Of Friday October 21 Attack". In: *Dyn* (Oct. 26, 2016). Original Source offline; Archive: https://web.archive.org/web/20161101171641if_/https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. URL: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (visited on 2023-11-15).

[Lil16] Lily Hay Newman. "What We Know About Friday's Massive East Coast Internet Outage". In: *Wired* (Oct. 21, 2016). Archive: https://web.archive.org/web/20231115155839if_/https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/. URL: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ (visited on 2023-11-15).

[KR20] James F. Kurose and Keith W. Ross. *Computer Networking - A Top-Down Approach*. Pearson Addison Wesley, 2020. ISBN: 9780136681557.

[Moc87] Paul Mockapetris. *Domain names - implementation and specification*. RFC 1035. Available: https://www.rfc-editor.org/rfc/rfc1035.txt. IETF, 1987.

[Mar] Mark Andrews. *Reason for Limited number of Root DNS Servers*. Archive: https://web.archive.org/web/20231020163243if_/https://lists.isc.org/pipermail/bind-users/2011-November/085653.html. URL: https://lists.isc.org/pipermail/bind-users/2011-November/085653.html (visited on 2023-10-20).

[Roo] Root Server Technical Operations Association. Archive: https://web.archive.org/web/20231020153025if_/https://root-servers.org/. URL: https://root-servers.org/ (visited on 2023-10-19).

[Som+21] Raffaele Sommese et al. "Characterization of Anycast Adoption in the DNS Authoritative Infrastructure". In: *TMA Conference 2021*. IFIP, 2021. ISBN: 9783903176409.

[CAIa] CAIDA. *RSDoS*. Archive: https://web.archive.org/web/20231020153700if_/https://www.caida.org/projects/stardust/docs/data/dos/. URL: https://www.caida.org/projects/stardust/docs/data/dos/ (visited on 2023-10-20).

[CAIb] CAIDA. *The UCSD Network Telescope*. Archive: https://web.archive.org/web/20231020153601if_/https://www.caida.org/projects/network_telescope/. URL: https://www.caida.org/projects/network_telescope/ (visited on 2023-10-20).

[Moo+06a] 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. URL: https://doi.org/10.1145/1132026.1132027.

[Ope] OpenINTEL. *OpenINTEL: Active DNS Measurement Project*. Archive: https://web.archive.org/web/20231020153917if_/https://www.openintel.nl/. URL: https://www.openintel.nl/ (visited on 2023-10-20).

[Dom] Domain Name Industry Brief. *The Domain Name Industry Brief Quarterly Report - Q2 2023 Data and Analysis*. Archive: https://web.archive.org/web/20231020153819if_/https://dnib.com/articles/the-domain-name-industry-brief-q2-2023. URL: https://dnib.com/articles/the-domain-name-industry-brief-q2-2023 (visited on 2023-10-20).

[Som+22] Raffaele Sommese et al. "Investigating the Impact of DDoS Attacks on DNS Infrastructure". In: *Proceedings of the 22nd ACM Internet Measurement Conference*. IMC '22. Association for Computing Machinery, 2022, pp. 51–64. ISBN: 9781450392594. DOI: 10.1145/3517745.3561458. URL: https://doi.org/10.1145/3517745.3561458.

[BB15] Robert Beverly and Arthur Berger. "Server Siblings: Identifying Shared IPv4/IPv6 Infrastructure Via Active Fingerprinting". In: *Passive and Active Measurement*. Ed. by Jelena Mirkovic and Yong Liu. 2015, pp. 149–161. ISBN: 9783319155098.

[Tij20] Tijs Hofmans. "Providers zijn maandag opnieuw getroffen door ddos-aanvallen". In: *Tweakers* (Dec. 1, 2020). Archive: https://web.archive.org/web/20231115170933if_/https://tweakers.net/nieuws/175228/providers-zijn-maandag-opnieuw-getroffen-door-ddos-aanvallen.html. URL: https://tweakers.net/nieuws/175228/providers-zijn-maandag-opnieuw-getroffen-door-ddos-aanvallen.html (visited on 2023-11-15).

[Tra] TransIP. *DDoS attack on March 22nd*. Archive: https://web.archive.org/web/20231115170221if_/https://transip.nl/img/cms/postmortem/ddos_post_mortem_english_march_22.pdf. URL: https://transip.nl/img/cms/postmortem/ddos_post_mortem_english_march_22.pdf (visited on 2023-11-15).

[Bri22] Brian Barrett. "Security News This Week: DDoS Attempts Hit Russia as Ukraine Conflict Intensifies". In: *Wired* (Feb. 26, 2022). Archive: https://web.archive.org/web/20231115172557if_/https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/. URL: https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/ (visited on 2023-11-15).

[MRS22] Jiarun Mao, Michael Rabinovich, and Kyle Schomp. "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, 2022, pp. 487–517. ISBN: 9783030987848. DOI: 10.1007/978-3-030-98785-5_22. URL: https://doi.org/10.1007/978-3-030-98785-5_22.

[Cloa] Cloudflare. *Cloudflare DDoS threat report for 2022 Q4*. Archive: https://web.archive.org/web/20231024154508if_/https://blog.cloudflare.com/ddos-threat-report-2022-q4/. URL: https://blog.cloudflare.com/ddos-threat-report-2022-q4/ (visited on 2023-10-24).

[Gar22] Gary Sockrider. "Direct-Path Flooding Attacks Are on the Rise". In: *NetScout* (July 19, 2022). Archive: https://web.archive.org/web/20231024155336if_/https://www.netscout.com/blog/direct-path-flooding-attacks-are-rise. URL: https://www.netscout.com/blog/direct-path-flooding-attacks-are-rise (visited on 2023-10-24).

[Clob] Cloudflare. *DDoS threat report for 2023 Q1*. Archive: https://web.archive.org/web/20231024154848if_/https://blog.cloudflare.com/ddos-threat-report-2023-q1/. URL: https://blog.cloudflare.com/ddos-threat-report-2023-q1/ (visited on 2023-10-24).

[Cloc] Cloudflare. *DDoS threat report for 2023 Q2*. Archive: https://web.archive.org/web/20231024155255if_/https://blog.cloudflare.com/ddos-threat-report-2023-q2/. URL: https://blog.cloudflare.com/ddos-threat-report-2023-q2/ (visited on 2023-10-24).

[Sta22] William Stallings. *Cryptography and Network Security: Principles and Practice, Global Ed*. Pearson, 2022. ISBN: 9781292437484.

[Moo+06b] 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. URL: https://doi.org/10.1145/1132026.1132027.

[Mou+19] Giovane C. M. Moura et al. "Cache Me If You Can: Effects of DNS Time-to-Live". In: *Proceedings of the Internet Measurement Conference*. IMC '19. Association for Computing Machinery, 2019, pp. 101–115. ISBN: 9781450369480. DOI: 10.1145/3355369.3355568. URL: https://doi.org/10.1145/3355369.3355568.

[Som23] Raffaele Sommese. "Everything in Its Right Place: Improving DNS resilience". PhD thesis. 2023. ISBN: 9789036556682. DOI: 10.3990/1.9789036556699.

[Pat+97] Michael A. Patton et al. *Selection and Operation of Secondary DNS Servers*. RFC 2182. Available: https://www.rfc-editor.org/rfc/rfc2182.txt. IETF, 1997.

[BK16] Dhruba Kumar Bhattacharyya and Jugal Kumar Kalita. *DDoS attacks: evolution, detection, prevention, reaction, and tolerance*. CRC Press, 2016. ISBN: 9781498729642.