A Comprehensive Analysis of DDoS attacks based on DNS

Journal of Physics: Conference Series **2024** (2021) 012027 doi:10.1088/1742-6596/2024/1/012027

A Comprehensive Analysis of DDoS attacks based on DNS

Lei Fang[1*], Hongbin Wu[1*], Kexiang Qian[1], Wenhui Wang and Longxi Han[1]

[1] State Grid Key Laboratory of Information and Network Security, Global Energy Interconnection Research Institute co., Ltd, Beijing, 102209, China

[*]wuhongbin@geiri.sgcc.com.cn

Abstract. Domain Name System (DNS) is a basic and important services on the Internet. However, Distributed Denial of Service (DDoS) has been a threat to the security and stability of DNS for a long time. In this paper, we take a review of DDoS attacks based on DNS aiming to make a better understanding of it. Firstly, we analyse the security vulnerabilities of DNS related to denial-of-service attack. Then we discuss the classification of DNS DDoS attacks, and divide them into four categories according to the attack mode. Finally, we summarize the existing defense methods of two aspects. We aim to get a better understanding of the DDoS attacks based on DNS and expand the understanding of DDoS attacks.

1. Introduction

DNS is one of the most important network infrastructures, mainly responsible for the transformation of domain names into IP addresses. Almost all Internet applications depend on DNS. Due to the easy implementation, difficult tracking and serious consequences, distributed denial of service attack become a major problem of network security. And the DDoS against DNS will bring great damages and extensive influence.

In October 2016, Dyn, a service provider, suffered a DDoS attack of its DNS, which took down the service for many websites, including Visa, Amazon, GitHub, and so on. It was one of the largest bandwidth DDoS attacks ever recorded, with attack bandwidth over 650 Gbps. In October 2019, the DNS server of the famous cloud services company AWS suffered a DDoS attack, which lasted for 15 hours and caused partial AWS service to be paralyzed.

DNS has the following security vulnerabilities related to denial-of-service attacks.

a) Lack of legitimacy verification: The client program determines whether the response matches with the query through the port number and serial number, but there is no mechanism to authenticate the legitimacy of the reply content. It is easy to receive the reply message of incorrect mapping between domain name and IP address.

b) Open system: The DNS system is open and provides services continuously. The data on most DNS servers is unencrypted and has no access restrictions. Customers in different regions can access the same DNS server, and most DNS servers allow recursive queries.

c) Connectionless: Each access is independent. Most of the network layer protocol used by DNS clients and servers for query requests is UDP, which does not require three-way-handshake.

d) Stateless: It means that the protocol has no memory for transactions. The DNS server does not record the client's request or its own response. If the client requests the same domain name resolution repeatedly, the server responds to the query continuously. The attacker can conceal himself from traceability very well.

Open systems result of DNS having to accept all user requests unconditionally, and the attack messages of DNS are all legitimate DNS UDP requests, which are difficult to be recognized by ordinary DDoS protection equipment. The failure of a single DNS server or domain name can cause the failure of other DNS systems, and causing Dominoes Effect.

In this paper, we try to further understand DDoS attack based on DNS, analyze and summarize the attack characteristics and defense methods, aiming to lay a theoretical foundation for future research. The remaining part is organized as follows. Section 2 discusses the classification of attacks, Section 3 summarizes current detection and defense methods, and make a conclusion in Section 4.

2. Attack classification

We can divide DNS DDoS attacks into different types according to its attack path, target, mode, etc. According to the attack path, it can be divided into direct attack and stepping attack. Direct attack is to send flood DNS request message to the target DNS server directly. Stepping attack does not attack the target DNS server directly, but by sending flood DNS request message to the common recursive server.

When it comes to attack target, one is aimed at the DNS server, and another is using DNS server as an attack amplifier to cause other host denying of service.

According to the mode of resource consumption, it can be divided into server resource consumption and bandwidth resource consumption. Server resource consumption is to send a large number of flooding DNS requests, consume the resources of DNS server, make it reach or exceed the service limit. For example, the domain name prefix or suffix DNS flood attack. Bandwidth resource consumption is to consume the outlet bandwidth of the DNS system, block the normal DNS reply message to the user. Such as DNS flood amplification attack.

According to the attack mode, it can be divided into DNS query flood, DNS reply flood, DNS water torture attack and hybrid attack. DNS query flood is to send a large number of DNS query requests to the selected server directly, forcing the server to run out of resources [1]. DNS reply flood is by using the open recursive service of DNS server to amplify the attack traffic and carry out DDoS attack on some victims. DNS water torture attack appends an invalid random prefix to the target domain to bypass the DNS cache and tries to overwhelm an outside victim's authoritative DNS servers.

2.1. DNS query flood

The attack is to send a large number of DNS query requests to the DNS server to achieve the purpose of denial of service. Common attack methods include using powerful servers or zombies to send plenty of domain name resolution requests with counterfeited source IP or using zombies to initiate a great deal of domain name resolution requests with real source IP. In general, when DNS servers receive a request with not recorded in the cache, the recursive server needs to perform a recursive query. If the attacker carefully constructs and forges the domain name, the cache will certainly have no record of it. Therefore, for each query, the DNS server has to issue recursive queries. With relatively low performance of recursive servers, they are easily to be overwhelmed. If the attack requests are mostly recorded in the cache server, it will mainly put pressure on the cache server.

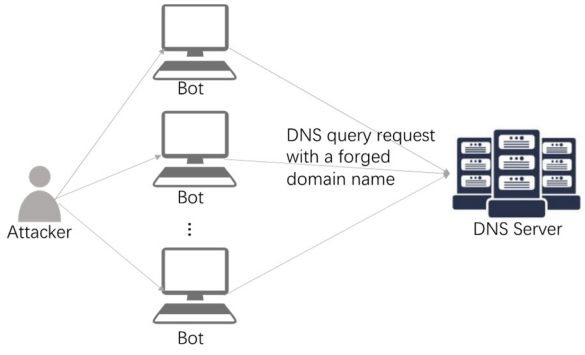

Figure 1. DNS Query Flood

2.2. DNS reply flood

DNS service is mainly based on UDP protocol, which is stateless. When the DNS server receives the reply message, it will process the message regardless whether it has sent a resolution request. DNS reply flood is that the attacker sends a large number of DNS reply messages to the DNS cache server, causing the cache server to run out of resources by processing these reply messages, as shown in figure 2.

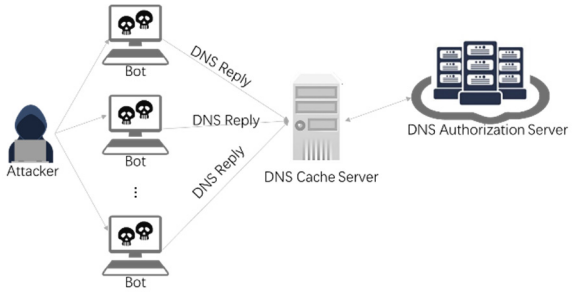

Figure 2. DNS Reply Flood

DNS reflection flood is a variation of the DNS reply flood. It's more aggressive and harder to trace. As shown in figure 3, attackers forge their own source IP address into the IP address of the target, and then send a flood of query requests to a series of open DNS servers. By forging the source IP address of the DNS request message, these DNS response messages will be directed to the target.

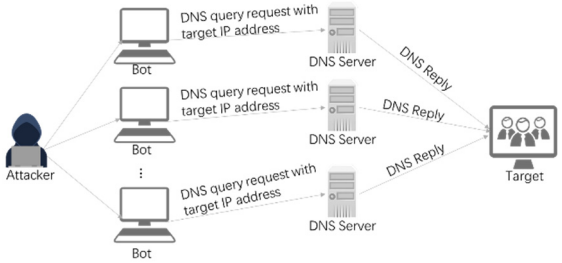

Figure 3. DNS Reflection flood

As early as 2001, Paxson et al. [3] mentioned that DNS servers can act as a reflector of traffic amplification attacks. The size of DNS reply message is usually several times or even dozens of times of that of DNS request message. It would not be too difficult for an attacker controlling thousands of zombies to generate DNS attack traffic. The amplification effect of attack traffic is measured by the Amplification Factor (AF), which is defined as $\mathrm{AF} = \frac{size(reply\ message)}{size(request\ message)}$. The size of request message is mainly determined by the length of the queried domain name. The shortest domain name is '.', so the query packet is at least 17 bytes. DNS protocol stipulates that UDP DNS reply message is 512 bytes at most, so the maximum amplification factor is 30. Anagnostopoulos M et al. [4] proposed a DNSSec based attack with a maximum amplification factor of 44 due to the introduction of digital signatures. Sieklik B et al. [5] proposed that the amplification factor can reach 60 at the Trivial File Transfer Protocol. The introduction of the EDNS0 mechanism makes the DNS reply packet size typically scalable to 4096 bytes, and the request packet requires an additional 11 bytes. Therefore, the range of amplification factors is approximately 1 to 146. In addition, Sattar U et al. [6] proposed amplification attack with modified bloom filters.

2.3. DNS water torture attack

DNS water torture attack first appeared in February 2014[7]. It attaches the invalid random prefix to the target domain to bypass the DNS cache, and then dynamically forward it to the relevant authority server by the DNS resolver, and finally achieve the purpose of draining the authority server resources. Take

the attack domain name abc.com as an example, the general attack process is shown in figure 4. The attacker controls zombies to generate a large number of random subdomains for abc.com and send them to the resolver. The resolver can be any device with DNS forwarding characteristics, such as a recursive DNS server or a gateway router. Since the above random subdomain does not exist, the resolver first requests the root server for the IP address of authoritative server containing .com. Eventually lead to all invalid attack queries are forwarded to that authoritative server. For each query, the authoritative server returns the NXDOMAIN record to the resolver, which then forwards the record to the client IP address (which is usually forged by the attacker). After the authoritative server becomes overwhelmed, the resolver waits for the full failure response time for each remaining attack query. In this case, the resolver's resources will quickly run out as well. For example, the notorious IoT botnet Mirai disrupted the Internet services of Twitter, Net-Flflix, Amazon, and other major companies through DNS water torture attack [8].

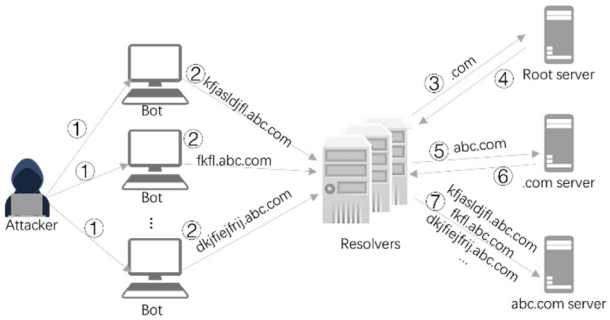

Figure 4. DNS Water Torture Attack

2.4. Hybrid Attack

Just as its name implies, it is a combination of various forms of attack. For example, Bushart J et al.[9] propose a new attack called DNS Unchained, which combines amplification with application layer attack. They carefully chain CNAME records and force resolvers to perform deep name resolutions effectively overloading a target authoritative name server with valid requests, to achieve an attack amplification of 8.51.

3. Detection and defense methods

In order to prevent DNS server from DDoS attacks, there are two main research directions at present. One is to study the detection method to find the attack behaviour quickly and filter the attack traffic effectively. And another is to study how to enhance the defense ability of DNS server to ensure that the server can still provide services for normal users when attacked.

3.1. Detection methods

Among the attack methods mentioned in section 2, DNS reflection flood and water torture attack are more effective and have a greater impact than DNS query flood. Related studies mainly focus on the effective detection methods for them.

DNS reflection flood and most of the DNS query attack use the source IP address forgery technology. If the forged IP address can be effectively detected, it will be easier for detecting the DDoS attack against DNS server. And according to the forged IP address, we can filter the attack traffic. In 2003, Jin C et al. [10] proposed a mechanism based on the number of routing hops to detect and filter the source IP address forgery packet As the attacker can forge the source IP address to send a request to the DNS server, but the packet sent by the host corresponding to the real IP address is difficult to forge through the number of routing hops to reach the DNS server. This method can identify nearly 90% of the source IP address forgeries. However, it uses the structure of hash table to store a large amount of network information and uses the chain address method to deal with conflicts. On the one hand, it needs a large amount of storage resources and cannot avoid the potential threat of DDoS attack to the dynamic storage structure. On the other hand, a large number of hash collisions can lead to slower queries. In 2006, Guo et al. [11]

proposed to arrange a DNS Guard at the front end of the DNS server. DNS Guard uses cookie combined with the method of communication and verification with the source side. It can identify and block the forged source IP address effectively. The accuracy of this method is high, but it needs to communicate back and forth with the source side continuously, resulting in large additional traffic, and it is easy to be attacked by DDoS based on cookie verification.

In 2007, Kambourakis et al. [12] found that the DNS query and reply packets present basic one-to-one under normal network condition. Thus, they proposed an effective method to detect the amplification attack of DNS. However, the traffic access to DNS servers is usually huge, but the paper does not make any explanation about the effective storage for packets, and the proposed method of blocking source IP addresses with firewalls may cause another form of denial-of-service attack. In 2008, Sun et al. [13] improved the storage for packets and improved the storage structure with bloom filter to reduce the storage space. The proposed method can detect DNS amplification attacks and filter the attack traffic. In 2014, Lim et al. [14] proposed mechanism based on SDN features to block legitimate looking DDoS attacks effectively.

With the development of machine learning technology, more new detection techniques emerge. In 2009, Rastegari et al. [15] proposed an intrusion detection system based on neural network for DoS attack against DNS. In 2010, Subbulakshmi et al. [16] took the normal data flow and DDoS attack flow as a classification problem and proposed a detection technique based on machine learning and support vector machine algorithm. In 2016, Alan Saied et al. [17] used artificial neural network to detect DDoS attack by blocking the forged packet before reaching the target.

In addition, there are some other detection techniques as follows. In 2006, Wang et al. [18] proposed a detection technique based on data mining to detect DDOS attacks. In 2007 and 2008, Choi et al. [19] and Ricardo et al. [20] proposed methods for detecting and monitoring botnet DNS traffic, respectively. In 2013, Wei et al. [21] classified the DNS query traffic and detect anomaly using data mining approach. In 2014, Jose et al. [22] proposed a detection method based on DNS log monitoring with Hadoop. In 2016, Takeuchi et al. [23] proposed a DNS water torture attack detection system based on domain name vocabulary and structure characteristics.

3.2. DNS sever capacity enhancement

One approach to this issue is to limit the speed of DNS traffic. In 2008, Zhang et al. [24] proposed boundary routing exit detection to prohibit packets whose source IP address is not the network segment from flowing out and discard super-large DNS reply packets at the victim server side. This method is simple, effective and can block the DNS amplification attack from the source. However, it requires extensive deployment of the whole network, and cannot effectively filter the attack packets with small amplification ratio. In addition，Response Rate Database (RRL) policy, which implements speed limit control for certain types of reply messages such as NXDOMAIN and NODATA, is an effective way to mitigate DNS amplification or reflection attacks. In 2012, Donnerhacke L [25] proposed DNS Dampening, which is similar to RRL, except that all traffic of this type is discarded for a period of time after the speed limit is triggered. Both of these speed limiting schemes use source IP to distinguish traffic. When the authoritative server is a reflector of amplification attack, the speed limitation can effectively reduce the reflected traffic. However, if the authority server is the target, the attacker can easily make the speed limit mechanism fail by forging a large number of source IP addresses. Attack traffic can also be diverted from legitimate recursive servers. If speed limits or packet loss are implemented based on the source IP, it may cause misjudgement and affect the DNS queries of normal users.

Another solution is to improve the defensive capabilities of authoritative server. In 2007, Pappas et al. [26] used various strategies to set longer TTL values to enhance the ability of DNS servers to resist DDoS attacks according to the characteristics of infrequent changes in resource records of authoritative domain name servers. This strategy can effectively improve the availability of servers and provide domain name resolution services for legitimate users. But it will increase the risk of cache poisoning attacks on DNS servers. In 2008, Ballani et al. [27] proposed to use stale cache to cache the stale resource records in DNS server to alleviate the effect of not being able to provide service normally when DDoS

attack occurs. However, the method of caching expired records violates the semantics of expired records in DNS protocol and cannot be used reasonably, as the canonical DNS specifies that expired TTLs should be discarded from the cache. In 2019, Wang et al. [28] recommend a combination of the authority side and the resolution side to redistribute user traffic. It uses DNAME records to quickly propagate the redirect signal from authoritative name servers to resolvers. These resolvers then track the DNAME records and redirect subsequent traffic to the redirect name servers. In case of DDoS attacks, such DNS traffic redirection would greatly reduce the query load flooding the original name server, thereby reducing the risk of its unavailability or outage.

In addition, there are some other detection techniques as follows. In 2016, Afek [29] proposed a novel mitigation system for amplified DNS DDoS (ADD) attacks called Distributed Rate Sharing based Amplified DNS-DDoS Attack Mitigation (DRS-ADAM), which allows each DNS resolver to detect and stop ADD traffic locally. In 2017, Booth [30] proposed to modify the DNS protocol, specifically, adding two additional timers to mitigate the effects of DDOS DNS attacks. In 2018, Chen et al. [31] proposed a novel method to reduce the DDoS traffic on TLD servers, in which traffic filter based on machine learning algorithms is applied to major recursive DNS servers.

4. Conclusion

The domain name system is a key piece of Internet infrastructure. Even a small part of the DNS infrastructure is not available for a short time can disrupt the entire Internet. Unfortunately, the connectionless and stateless of DNS makes it vulnerable to DDoS attacks, which are very difficult to defeat. DDoS attacks against DNS present a security challenge that needs to be addressed. Only by understanding the attack can we defend against it more effectively. This paper makes a detailed analysis of DDoS attacks based on DNS aiming to extend the knowledge on DDoS attacks. According to the attack mode, DDoS attack based on DNS is classified as DNS query flood, DNS reply flood, DNS water torture attack and hybrid attack. And then the present research results are analysed from the detection and capacity enhancement perspectives. Attack methods will continue to evolve with the development of new technologies, and we suggest that the future research should focus on the DNS DDoS attack in the Internet of things.

Acknowledgments

This work was supported by the National Key R&D program of China (No. 2018YFB0804704).

References

[1] Cheung S. (2006) Denial of Service against the Domain Name System. IEEE Security & Privacy, 4(1):40-45.
[2] Vaughn R, Evron G . (2006) DNS amplification attacks. Network Security.
[3] Paxson, Vern. (2001) An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks. ACM SIGCOMM Computer Communication Review. 31(3): 38-47.
[4] Anagnostopoulos M, Kambourakis G, Kopanos P , et al. (2013) DNS amplification attack revisited. Computers & Security, 39(pt.B):475-485.
[5] Sieklik B , Macfarlane R , Buchanan W J. (2016) Evaluation of TFTP DDoS amplification attack. Computers & Security, 57(mar.):67-92.
[6] Sattar U, Naqash T, Zafar M R, et al. (2014) Secure DNS from amplification attack by using modified bloom filters. Eighth International Conference on Digital Information Management.
[7] Secure64 Software Corporation. (2014) Water torture: a slow drip DNS DDoS attack. https://secure64.com/water-torture-slow-drip-dns-ddos-attack/
[8] M. Antonakakis, T. April, M. Bailey, et al. (2017) Understanding the Mirai botnet. 26th USENIX Security Symposium. pp. 1093–1110.
[9] Bushart J, Rossow C. (2018) DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives. RAID 2018: 139-160

[10] Jin C, Haining W, and K. G. Shin. (2003) Hop-count filtering: An effective defense against spoofed DDoS traffic. CCS'03 Proceedings of the 10th ACM Conference on Computer and Communications Security. pp. 82-96.
[11] Guo F, Chen J, Chiueh T. (2006) Spoof Detection for Preventing Do S Attacks against DNS Servers. ICDCS'06 Proceeding of the 26th IEEE International Conference on Distributed Computing Systems. pp. 52-64.
[12] Kambourakis G , Moschos T , D Geneiatakis, et al. (2007) A fair solution to DNS amplification attacks. WDFIA'07 Proceedings of the Second International Workshop on Digital Forensics and Incident Analysis. pp. 38-47.
[13] Sun C, Liu B, Shi L. (2008) Efficient and Low-Cost Hardware Defense Against DNS Amplification Attacks. Global Telecommunications Conference - GLOBECOM. pp. 2062-2066.
[14] Lim S, Ha J, Kim H, Kim Y, Yang S. (2014) A SDN oriented DDoS blocking scheme for botnet-based attacks. In Ubiquitous and Future Networks. pp. 63-68.
[15] Rastegari, S., Saripan, M.I., Rasid, M.F.A. (2009) Detection of Denial of Service Attacks against Domain Name System Using Neural Networks. IJCSI International Journal of Computer Science Issues. pp. 6(1):23-27.
[16] Subbulakshmi T，Shalinie S M，Ramamoorthi. (2010) A Detection and classification of DDoS attacks using machine learning algorithms. European Journal of Scientific Research. 47(3)：334-346.
[17] A Saied，RE Overill，T Radzik. (2016) Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 172:385-393.
[18] Wang Y, Hu M, Li B, et al. (2006) Tracking anomalous behaviors of name servers by mining DNS traffic. Lecture Notesin Computer Science. 4331:351-357.
[19] H. Choi, H. Lee and H. Kim. (2007) Botnet Detection by Monitoring Group Activities in DNS traffic. 7th IEEE International Conference on Computer and Information Technology. pp. 715-720.
[20] Villamarin-Salomon R, Brustoloni JC. (2008) Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic. 5th IEEE Consumer Communications and Networking Conference. pp. 476-481.
[21] Ruan W. (2013) Pattern Discovery in DNS Query Traffic. Procedia Computer Science, 17:80-87.
[22] A. S. Jose and A. Binu. (2014) Automatic detection and rectification of dns reflection amplification attacks with hadoop mapreduce and chukwa. International Conference on Advances in Computing and Communications.
[23] Takeuchi, Y., Yoshida, T., Kobayashi, R., Kato, M., Kishimoto, H. (2016) Detection of the DNS water torture attack by analyzing features of the subdomain name. pp. 793–801.
[24] Zhang X, Zhao R, Shan Z, Chen J. (2008) Research on exploiting DNS for DoS attack and defence. 29(1):21-24
[25] Donnerhacke L. (2012) DNS Dampening. https://lutz.donnerhacke.de/eng/Blog/DNS-Dampening.
[26] V Pappas，M Dan，L Zhang. (2007) Enhancing DNS Resilience against Denial of Service Attacks. DSN'07 Proceedings of the 37th Annual IEEE/IFIP Conference on Dependable Systems and Networks. pp. 450-459.
[27] H Ballani, P Francis. (2008) Mitigating DNS DoS Attacks. CCS'08 Proceedings of the 15th ACM Conference on Computer and Communications Security. pp. 189-198.
[28] Wang Z. (2019) An elastic and resiliency defense against DDoS attacks on the critical DNS authoritative infrastructure. Journal of Computer & System Sciences.
[29] Afek Y, Bremler-Barr A, Cohen E, et al. (2016) Efficient Distinct Heavy Hitters for DNS DDoS Attack Detection.

[30] Booth T, Andersson K. (2017) DNS DDoS Mitigation, via DNS Timer Design Changes. International Conference on Future Network Systems and Security. Springer, Cham.
[31] Chen L, Zhang Y, Zhao Q, et al. (2018) Detection of DNS DDoS Attacks with Random Forest Algorithm on Spark. Procedia Computer Science, 134:310-315.