Exploring DDoS amplification attack vectors prevalent in the Dutch IP range

Konstantin Dimitrov[1]
Supervisor(s): Georgios Smaragdakis[1], **Harm Griffioen**[1]

1. Background

A **Distributed Reflective Denial-of-Service (DRDoS)** is a distributed Denial-of-Service (DDoS) attack that uses publicly accessible User Datagram Protocol (UDP) servers, capable of amplification, to overwhelm the target system with UDP response traffic [1].
Amplifiers are vulnerable servers or devices that respond to requests with significantly larger responses.
IP address spoofing is the act of falsifying the source IP address of a packet.
In a **DDoS amplification attack** an attacker sends spoofed requests with the victim's IP address as the source to the amplifiers. The amplifiers then send the larger responses to the target.

Protocols that can be abused for DDoS amplification attacks include:

- **Domain Name System (DNS)** - the protocol used to translate human-readable domain names into their corresponding numerical IP addresses[2].
- **Network Time Protocol (NTP)** - used to synchronize the clocks on computer networks with very high precision.
- **Memcached** - a high-performance memory caching system, commonly used to speed up dynamic web applications.

In order to measure the amplification we use the **bandwidth amplification factor (BAF)** [3]:

$$BAF = \frac{len(UDP\ payload)\ amplifier\ to\ victim}{len(UDP\ payload)\ attacker\ to\ amplifier}$$

Application layer traffic loops are an attack primitive that can be abused to launch DoS attacks. They happen if two servers indefinitely respond to each other's messages, creating an infinite traffic loop without requiring continuous traffic from the attacker.

2. Research Question:

What are the DDoS amplification attack vectors prevalent in the Netherlands' IP range, and what are the factors that make them potent?

- *How to identify potential amplifiers in a given network?*
- *How to estimate the amplification factor for identified infrastructures amplifiers?*
- *How to perform a sensitivity analysis of amplification attack success?*

3. Methodology

1. Gathering IPs of potential amplifiers:

- **Authoritative DNS Servers** - The most popular ".nl" domains were collected. Then the IPs of authoritative servers for those domains were gathered using an NS query, which indicates which DNS server is authoritative for that domain.
- **NTP and Memcached servers** - Censys Search [4] was utilized to collect the IPs.

2. Testing for amplification:

Packets were created using the Scapy Python library [5] and were then sent to the potential amplifiers without changing the source IP. The responses were then collected and the **BAF** was calculated.
For application layer traffic loops the methodology by Pan et al. [6] was followed.
In order to not overload the potential amplifiers at no point multiple requests were sent to the same IP simultaneously.

4. Results

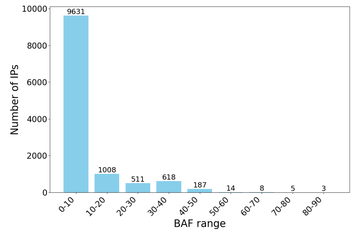

Figure 1. Distribution of BAF for DNS ANY responses.

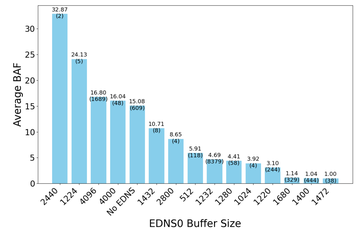

Figure 2. Average BAF for different EDNS0 buffer sizes.

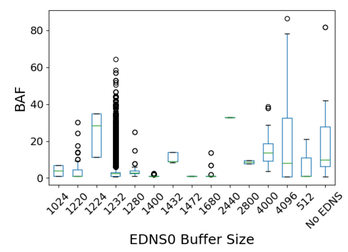

Figure 3. Box plot of BAF for different EDNS0 buffer sizes.

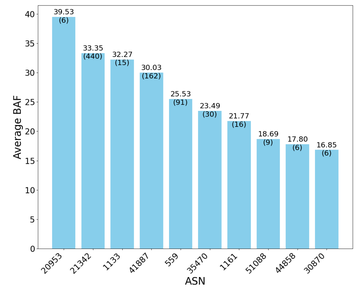

Figure 4. Autonomous systems with highest average BAF.

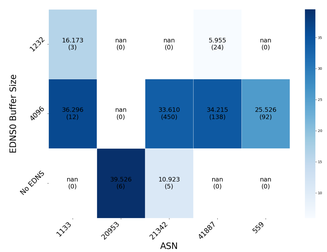

Figure 5. Autonomous systems with highest BAF and the EDNS0 buffer size their hosts use.

Memcached:

- **341** hosts in the Netherlands.
- **12** vulnerable servers.
- Highest achieved BAF of **58,509**.
- BAF of over **10,000** achieved for all servers.

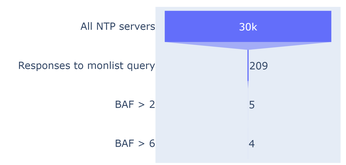

Figure 6. Distribution of NTP monlist responses.

Application layer traffic loops:

- **1** pair of vulnerable NTP servers discovered.
- No DNS, DNS-NTP, or NTP-DNS loops.

5. Findings

1. DNS:

- **Correlation between EDNS0 buffer size and BAF** of a DNS server with lower buffer relating to lower BAF.
- Most servers using the recommended EDNS0 buffer size of **1,232**.
- Differences between advertised EDNS0 buffer size and actual buffer size.
- Autonomous systems with high numbers of poorly configured servers.

2. NTP:

- Only **0.7%** of tested servers are vulnerable.
- All vulnerable servers run versions older than **4.2.7-p26**.

3. Memcached:

- Most of the vulnerable servers use version **1.4.15**.
- 1 server with manually enabled UDP.
- Differences between expected and actual BAF for servers running 1.4.15.

6. Conclusions

- Significant amplification potential for servers in the Dutch IP range.
- Widespread misconfigurations within autonomous systems.
- Older versions of NTP and Memcached create potential for very high amplification.
- Need to implement mitigation strategies to address the identified vulnerabilities.

7. Limitations

- Study limited to the Dutch IP range.
- Not a complete list of servers in the Netherlands.
- Hosts not tested for all requests that may lead to high BAF.
- DNS authoritative servers not geolocated. There could be outliers.

8. Recommendations

- Set EDNS0 buffer size of DNS servers to 1,232 and block ANY requests over UDP.
- Update NTP servers to the latest versions or manually disable the monlist command.
- Update Memcached servers to a version newer than 1.5.6 where UDP is disabled by default.

References

[1] Cybersecurity and I. S. Agency, "UDP-Based Amplification Attacks," 2019. `https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks`, Last accessed on 2024-05-08.
[2] Cloudflare, "What is DNS?," `https://www.cloudflare.com/learning/dns/what-is-dns/`, Last accessed on 2024-05-08.
[3] C. Rossow, "Amplification hell: Revisiting network protocols for ddos abuse," 01 2014.
[4] `https://search.censys.io/`.
[5] `https://scapy.net/`.
[6] Y. Pan, A. Ascheman, and C. Rossow, "Loopy Hell(ow): Infinite Traffic Loops at the Application Layer," 4 2024.
[7] Akamai, "State of the Internet Security Report (Attack Spotlight: Memcached)," 2018. `https://www.akamai.com/site/en/documents/state-of-the-internet/soti-summer-2018-attack-spotlight.pdf`, Last accessed on 2024-05-18.

[1]EEMCS, Delft University of Technology, The Netherlands
K.Dimitrov@student.tudelft.nl