National Cyber Security Centre
Ministry of Security and Justice

DNS amplification

Don't leave the backdoor open!

Factsheet FS-2013-03
version 1.0 | 4 October 2013

DNS amplification remains a popular form of (distributed) denial of service ((D)DoS) attacks. It involves attackers using publically accessible, open DNS resolvers to flood their target with large amounts of data traffic. Owners of open DNS resolvers therefore unintentionally and unwittingly become involved in these attacks. Although this is a global problem, the large number of internet connections in the Netherlands comes with a large number of open DNS resolvers. As a consequence, such attacks may occur via Dutch internet infrastructure, even if the attacker and victim of a (D)DoS attack are located abroad. The solution may appear simple: owners of vulnerable DNS systems can easily secure their systems against these forms of abuse. Yet, a considerable number of DNS servers in the Netherlands remain open. Maybe even yours. This factsheet provides information about DNS amplification, including how to recognise a DNS amplification attack and what you can do protect yourself from it.

What is DNS amplification?

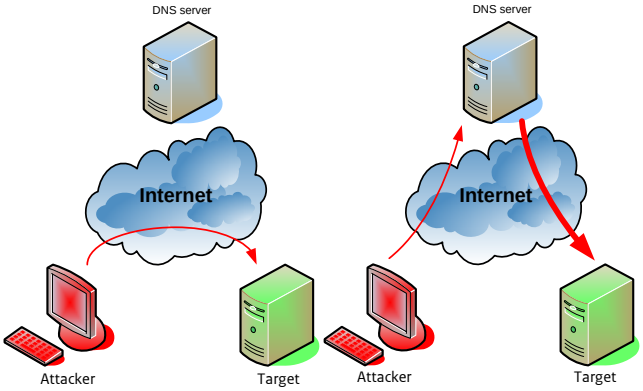
In a (D)DoS attack, the victim's system or network is (temporarily) made unavailable by overwhelming it with a large amount of data traffic.[1] In theory, an attacker could directly send such a large amount of data traffic to the victim, but this would require a huge capacity of his own network or system. The best option for the attacker is to cause maximum damage by making use of one or more third-party servers. If he goes about this in a smart way, he can reach a huge amplification of data traffic being sent to the victim. One example of such an attack is known as DNS amplification. This involves one or more 'innocent' DNS servers being used to amplify data traffic sent to the victim.

DNS stands for Domain Name System. This 'system' forms a vital part of the internet, as it converts a domain name into an IP address. If, for instance, *www.example.nl* is entered in the browser, the DNS server converts it into the IP address (e.g. 192.168.1.1) that is required to route data packets across the internet. Incidentally, DNS not only enables a person to find the IP address associated with a domain name, but also additional information. For instance, a so-called DNS query can reveal which mail servers are associated with a certain domain, or which digital signatures guarantee the domain's authenticity.

In DNS amplification attacks, attackers make smart use of the fact that a DNS response is often larger than a DNS query. Sometimes, attackers abuse the domain names that automatically send large responses, for instance, because they have DNSSEC security and they have to send digital signatures along with the response. This results in an amplification factor. Since the size of the query is small and the response may be relatively large, an amplification factor of 50 is not unusual at all. A large number of DNS servers on the internet are open to such queries without the administrators even realising it.

100 Mb/s can be amplified to 5 Gb/s If an attacker uses a botnet of 100 PCs which each have a bandwidth of 1 Mb/s, this is usually enough to take down an average company website.

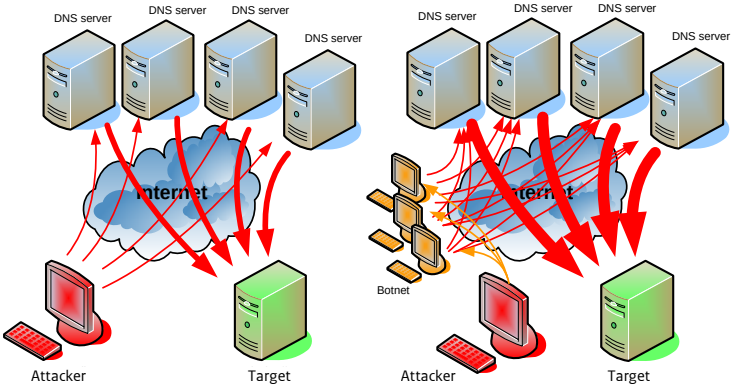
[1] For more information about (D)DoS attacks, read the Continuity of Online Services factsheet of the NCSC.



DoS attacks without (left) and with (right) amplification

In order to have the packets arrive at the victim via the DNS server, the attacker has to change the source address in the IP packets to the victim's address. This is also called IP spoofing (see text box). With IP spoofing, an attacker can send the DNS server's responses to the victim.

By sending many responses from a spoofed IP source address to one or more servers, a huge data flow is generated and sent to the victim. The result is that the victim's system, or even his network, can become overloaded. Furthermore, an attacker may use a botnet to send DNS queries to the DNS servers in order to increase the amount of data traffic sent to the victim.



DDoS attack with amplification (left) and amplification with botnet (right)

Who are the attackers?

A (D)DoS attack is often used as an attack tool by the following actors:[2]

- Hacktivists
- Criminal organisations
- State actors
- Script kiddies

In carrying out (D)DoS attacks, actors may switch between certain attack techniques, of which DNS amplification is a popular tool.

[2] More information about actors is available in other publications of the NCSC, including the Continuity of Online Services factsheet and the Cyber Security Assessment Netherlands 3.

IP spoofing

- IP packets, data packets on the internet, contain a source address where the IP packet was sent from, as well as a target address to which the IP packet is to be sent.
- In IP spoofing, an attacker forges the source address, his own IP address, with another. An attacker does this to be less traceable, or because it is an essential element of the attack.
- In DNS amplification, IP spoofing is necessary to make the DNS server think that the queries did not originate from the attacker, but from the victim. The (large) responses to the queries are targeted at the victim by the DNS server.

Depending on the attacker's intentions, the following motives may play a role:

- Monetary and/or material motives
- Ideological motives and inciting fear
- Political, state motives and/or cyber offence
- Revenge and/or retaliation
- Seeing if something works, just for fun
- Distracting, masking and/or evading[3]
- Testing botnets[4]

Who are the victims?

A (D)DoS attack with DNS amplification has two victim categories. On the one hand, there is the intended target; on the other hand, the intermediary who manages the DNS server. Both parties will experience a reduced continuity of their services due to amplified data traffic.

The intermediary does not even have to notice this taking place. After all, the attacker does not intend to disrupt the intermediary's services. In fact, the attacker has a vested interest in being able to continue uninterrupted. So, even though this party does not necessarily encounter difficulties, he is still a victim. Not only because of some material nuisance, such as increased data use and energy consumption, but also reputational risk. After all, the amplified traffic comes from the intermediary, who may be confronted about it. Being vulnerable to DNS amplification is seen as not having your infrastructure in order, and not solving the issue is seen as failing to meet your responsibility.

[3] A (D)DoS attack that is a cover-up for another operation or that ensures that an attacker can abscond from certain obligations (such as students who want to avoid taking an exam).
[4] Botnets can be rented for carrying out DDoS attacks. A botnet administrator regularly tests his 'services'.

Am I vulnerable?

Not only network administrators, but also end-users, can use certain tools to identify open DNS resolvers.

What can I do?

Is my DNS server vulnerable to misuse?

- We recommend you use one of the tools provided on the following websites:
  - http://www.openresolverproject.org/
  - http://www.thinkbroadband.com/tools/dnscheck.html
  - http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl
- Please bear in mind that these tools may wrongly indicate an open resolver. It is therefore important to have your network administrator check the results with the help of network tool NMAP.
- Please be warned that your security software may classify these checks as an attempted attack.

There are three factors that contribute to (D)DoS attacks based on DNS amplification. We have listed the associated counter-measures below.

- **Make a list of any open resolvers and close them.** An open resolver is a publicly accessible resolver, which is always ill-advised. Malevolent parties take advantage of such resolvers on a large scale. Administrators who install resolvers should be aware of this aspect, particularly if the resolvers can be reached via the internet. We recommend you only make the resolver accessible to a limited target group, for example, only your internal users. This can be easily set up in most name server software programs. If this is not possible, a firewall is the solution. Unreliable software, such as firmware of some types of routers or poorly chosen default values, often results in unintentionally open resolvers.

- **Proper monitoring of authoritative name servers.** Authoritative name servers may also be used in DNS amplification attacks. However, this can be detected with good monitoring. More and more suppliers of name servers provide so-called *Response Rate Limiting* functionality in their software (BIND, Knot and NSD).[5] This restrictive measure ensures that in certain cases, no responses (or only short responses) are given to DNS queries, resulting in a less effective DNS amplification attack. Similar, but less intelligent, restrictions may be obtained with certain firewall rules. However, this is not without risk and requires a meticulous approach. If configured incorrectly, there is a risk that legitimate data traffic will be blocked or that certain rules will not achieve their goals.

- **Block spoofed source addresses.** The crucial element of DNS amplification attacks is that malevolent parties change the source IP address in packets to their victims' IP addresses. Network administrators can prevent this from happening by configuring filters in (parts of) their networks. In professional practice, this is known as 'BCP38'. This *Best Current Practice* has been changed to RFC2827.[6] Suppliers of network equipment provide assistance in this area (sometimes called *Unicast Reverse Path Forwarding*, or uRPF). This filtering prevents attackers from spoofing source address from a network targeted at victims in other networks.

Spamhaus

The Spamhaus Project is a non-proft organisation which is responsible, among other things, for managing databases and blacklists of IP addresses and domain names which were or could be used for sending spam. E-mail providers use Spamhaus data in their spam filters to block e-mail messages from domains registered in the Spamhaus blacklists. In March 2013, the Spamhaus website was attacked with a DNS amplification attack, which would become known as the largest DDoS attack ever to take place. The attack started on 18 March 2013, during which 10 Gbps of data traffic was recorded at first, with peaks of up to 100 Gbps in the evening. After Spamhaus had hired an external supplier anti-DDoS services, the website was available again on 20 March. When the attackers realised that the supplier's measures were effective, they redirected their attack to the internet exchange points through which the supplier delivered its services and which were also used by large ISPs for their communication. This attacks was characterised by values of up to 300 Gbps and even had noticeable consequences for internet performance in several European and Asian countries. According to the supplier, some 30,000 open DNS resolvers had been used in the DDoS attack.

[5] See http://www.redbarn.org/dns/ratelimits and http://www.sidnlabs.nl/laatste-berichten/nieuwsdetail/article/nieuwe-kwetsbaarheden-in-dns-maken-dnssec-validatie-noodzakelijk/ and http://www.nlnetlabs.nl/blog/2013/09/16/rrl-slip-and-response-spoofing/ and https://lists.isc.org/pipermail/bind-users/2012-July/088220.html (rate limiting with the help of IPtables)

[6] See http://www.bcp38.info/ and http://dnssec.nl/cases/dns-amplificatie-aanvallen-straks-niet-meer-te-stoppen-zonder-bcp-38.html and http://tools.ietf.org/html/bcp38 and http://tools.ietf.org/html/rfc2827

How to proceed

1. Do not have open resolvers connected to the internet when this is not necessary or without your knowledge. Be prepared that open resolvers may come up in unexpected places.
2. Consider Response Rate Limiting (RRL) on authoritative name servers, but take into account that this is not a trivial matter with firewalls. It is better to use RRL functionality that is currently available, particularly in server software of particular suppliers (BIND, NSD, Knot).
3. Implement filters against address spoofing in your own network (BCP38).

In conclusion

The Spamhaus attack of March 2013 made it clear once again what the consequences may be of DNS amplification attacks, and how numerous the worldwide open DNS resolvers and authoritative name servers are. If owners and administrators take responsibility by protecting their network against this form of misuse, it becomes less appealing for attackers and the victims of (D)DoS attacks have one less thing to worry about.

Make sure that others are not victimised by your DNS infrastructure. Protect your network against misuse.

This is a publication of the **National Cyber Security Centre,** with the cooperation of **SIDN**, **NLNCSA** and the **Ministry of Defence**
Turfmarkt 147 | 2511 DP Den Haag
P.O. Box 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55 | F 070-322 25 37
Publication no.: FS-2013-03 1.0 | No rights may be derived from this information.