DNS Open Resolver Issues

There has been a spate of incidents in which recursive DNS servers without appropriate access restrictions implemented were used as stepping stones in DDoS attacks. Here we discuss the issues with recursive DNS servers such as these, which are known as open resolvers.

2.1 Introduction

In March 2013, it was reported that a large-scale DDoS attack had taken place*1, described as "the largest cyber attack ever." In this incident the anti-spam organization Spamhaus, as well as its host CloudFlare, were targeted in DDoS attacks that peaked at 300 Gbps*2. CloudFlare used the somewhat hyperbolic phrase that the attacks "almost broke the Internet"*3, which contributed to them gaining a lot of exposure.

The technique that was used for these attacks is called DNS amplification (DNS amp). Following the CloudFlare incident, it was announced that the Prolexic DDoS protection service was also the victim of a DNS amp attack that reached 167 Gbps*4, and it is believed that there are many other incidents that have gone unreported. IIJ's observations also demonstrate that these attacks are occurring on an almost constant basis.

In this report, we examine the issue of DNS amp attacks, as well as the open resolvers that they use as stepping stones.

2.2 DNS Amp Attacks and Open Resolvers

Most DNS transactions take place over UDP, but UDP has no protocol for session establishment like TCP. As a result, servers cannot verify when a client maliciously spoofs its IP address. This leads to responses being delivered to the spoofed IP addresses of users who did not initiate communications. These are known as reflection attacks.

DNS response packets are larger than those for queries by nature, sometimes by a factor of over 50. By combining this amplification effect with reflection attacks, attackers can saturate the target network by simply directing a small amount of attack traffic at the DNS server (reflector) that serves as a stepping stone. This is a DNS amplification attack (Figure 1). The use of a botnet enables even more efficient traffic saturation attacks.

DNS amp attacks are targeted at networks, and do not attempt to exploit specific vulnerabilities on a host. This makes them hard to counter, and because the targeted victims can only see the DNS server used as a stepping stone, they characteristically make it difficult to identify the true attacker.

Recursive DNS servers are established either for individual organizations or ISPs, and it is sufficient for them to offer functionality only to those internal users, so it is not necessary for them to serve the needs of unspecified numbers of people. Recursive DNS servers with no restrictions on unwanted external access like this are called open resolvers.

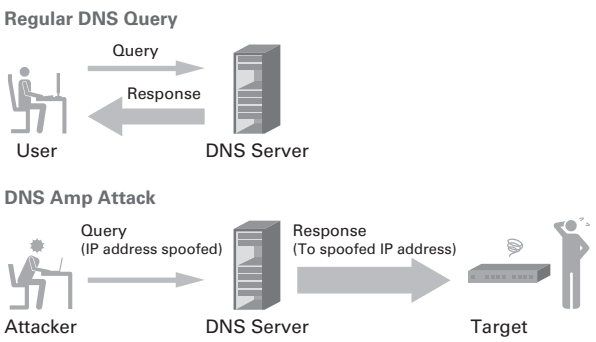


Figure 1: DNS Amp Attacks

*1 Internet Watch, "Light Shed on the 'Biggest Cyber Attack in History' that Brought the Internet to the Brink of Destruction - Open Resolver DNS Issues Requiring Urgent Attention" (http://internet.watch.impress.co.jp/docs/news/20130328_593523.html) (in Japanese). Datamation, "Massive Cyberattack Slows Down the Global Internet - A cyberfight between spam-fighters and a black-listed organization is resulting in slow download speeds for everyone." (http://www.datamation.com/news/massive-cyberattack-slows-down-the-global-internet.html), etc.

*2 http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf

*3 http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet

*4 http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html

Open resolvers respond to queries from all source IP addresses, so it is possible to exploit them freely from outside as stepping stones in DNS amp attacks. They are extremely dangerous, and there are many around the world. After the incident in March, CloudFlare announced that approximately 80,000 open resolvers had been involved (the figures show that Japan was unfortunately the top source of these in the Asia-Pacific region)*5. A survey by the Open Resolver Project stated that as many as 28 million open resolvers actually exist around the world*6, indicating that the response to this issue has been slow.

The techniques used in reflection attacks and amp attacks have been known for a long time, and it appears that an alert was issued in 1999 at the latest*7. Attacks chiefly use DNS, but this is essentially UDP, so similar attacks are possible using other UDP-based protocols such as SNMP or NTP*8. In particular, SNMP can have an amplification factor of close to 1,000*9, making it extremely hazardous.

2.3 DNS Cache Poisoning Attacks

In addition to being used as stepping stones in DNS amp attacks, open resolver recursive DNS servers are also susceptible to cache poisoning attacks.

Cache poisoning refers to attacks in which specially crafted responses are injected into recursive DNS servers to make them cache fraudulent information. For this to succeed, it is necessary to insert the forged response during a period of just a few dozen milliseconds or less before the response is returned after a recursive DNS server sends a query to an authoritative DNS server. This means that when access restrictions are properly implemented, opportunities for attack are extremely limited.

However, attackers can send triggering queries at will to recursive DNS servers with no access restrictions implemented, making it easy to control the time that forged responses are sent. As a result, users of these servers face a higher risk of receiving forged information.

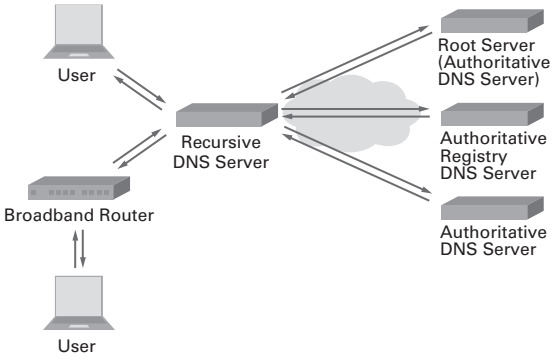
2.4 DNS Amp Stepping Stones

Reflection attacks control the target of response packets by spoofing the IP address, so anything that returns a DNS response can act as a stepping stone (Figure 2).

2.4.1 Recursive DNS Servers

These servers receive queries from clients, and perform name resolution by finding authoritative servers starting from the root server. As previously mentioned, external access should be restricted, but in reality this is not done in many cases. An example of this is servers meant to be run as authoritative DNS servers that are unintentionally operating as recursive DNS servers. Caching is enabled through an administrator's configuration error or lack of knowledge, leading to these servers often being used as stepping stones.

Additionally, because this attack method was not known in the early days of the Internet, it was not uncommon to intentionally omit access restrictions in aid of mutual



Anything that returns a DNS response can act as a stepping stone in amp attacks.

Figure 2: DNS Players

*5 Cited previously (http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf).
*6 http://openresolverproject.org/breakdown.cgi
*7 http://www.auscert.org.au/render.html?it=80
*8 An Analysis of DrDoS SNMP/NTP/CHARGEN Reflection Attacks (http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/index.html). SNMP Reflected Amplification DDoS Attack Mitigation (http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf).
*9 http://mailman.nanog.org/pipermail/nanog/2013-July/060094.html

cooperation. Circumstances today are very different from that time, but it is difficult to implement restrictions at a later date for elements that have been left open, and in some cases companies such as ISPs continue to operate without access restrictions due to their historical background.

2.4.2 Broadband Routers

Many home or commercial broadband routers have functions called DNS forwarders or DNS proxies. These are used for name resolution on home equipment, and should only need to respond to name resolution requests from the LAN side, but some products respond to WAN-side queries without restriction by default*10.

It has been identified that some broadband router products have vulnerabilities that are exploited by external parties in addition to being open resolvers, and the need to implement measures has been discussed. See our discussion of this in the previous IIR Vol.20 for more information.

2.4.3 Authoritative DNS Servers

Of the players that constitute DNS, authoritative DNS servers (content servers) assume the role of registering zone information and responding to queries from recursive DNS servers.

Recursive DNS servers and broadband router DNS forwarders respond with copies of information obtained externally, so it was easy for outside attackers to prepare information that raised the amplification factor. However, authoritative DNS servers only allow legitimate administrators to register information, making it difficult for outside attackers to orchestrate responses with a high amplification factor. For this reason, authoritative DNS servers were almost never exploited as stepping stones in DNS amp attacks up until now.

However, responses are digitally signed when DNSSEC is enabled, making responses drastically larger than unsigned counterparts. DNSSEC is a mechanism for increasing DNS security, but seen in a different light, it can also be thought of as a mechanism that creates stepping stones enabling attackers to amplify attacks with enough efficiency that they need not make any special preparations.

Authoritative DNS servers do not fall under the category of open resolvers, but incidents of their exploitation as stepping stones in DNS amp attacks are expected to increase as DNSSEC spreads in the months ahead, so urgent action must be taken.

2.5 DNS Amp Attack Countermeasures

Here we will cover a number of methods for effectively countering DNS amp attacks. This information is also summarized under RFC5358 (BCP140), so please refer to that as well*11.

2.5.1 Access Restriction

Appropriately restricting external access means unauthorized queries will be ignored even when targeted as a stepping stone in a DNS amp attack, causing the attack to fail. Restrictions can be circumvented when the IP address is spoofed to one with access permission, but even in this case there is at least no chance of being used as a stepping stone in attacks on an external party, as the response target is on the internal network.

It is also possible to protect against all fraudulent queries by implementing restrictions based on the network interface, such as only allowing queries from the LAN-side interface and ignoring those from the WAN side, as this does not rely on IP addresses. This countermeasure is particularly effective on equipment with multiple network interfaces, such as broadband routers.

2.5.2 Ingress Filtering

Reflection attacks are carried out by spoofing the IP address of the packet source, so configuring routers to deny the transfer of spoofed packets will cause attacks to fail. A number of other attack methods are known to use spoofed IP addresses, such

*10 JVN, "JVN#62507275 Multiple broadband routers may behave as open resolvers" (https://jvn.jp/en/jp/JVN62507275/). Note that caution is required, as it seems that devices other than those listed in this vulnerability report are (were) widely available for sale.

*11 RFC5358 (http://tools.ietf.org/html/rfc5358).

as TCP SYN flood attacks and Smurf attacks, and this is also an extremely effective fundamental countermeasure for all of these. This method is explained in detail in RFC2827 (BCP38)*12.

However, while it is comparatively easy to identify when an external IP address has been assigned to packets leaving an internal network, it is difficult to tell when packets flowing in from external network A have been spoofed to an IP address for network B. In other words, BCP38 is a countermeasure for preventing internal clients from carrying out fraudulent behavior due to IP address spoofing, and not a defensive measure for preventing exploitation as a stepping stone in DNS amp attacks from outside sources. Most DNS amp attacks involve involuntary and unknowing participation in attacks as a bot after infection by malware rather than the willful execution of attacks, so this countermeasure is also necessary to prevent these attacks from being launched from within a network.

If the implementation of BCP38 measures is completed on networks around the world, attacks based on IP address spoofing should in theory stop, but unfortunately implementation has not progressed much at all as of now.

2.5.3 Rate Limiting

Unlike recursive DNS servers or broadband routers, authoritative DNS servers must accept a wide range of queries from an unspecified number of recursive DNS servers, making access restrictions impossible.

Recursive DNS servers cache the responses they receive for a set period of time, and during this period they should not send the same query to an authoritative DNS server. On the basis of this thinking, the technique of deterring large numbers of responses on authoritative DNS servers by limiting the response rate per unit time (response rate limiting, or RRL) is seen as viable*13. The Afilias registry for domains such as .org or .info reports that outbound traffic that had soared as high as 2.3 Gbps when it was used as a stepping stone in amp attacks was kept down to 70 Mbps through the implementation of RRL*14.

The approach of making it harder to be exploited as a stepping stone in amp attacks through rate limiting rather than access restriction has also been taken on some DNS servers. Google Public DNS provides open resolvers to unspecified numbers of users by carrying out these measures*15.

2.6 Conclusion

While the techniques themselves behind DNS amp attacks have been known for a comparatively long time, until now adequate countermeasures have not been implemented in many cases, and essentially these attacks are left almost unchecked.

In Japan, telecommunications carriers and security organizations have been active issuing alerts and conducting surveys since the beginning of this year, but we have only just begun to look at actual measures, and it must be said that the road ahead is still steep and long.

This may seem written from the perspective of a bystander, but IIJ actually also has recursive DNS servers that are open resolvers, and we are currently in the middle of dealing with these issues ourselves*16. We are intent on correcting past oversights so we can provide a stable service.

Author:

Takanori Yamaguchi
Messaging Service Section, Product Development Department, Product Division, IIJ. Mr. Yamaguchi joined IIJ in 2006. He is engaged in the operation of mail and DNS services.

*12 RFC2827 (http://tools.ietf.org/html/rfc2827). BCP38 (http://www.bcp38.info/).
*13 http://www.redbarn.org/dns/ratelimits
*14 http://lists.redbarn.org/pipermail/ratelimits/2012-December/000144.html
*15 https://developers.google.com/speed/public-dns/docs/security#rate_limit
*16 IIJ, "Initiatives to Eradicate Open Resolvers" (http://www.iij.ad.jp/company/development/tech/activities/open_resolver/) (in Japanese). Techlog, "A request to those who used IIJ in the past - open resolver countermeasures" (http://techlog.iij.ad.jp/archives/718) (in Japanese).