DDoS attack: DNS Reflection and Amplification

Andreoli C. - Ligari D. - Alberti A. - Scardovi M. - Intini K.
University of Pavia, Italy
Department of Computer Engineering - Data Science

Abstract

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

1 DNS based DDoS attacks

The DNS service is a critical part of the Internet infrastructure. Almost every communication exploits the DNS service, and attacking it could lead a significant number of networked applications to run out of service. The DNS service has been designed to provide fast responses and is less oriented towards security, which makes it vulnerable to different types of attacks. According to a recent Cloudflare's report[6] the most used vector in DDoS is the DNS. The types of attacks involving DNS are of three main types: *DNS query flood*, *TCP flood*, *DNS reflection and amplification*, and *DNS water torture*.

DNS query flood
This is a direct attack aimed at consuming the server resources until run it out of service. The attacker sends a large number of DNS queries to the target recursive DNS server, leveraging a zombie devices army (botnet). The requests are structured in a way that the server has not the record cached and it is forced to perform recursive queries to provide the responses. It is easier to perform this type of attack on smaller DNS servers that may have limited resources to handle a large number of queries.

TCP flood
This is another type of attack aimed at consuming the server resources. These latter are consumed by the attacker sending lots of TCP connection requests without closing them. The server is forced to allocate resources to handle the TCP connections and, when the numbers get larger it may run out of resources.

DNS water torture
This is a type of indirect attack aimed at consuming the resources of a target authoritative DNS server. The attacker sends a huge number of queries about properly constructed hostnames. These are made up by two parts: the domain whose authoritative server is the target, and a random string such that the FQDN cannot exist. That way the recursive NS starts its search until it reaches the authoritative server. This latter notices the non-existence of the FQDN and sends NXDOMAIN response. All the queries travel until the authoritative server, which is forced to handle all of them until it is overwhelmed.

DNS reflection and amplification
This is an indirect attack aimed at consuming the target network bandwidth. It start with the spoofing of the target's IP address, then lots of queries are sent to the DNS server using as the source address the spoofed IP address. This latter will receives the responses from the DNS server (reflection). The queries are structured in a way that the responses are larger in size (amplification). That way the target's bandwidth is fulfilled, with the

attacker having used just a small quantity of its resources. The effectiveness of this attack is given by the amplification factor (AF), measured as the ratio between the size of the response and the size of the query. An easy but effective choice for the attacker is to perform a type ANY which provides a large AF.

Since according to the already cited report[6] the most common type of attack is the DNS reflection and amplification, in this project we focus on this type of attack.

2 Mitigation measures

There exist a variety of measures that can be employed to mitigate the effects of DNS amplification attacks. These measures can be broadly categorized into two groups: those that aim to reduce the probability of an attack occurring, and those that aim to minimize the impact of an attack by detecting it early and enhancing the resilience of the DNS service.

2.1 Proactive measures

Rate limiting
Rate limiting is a measure that can be used to mitigate the impact of DNS amplification attacks. The idea behind rate limiting is to limit the number of responses that a DNS server can send to a specific IP address within a certain time period. That way the queries sent by the attacker are dropped by the DNS server, thus reducing the amplification effect.

Trusted sources
When a DNS recursive server is open on the Internet, it can receive queries from any source. The range of IP addresses that can be spoofed is very large and it is not possible to block all of them. However, it is possible to limit the number of sources that can send queries to the DNS server, creating a whitelist of trusted sources. This measure reduce the probability of an attack occurring, however, the trusted sources could be spoofed, thus the attack be performed.

Firewall
A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. Setting up a proper firewall both DNS server side and victim side can block unauthorized traffic and reduce the impact of the attack.

2.2 Detection measures

The DNS amplification attack has as core activity the IP spoofing. A mechanism able to discriminate between a original source IP address and a spoofed could detect the attack. This is the main idea behind the *detection* techniques.

Routing hops detection
This mechanism was proposed by Jin and Wang in this paper[11]. The idea is to exploit the inconsistency between the number of hops of a spoofed IP packet and the spoofed IP address itself. The hops number is inferred by the TTL value in the IP header. This mechanism can detect almost 90% of the spoofed packets.

Machine Learning
In the last decade with the developing of machine learning, some algorithm have been proposed to detect the DNS amplification attack. In 2015 Meitei et al.[9] proposed a machine learning based approach to detect the attacks, using *Random Forest*, *MLP* and *SVM* algorithms. However, a more recent publication[10] by Mathews et al., shows that using an adversarial neural network approach (EAD) it is possible to easy circumvent the detection. The core idea is to train a network to slightly modify the input data (DNS queries) in order to fool the detection algorithm.

2.3 Resilience measures

These measures are more focused on making the DNS more robust to the attack, allowing it to continue to provide the service even during the attack.

Anycast scheme
The DDoS attack is aimed at causing a service outage on a victim server by flooding it with a large number of packets. The idea behind the anycast solution is to have many replicas of the victim server with same logical IP address, and to choose the destination of the packets according to some routing criteria. That way, the packets are distributed among the replicas, thus reducing the load on each of them. In 2015[8] the DNS root name servers received a big DDoS attack, which lead to e denial of service in some of them. Thanks to the anycast schema (11 out of 13 root servers are anycasted), the attack was mitigated. The attack showed that the anycast schema can helps increasing the DNS server resilience but not completely protect from DDos attacks.

Caching behavior
This approach is discussed by Wei-min et al. in this paper[3]. They support that a relatively simple change in the caching behavior of a DNS server can significantly improve the DNS performance under a DDoS attack. They propose a DNS server should not evict the cache entries when it detects the relevant DNS servers are unavailable and delete them as soon as this latter become available again. That way, even during an attack running out of service a relevant server, the DNS recursive server can still serve the cached entries, thus providing part of the requested domain names.

References

[1] Admir Dizdar. DNS Amplification Attack: How they Work, Detection and Mitigation, October 2021. URL https://brightsec.com/blog/dns-amplification-attack/.

[2] Lei Fang, Hongbin Wu, Kexiang Qian, Wenhui Wang, and Longxi Han. A comprehensive analysis of ddos attacks based on dns. *Journal of Physics: Conference Series*, 2024:012027, 09 2021. doi: 10.1088/1742-6596/2024/1/012027.

[3] Li Wei-min, Chen Lu-ying, and Lei Zhen-ming. Alleviating the impact of dns ddos attacks. *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, 1:240–243, 2010. doi: 10.1109/NSWCTC.2010.63.

[4] Rebekah Taylor. Four major DNS attack types and how to mitigate them, August 2021. URL https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/.

[5] Admir Dizdar. 5 dns attack types and how to prevent them, May 2022. URL https://brightsec.com/blog/dns-attack/.

[6] Pacheco Yoachimik. Ddos threat report for 2023 q1_2023, Apr 2023. URL http://blog.cloudflare.com/ddos-threat-report-2023-q1/.

[7] G. Usha Devi. Detection of ddos attack using optimized hop count filtering technique. *Indian Journal of Science and Technology*, 8(1):1–6, Jan 2015. ISSN 09746846, 09745645. doi: 10.17485/ijst/2015/v8i26/83981.

[8] Wouter de Vries, Ricardo Schmidt, and Aiko Pras. Anycast and its potential for ddos mitigation. *ResearchGate*, Jun 2016. doi: 10.1007/978-3-319-39814-3_16.

[9] Irom Meitei, Johnson kh, and Tanmay De. Detection of ddos dns amplification attack using classification algorithm, 08 2016.

[10] Jared Mathews, Prosenjit Chatterjee, Shankar Banik, and Cory Nance. A deep learning approach to create dns amplification attacks. In *2022 4th International Conference on Management Science and Industrial Engineering (MSIE)*, page 429–435, Apr 2022. doi: 10.1145/3535782.3535838. URL http://arxiv.org/abs/2206.14346. arXiv:2206.14346 [cs].

[11] Cheng Jin and Haining Wang. Hop-count filtering: an effective defense against spoofed ddos traffic, 01 2003.