Estimating the Amplification Factor in the Network Infrastructure of France

Defining factors that affect amplification DoS attacks

Author: **Panayiotis Hadjiioannou**
P.Hadjiioannou@student.tudelft.nl

Supervisor: **Harm Griffioen**
Responsible Professor: **Georgios Smaragdakis**

1. Introduction

Background

- Amplification DoS attacks aim to overwhelm target's resources making them unavailable

Gap in knowledge

- Lack of automated tools that identify vulnerable components within specific network infrastructures that could be exploited into aiding amplification attacks

Research goal

- Define parameters that affect the success and magnitude of amplification by estimating the amplification factor produced by vulnerable servers

2. Methodology

Followed the steps typically pefrormed by attackers in Amplification DoS attacks [1]:

Attacking Grounds
Protocols and parameters attackers exploit [2]
- DNS [3], NTP, Memcached, Loopy Attack [4]

Amplifier Discovery
Identified potential amplifiers in France
- Censys and IPinfo

Firing Single Packets

$$BAF = \frac{\text{len(UDP payload of response)}}{\text{len(UDP payload of request)}}$$

Analysis
- Server fingerprinting
- Testing hypothesis with tailormade experiments
- Compare results with peers

3. Results

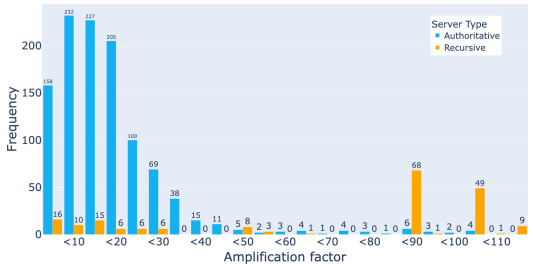

Figure 1: BAF for DNS servers queried with ANY and TXT parameters

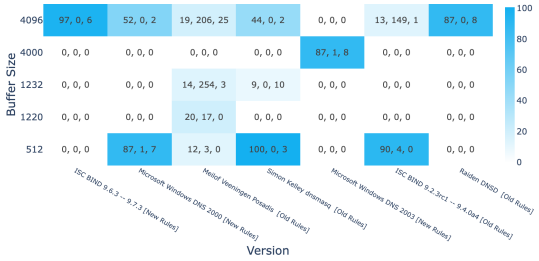

Figure 2: Median BAF per version and buffer size pairs for Authoritative and Recursive DNS servers

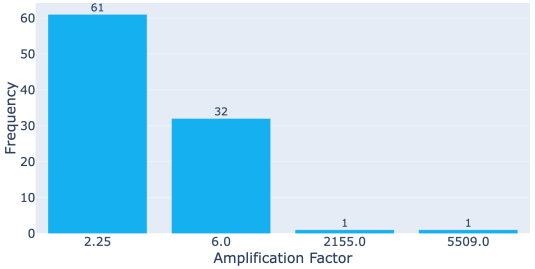

Figure 3: BAF from NTP requests with monlist command

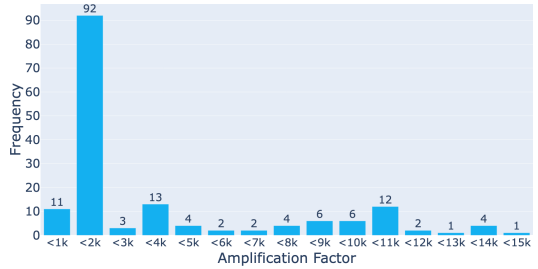

Figure 4: BAF from get key requests on Memcached servers

4. Conclusion

DNS

- Buffer size
- Authoritatitive DNS selection by recursive DNS
- Minimal ANY responses (RFC 8482)
- Type and quantity of RR set for a domain name
- Number of NS returned by recursive DNS and if they support IPv6

NTP

- Version (prior to 4.2.7)
- Number of last clients contacted the server

Loopy

- 130 potentially vulverable servers
- Majority of loops caused by NTP responses

Memcached

- Version (prior to 1.5.6)

STATS

- Value size for each statistic

Get key

- Length of the key
- Amount of data stored per key

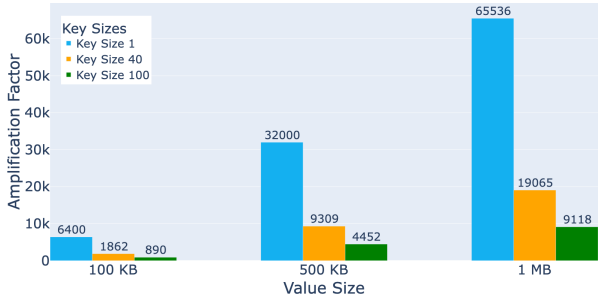

Figure 5: Theoritical BAF for different key value sizes when requesting get key for a Memcached server

5. Limitations

- Passive scanning limited the total number of collected servers
- Amplification factor of DNS servers is domain dependant
- No verification of identied loops between servers

References

[1] Harm Griffioen , Kris Oosthoek , Paul van der Knaap , Christian Doerr, "Scan, Test, Execute: Adversarial Tactics in Amplification DDoS Attacks", In ACM Conference on CCS 2021.
[2] Christian Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse", in NDSS Symposium 2014.
[3] Olivier van der Toorn, Johannes Krupp, Mattijs Jonker, Roland van Rijswijk-Deij, Christian Rossow, Anna Sperotto, "ANYway: Measuring the Amplification DDoS Potential of Domains", International Conference on CNSM 2021.
[4] Y. Pan and C. Rossow, "Loope hell(ow): Infinite traffic loops at the application layer," 2024, [Online]. Available: https://doi.org/10.60882/cispa.25470952.v1