DOI: 10.2507/34th.daaam.proceedings.xxx

PREVENTION OF DNS AMPLIFICATION ATTACKS

Josip Stanešić, Zlatan Morić, Vedran Dakić & Matej Bašić

This Publication has to be referred as: Stanesic, J[osip]; Moric, Z[latan]; Dakic, V[edran] & Basic, M[atej] (2023). Prevention of DNS Amplification Attacks, Proceedings of the 34th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/34th.daaam.proceedings.xxx

Abstract

The Domain Name System (DNS) is a critical internet infrastructure component, that translates domain names to IP addresses. This study examines the persistent threat of DNS amplification attacks, which exploit certain DNS servers to magnify query responses, causing network congestion. Despite existing mitigations like Response Rate Limiting (RRL) and DNS Security Extensions (DNSSEC), these attacks remain prevalent. Our comprehensive analysis of over 1.7 million IP addresses reveals that approximately 14.77% of Internet DNS servers support recursive queries without access controls. Notably, vulnerable servers are distributed globally, with Asia, Africa, and South America showing the highest vulnerability rates. This research underscores the urgency of enhancing DNS server security. Recommendations include disabling recursion or implementing strict access controls, deploying rate-limiting measures, and restricting "ANY" queries to mitigate DNS amplification attacks. Collaboration between regulatory bodies and network operators is crucial, especially for government infrastructure. In conclusion, this study provides crucial insights into the state of public DNS servers, their vulnerabilities, and the ongoing threat of DNS amplification attacks. As the internet evolves, vigilance and proactive measures are essential to protect DNS service integrity and availability.

Keywords: DNS; DNS security; Amplification attack; Recursive DNS; DNS RRL.

1. Introduction

Domain Name System (DNS) is a distributed naming system. It enables looking up values of resource records that are distributed in different zones. The most common use case for DNS is translating hostnames to IP addresses. A mapping of a hostname to an IP address is a resource record of type A. There are different record types. Some of the most common types of resource records are A, SOA, AAAA, PTR, MX, NS, and CNAME. and AAAA records are used to translate hostname into IPv4 and IPv6 records respectively. PTR records are used to translate IP addresses into hostnames. CNAME records serve as aliases for A records. SOA records contain information about the DNS zone and NS records identify DNS servers authoritative for the zone.

Hostname together with the zone name represents a Fully Qualified Domain Name (FQDN), for example, the host webserver in DNS zone example.com would have FQDN of webserver.example.com. Zones themselves are hierarchically organized into an inverted tree structure with the . or root zone at its start, top-level domains like .com. one level beneath it, and domains like example.com. beneath TLDs as seen in Fig. 1. Domain hierarchy. Root zone has information on

which servers are responsible for TLDs, and TLDs hold information on which servers are responsible for domains underneath them.

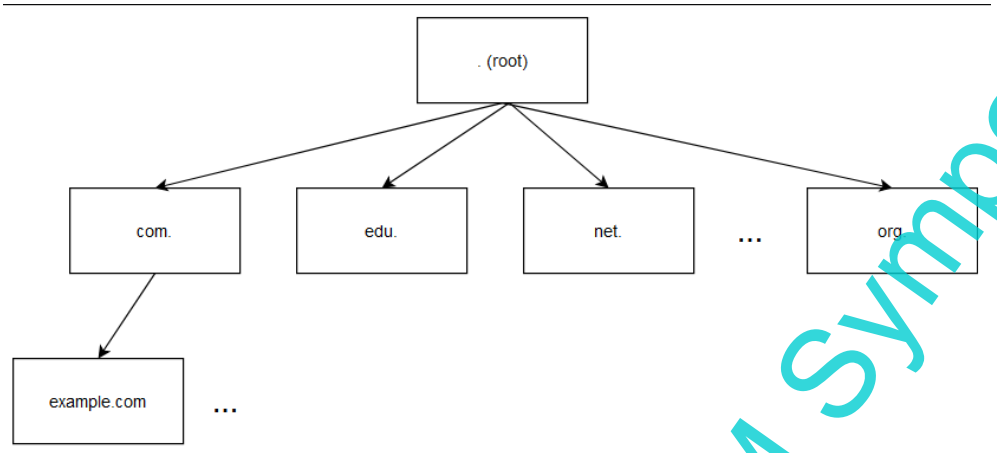

Fig. 1. Domain hierarchy

The client makes a DNS query each time it wants to access a host by referencing its hostname. Resolver is a program that retrieves answers from DNS servers in response to client queries.

Queries themselves can be iterative or recursive. Iterative query means that the server if it is not authoritative for a DNS zone will refer the client to another server and the client must contact the next server. Recursive query means that the DNS server upon getting a request for a zone it is not authoritative for, will query further nameservers to obtain it and return it to the client. This enables more efficient caching of DNS responses. A DNS server can be authoritative for one or more zones, and it is considered authoritative if it contains zone data (resource records) about a specific zone. Also, it needs to be referenced as authoritative by the DNS server one step higher in the hierarchy. A recursive server is a server which will respond to recursive queries.

Having a recursive server inside a network is useful as it will lower the number of queries done due to the caching of responses. DNS servers themselves cache query results for efficiency reasons. In a scenario in which there is nothing cached and there is no recursive DNS server, a client will contact its configured DNS server for a record. If the DNS server is not authoritative for that zone it will forward its request to a root server. The root server will point to the authoritative TLD server. TLD server will point to the authoritative server for that zone, which should return an answer about the requested record. The process would be repeated if another client requires information about the same host. By having a recursive server, the second client would get a cached response without having the whole query process repeated.

The problem with DNS amplification attacks with public DNS servers is that attackers can spoof their source IP addresses to the IP of their target, request records with large responses, and exhaust the bandwidth of their target with responses. Security of public DNS servers is hard to improve as their ownership and the possibility to remediate the configuration is distributed among many entities across the globe.

In scientific literature, DNS amplification attacks were covered for the first time in 1999 [1]. Even 24 years later, solutions recommended then are still not applied, leaving the Internet vulnerable to DDoS attacks. DNS was the protocol used in 24% of UDP reflected amplification attacks observed from April 1, 2021, to March 31, 2022, incoming and outgoing from Azure [2]. This paper aims to investigate the prevalent issue of DNS amplification attacks, which exploit specific DNS server vulnerabilities to magnify query responses. The central questions guiding this research are:

- What is the extent of vulnerability among public DNS servers to DNS amplification attacks, and how prevalent is support for recursive queries without access control?
- Which geographic regions are most affected by these vulnerabilities, and what factors contribute to their distribution?
- What effective mitigation strategies can be recommended to fortify DNS servers against DNS amplification attacks and enhance internet security?

2. Related works

There have been multiple works regarding DNS protocol vulnerabilities, attacks on DNS protocol and DNS servers, improving the security of DNS, and mitigation techniques for the mentioned attacks. DNS was first introduced by RFC 882 in 1983 [3]. 14 years later DNSSEC was introduced in RFC 2065 [4] to add mechanisms that will assure data integrity and authentication by adding cryptographic signatures to DNS records. Unfortunately, this did not make DNS fully secure and immune to malicious usage.

The paper "Motivation for Behaviour-Based DNS Security: A Taxonomy of DNS-Related Internet Threats" by Nikolaos Chatzis from 2007. discusses various DNS-related attacks and categorizes them into three main categories.

Name server vulnerabilities in which attackers are exploiting weaknesses in name server implementations to obtain unauthorized control or perform reconfiguration, and corruption of zone files. These types of attacks are achieved by exploiting software vulnerabilities or misconfiguration. Authenticity and Integrity Attacks in which attacks to authenticity and integrity are done to misdirect users to fraudulent sites or to perform DDoS attacks. These types of attacks include domain hijacking, domain theft, cache poisoning, man-in-the-middle attacks, attacks against non-existent names and reflection attacks using DNS servers (DNS amplification). Consumption attacks can be further split into two more categories: exhausting resources from a single name server or exploiting DNS servers to attack other Internet hosts. Other Internet hosts can be attacked with reflection and amplification attacks. As DNS records can be quite long attackers can use them to deliver malware. Another misuse of DNS is by creating DNS tunnels to avoid firewalls. The paper also emphasizes that while name server vulnerabilities and authenticity/integrity attacks are being addressed, consumption attacks require additional research work [5].

Amplification attacks are effective because of the high amplification rate. “By combining different response types, the amplification effect can reach up to a factor higher than 60. If, for example, the response consists of a 122-byte A type response, a 4000-byte TXT response, and a 222-byte SOA response, the total response consists of 4320 bytes. This yields an amplification factor of 73. Other amplifications are possible depending on the query size and the experienced packet distributions in an actual attack. Due to networking limits, traffic collisions, and other factors, the effective rate of an attack will be significantly smaller than the amplification’s theoretical upper limit.” [6] One of the most famous DNS amplification attacks is the 2013 attack on SpamHous. Attackers were requesting Internet zone files from open DNS resolvers and spoofed IP addresses CloudFlare issued for SpamHous. Open resolvers were responding with a complete DNS zone file creating 75 Gbps of attack traffic. Attackers were issuing requests approximately 36 bytes long and getting responses of approximately 3000 bytes, resulting in almost a 100x amplification factor [7].

CISA describes the DNS Amplification attack as a popular form of a distributed denial of service (DDoS) attack that relies on publicly accessible DNS servers that support recursion to overwhelm the target with DNS response traffic. Attackers will make a DNS request while spoofing the source IP to be that of the target’s with a small request which will result in a very large response. Mitigation techniques recommended are to disable recursion on publicly accessible DNS servers or to allow it only from authorized clients. In case the attack does not rely on recursive DNS servers’ response rate limiting (RRL) should be implemented. Authoritative and recursive servers should run on different systems, with response rate limiting implemented on authoritative servers and access control lists implemented on recursive servers. Another mitigation can be implemented by Internet Service Providers by implementing controls to filter network traffic on their network to reject packets with source addresses not reachable via the actual packet’s path [8]. Based on the results of the Spoofer project conducted by the Centre for Applied Internet Data Analysis (CAIDA) around 20% of Autonomous Systems do not block spoofing [9].

Bind introduced RRL support with version 9.9.4 in 2013 [10] and Windows Server 2016 in 2015 [11]. In a 2020 paper, “The Impacts of DNS Protocol Security Weaknesses” the authors state that “DNS is a highly sensitive part of every ICT system. If attackers can take control of DNS, it would give them unlimited possibilities to abuse the organization in different aspects. DNS is a key component in the concept of multilayered security.” [12] In comparison to [5]. As opposed to 13 years ago attackers are still using similar attacks and combining them with other attacks to achieve their goals. One example of that is a DNS rebinding attack in which attackers trick the victim’s browser into making requests to local network devices. In a 2019 quantitative study [13] researchers found that about 16% of authoritative DNS servers employ some sort of rate limiting.

Waseda University has conducted a large-scale survey into the adoption of various DNS security mechanisms - DNSSEC, DNS Cookies, CAA, SPF, DMARC, MTA-STS, DANE, and TLSRPT and in doing so identified what effects adoption rates and reported its results in a blog post [14]. They discovered that DNS security that is easier or cheaper to deploy is more widely adopted and that root servers and top-level domains are leading adopters of DNSSEC and DNS Cookies.

One of the most important guidelines for securing DNS is NIST’s Secure Domain Name System (DNS) Deployment Guide [15] which should be followed by all administrators of private and public DNS servers. Due to the distributed nature of DNS, all entities that host DNS servers should take part in protecting such an important system and making sure it is not misused. It does not mention ANY records, but Cloudflare recommends their removal and disputes their usefulness in real-life scenarios [16].

In a 2015 paper researchers reported statistics on DNS servers after tracking them for 13 months starting on January 31st, 2014. During that time, DNS resolvers dropped from 26.8 to 17.8 million servers. Also, by comparing responses they found out that more than 3 million servers redirect specific domain names to landing pages for censorship [17]. In a 2019 paper researchers found that there are around 3 million open resolvers on the Internet, and of those 110k provide incorrect IP addresses as a DNS response with more than 26k servers returning IPs reported as malicious. [18]

Attackers can use information stored inside DNS records with other information related to a particular entity to perform OSINT investigations as demonstrated in “Croatian Bank Security Analysis by Publicly Available Data” [19].

DNS did not lose its importance with IPv6 or move from self-hosted to cloud and hybrid infrastructure. DNS as a service, operated by cloud providers offers easier protection from DDoS attacks, higher availability, and moving the responsibility of securing DNS servers to cloud providers [20]. Cloud vendors due to the centralization of resources have higher budgets and easily available infrastructure distributed throughout the globe. Although by centralizing where the

DNS zones are hosted a potential compromise can be more damaging. Applications designed for the cloud still reference other hosts and services through their DNS names.

DNS in Internet of Things (IoT) environments offers to solve multiple use cases. It can help with uniquely identifying devices, autoconfiguration, security, and interoperability. One of the challenges is that IoT devices are designed with constricted capabilities. [21]. In 2015 papers authors stated that "The concept of IoT represents the evolution of the Internet and its appliance is continuously growing. According to estimates, through this concept, 50 billion devices will be connected by 2020 which places heavy demands and challenges in maintaining the required safety level of such an environment." [22] As the growth of IoT added a huge number of devices with often low levels of security, attackers are using them to create botnets for malicious purposes. One of the biggest DDoS attacks was done by the Mirai botnet against the Dyn DNS service provider by using several hundred thousand devices. For approximately two hours, the attack on Dyn made multiple internet platforms inaccessible including PayPal, Twitter, Reddit, Sony, Amazon, Netflix, Spotify, Pinterest, SoundCloud, Squarespace, and several major news websites. Due to the attack on Dyn and its business interruption, it lost 8% of its customer base [23].

3. Data Collection

To find all DNS servers on the Internet masscan [24] was used to find all IP addresses listening on port 53 UDP and TCP. Afterwards, to get valid DNS recursive DNS servers, all of them were queried for A record for google.com. Those that provided a valid DNS response were later tested for recursion. A response was considered valid if it was returned in 3 seconds. IPs were related to a country by using the MaxMind GeoLite2 database.

Initially, we wanted to test servers for zone transfer, recursion, DNSSec, RRL, DNS Socket Pool utilization, and DNS Cache locking, but we were unable to do so without deducing zones which the DNS server is hosting from its IP address. Performing reverse lookup was not a reliable method as DNS servers can host multiple zones and the FQDN of the DNS server does not need to match the zone it is hosting. Zone transfer and DNSSec require knowing the zone name, DNS socket pool utilization requires tracking which port does DNS server uses to issue queries, and checking DNS cache locking requires effectively attempting to do DNS cache poison on every DNS server. Testing RRL was not conducted as DNS servers can be behind a load balancer or have different RRL based on the domain as noted in [13]. Another limitation of our data collection is that we did not track changes to these settings over a longer period.

As opposed to [25] our focus was not analysing data collected at Internet eXchange Points but collecting data from servers like it was done in [17].

4. Data analysis and results

Examining the entirety of public IPv4 addresses culminated in the identification of a substantial dataset comprising 1,740,663 distinct IP addresses, each characterized by the presence of an open port 53—an indicative marker of potential involvement with the Domain Name System (DNS), an integral facet of internet functionality. IP addresses in the resulting data set were further analysed by assessing the responses IP addresses returned for DNS queries to identify valid DNS server installations within this subset, with a focus on ascertaining the subset capable of facilitating recursive query resolution.

Parsing the responses yielded a compelling insight: within the subgroup of IP addresses harbouring an open port 53, 957,806 addresses exhibited a coexistence of DNS server installations. DNS installations were identified by receiving a valid DNS response. Valid DNS servers were further tested for the presence of the Recursion Available (RA) flag within their responsive DNS messages, signifying their potential for engagement in the mechanics of recursive query resolution.

A total of 141,443 servers emerged, each endowed with the capacity to undertake recursive query resolution. This means that of all DNS servers on the Internet, 14.77% support recursive resolution without any access control. It is theoretically possible that an access control exists albeit very wide. However, our research was not confined to empirical observation alone; rather, it underscored a formidable concern, thereby enhancing the gravity of our findings. The spectre of DNS amplification attacks underscores the necessity to fortify these servers against vulnerabilities susceptible to malicious exploitation.

Transitioning from empirical revelations to a broader contextualization, we shift our gaze to the geographical distribution of these vulnerabilities. Our inquiry led us to discern that the top 20 countries harbouring vulnerable servers are China (21,393), the United States (20,661), South Korea (10,147), Bangladesh (8,131), Indonesia (7,853), Russia (7,733), Brazil (5,978), India (5,276), France (3,460), Ukraine (2,573), Japan (2,485), Germany (2,051), Argentina (1,961), Poland (1,761), Turkey (1,756), Colombia (1,750), South Africa (1,668), Taiwan (1,572), United Kingdom (1,537), and Canada (1,468). We observed a correlation between the number of DNS servers and the prevalence of vulnerable instances. Notably, countries with a higher number of DNS servers exhibited a proportionate increase in vulnerable instances. We found that the correlation between the number of DNS servers and the number of ones that accept recursive queries is 0.788955.

However, our investigation did not cease at a mere enumeration of vulnerable instances; it extended to a nuanced exploration of the correlation between the number of DNS servers and the percentage of instances supporting recursion. Intriguingly, a negative correlation emerged (-0.127182), emphasizing that an abundance of DNS servers does not

inherently correlate with an equal proportion of instances supporting recursion. This observation underscores the complexity of the underlying dynamics.

To circumvent potential distortions introduced by countries with minimal DNS servers, we analysed by excluding nations with fewer than 100 DNS servers. This refined analysis revealed a distinct hierarchy of vulnerability. Bangladesh (91.68%), Yemen (89.03%), Dominican Republic (85.48%), Colombia (74.98%), Palestine (72.62%), South Korea (70.63%), Guatemala (70.04%), Lebanon (69.23%), Kenya (67.26%), Cambodia (65.78%), Philippines (65.17%), Pakistan (62.62%), Honduras (61.87%), Libya (61.82%), Nicaragua (60.74%), Indonesia (59.89%), Albania (58.67%), Bolivia (57.91%), Venezuela (57.38%), and Mongolia (57.07%) were identified as the countries with the highest percentages of vulnerable servers.

Seeking to distil broader patterns, we aggregated countries into continents.

Continent	DNS server instances	Recursive DNS servers	Percent
North America	344928	24332	7.05%
Asia	286221	77224	26.98%
Europe	267283	22963	8.59%
South America	33014	11793	35.72%
Oceania	13156	1502	11.42%
Africa	8571	3216	37.52%

Table 1. DNS and recursion across continents

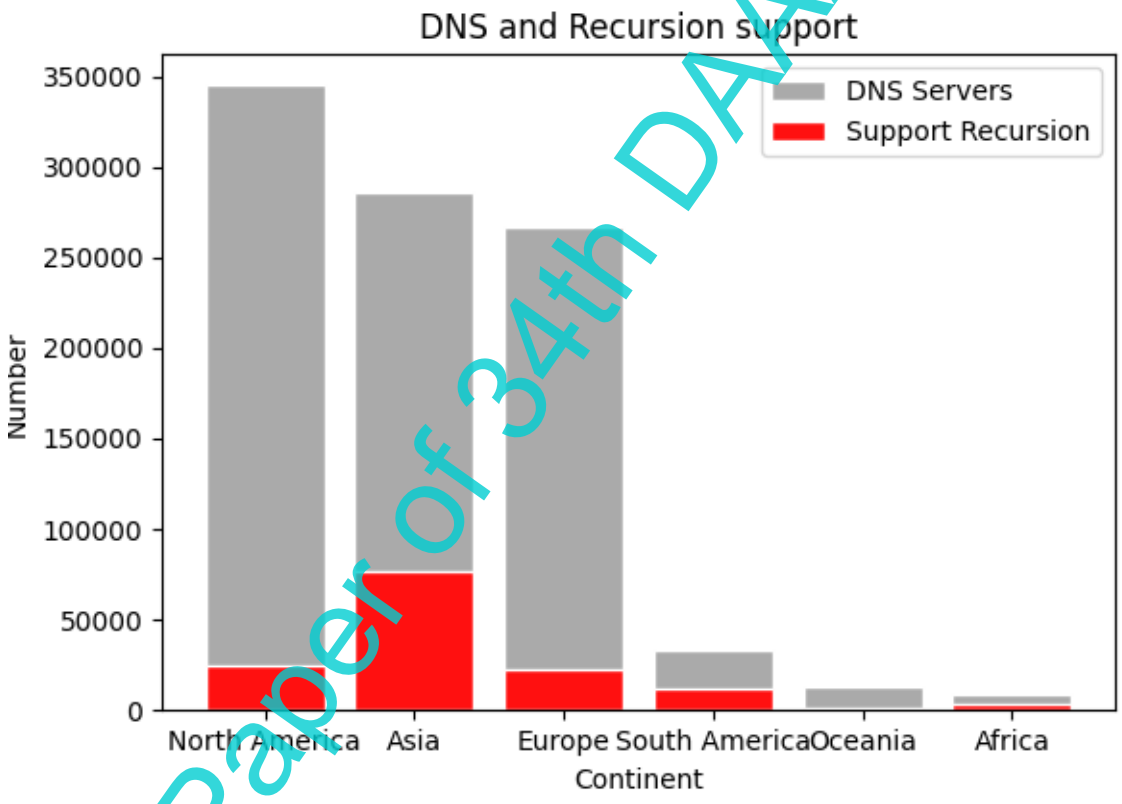

Fig. 2. DNS and recursion support

Africa, South America, and Asia have the highest number of vulnerable servers with more than 20% of them being recursive as seen in Table 1 – DNS and recursion across continents, and Fig. 2. DNS and recursion support. This continental-level analysis accentuates the necessity for comprehensive security measures and vigilance, particularly within previously mentioned regions. On the other side, Europe, and North America with many DNS servers have a small percentage of vulnerable DNS servers. MaxMind GeoLite2 database used was not able to correlate 3417 IP addresses with a country/continent.

For further research, there are multiple directions of whom all can contribute to the ongoing efforts to strengthen the security of DNS infrastructure and protect against DNS amplification attacks, which continue to pose a significant threat to the stability and availability of the Internet. One of the possible directions is tracking how the number of public and recursive DNS servers change over time and how does increasing number of IoT devices will affect the amount of valid

and malicious DNS traffic. Another direction would be tracking the implementation of global DNS security mechanisms and correlating to multiple other factors like changes in attack methodology used by malicious actors, the correlation between implementation of security mechanisms and industry and government regulations of IT infrastructure, and the level of awareness and education of DNS server administrators.

5. Conclusion

High amplification rates created by queries with large responses provide an easy way for attackers to make their attacks more efficient and destructive. The growth of IoT represents a challenge for defence against DDoS attacks as number of devices connected to the Internet rapidly increases. Based on the results of our study we identified that the number of DNS servers on the Internet is decreasing as compared to the results of previous studies. Among the remaining DNS servers, 14.77% of them is recursive which can be abused by malicious actor and should be properly secured. The number of DNS servers that support recursion does not correlate directly with the number of DNS servers but depends on other factors as well. The highest number of recursive DNS servers was found in Asia.

Responsibility for the implementation of security measures lies with operators of specific DNS servers. In case when those servers are part of government infrastructure regulatory bodies should enforce adherence to best practices. Operators of DNS servers should completely disable recursion or restrict it by ACLs. If required recursive DNS servers can be deployed only for internal clients. Deploying rate limiting will also decrease the efficiency of amplification attacks as the total number of queries will decrease. Blocking or restricting ANY queries will limit the size of records attackers can request. NIST Secure DNS deployment guide offers useful guidelines to secure DNS servers but due to its age, it is ready for a new revision.

For future work, it would be useful to measure the implementation of DNS security measures over time and track how the attacker's methodology changes.

6. References

[1] https://web.archive.org/web/20070203060758/http://www.ciac.org/ciac/bulletins/j-063.shtml (1999). J-063: Domain Name System (DNS) Denial of Service (DoS) Attacks, Computer Incident Advisory Capability, Accessed on: 2023-06-02

[2] https://www.microsoft.com/en-us/security/blog/2022/05/23/anatomy-of-ddos-amplification-attacks (2022) Azure Network Security Team, Anatomy of a DDoS amplification attack, Accessed on: 2023-06-01

[3] Mockapetris, P. (1983), Domain Names - Concepts and Facilities, IIS

[4] https://datatracker.ietf.org/doc/html/rfc2065 (1997) Domain Name System Security Extensions, Internet Requests for Comments

[5] Chatzis, N. (2007), Motivation for Behaviour-Based DNS Security: A Taxonomy of DNS-Related Internet Threats in The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007), Valencia, Spain

[6] Anagnostopoulos, M.; Kambourakis, G.; Kopanos, P.; Louloudakis G. & Gritzalis, S. (2013), DNS amplification attacks, Computers & Security, doi:10.1016/j.cose.2013.10.001

[7] M. Prince (2013). The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)

[8] https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks (2013). DNS Amplification Attacks, Cybersecurity and Infrastructure Security Agency

[9] https://spoofer.caida.org/summary.php (2015). State of IP Spoofing, Center for Applied Internet Data Analysis

[10] Behjat A. (2013), BIND 9.9.4 Released, Internet Systems Consortium

[11] https://learn.microsoft.com/en-us/archive/blogs/teamdhcp/response-rate-limiting-in-windows-dns-server (2015). Response Rate Limiting in Windows DNS Server, Microsoft

[12] Dimitrov, W. & Panayotova, G. (2020). The Impacts of DNS Protocol Security Weaknesses

[13] Deccio, C.; Argueta, D. & Demke, J. (2019). A Quantitative Study of the Deployment of DNS Rate Limiting, IEEE, 2019, pp. 442-447

[14] https://blog.apnic.net/2021/11/26/adoption-of-dns-security-mechanisms-related-to-ease-of-use-cost (2021). Adoption of DNS security mechanisms related to ease-of-use, cost, APNIC, Accessed on: 2023-05-22

[15] Chandramouli, R. & Rose, S. (2013). Secure Domain Name System (DNS) Deployment Guide

[16] Majkowski, M. & Guðmundsson Ó. (2015), Deprecating the DNS ANY meta-query type

[17] Kührer, M.; Hupperich, T.; Bushart, J.; Rossow, C. & Holz, T. (2015). Going wild: Large-scale classification of open DNS resolvers, 15th ACM Internet Measurement Conference (IMC)

[18] Park, J.; Mohaisen, M & Mohaisen A. (2019). Investigating DNS Manipulation by Open DNS Resolvers, CoNEXT '19 Companion: Proceedings of the 15th International Conference on emerging Networking EXperiments and Technologies, doi:10.1145/3360468.3368172

[19] Matvej, E.; Morić, Z. & Papić, S. (2020). Croatian Bank Security Analysis by Publicly Available Data in Proceedings of the 31st International DAAAM Symposium

[20] Aishwarya, C.; Sannidhan, M. S. & Rajendran, B. (2014). DNS Security: Need and Role in the Context of Cloud Computing in 3rd International Conference on Eco-friendly Computing and Communication Systems, Mangalore, India
[21] Ayoub, I.; Balakrichenan, S.; Khawam, K. & Ampeau, B. (2023). DNS for IoT: A Survey, Sensors
[22] Cvitić, I.; Vujić, M. & Husnjak, S. (2016). Classification of Security Risks in the IoT Environment, in Proceedings of the 26th DAAAM International Symposium
[23] Young, K. (2022). Cyber Case Study: The Mirai DDoS Attack on Dyn
[24] Graham, R. D. (2021), Masscan, Github, https://github.com/robertdavidgraham/masscan, Accessed on: 2023-04-04
[25] Nawrocki, M.; Jonker, M.; Schmidt, T. C. & Wählisch, M. (2021). The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core, In Proceedings of the 21st ACM Internet Measurement Conference (pp. 419-434), doi: 10.48550/arXiv.2109.01104 ecosystem from the internet core..