Amplification Detection: Determining DDoS Abuse Potential of Your Network

A Quantitative Study of the Amplification Potential of Three Popular Protocols

Author: Piotr Politowicz
p.a.politowicz@student.tudelft.nl

Responsible Professor: Georgios Smaragdakis
g.smaragdakis@tudelft.nl

Supervisor: Harm Griffioen
h.j.griffioen@tudelft.nl

1. INTRODUCTION

- **Amplification DDoS attacks** reached **Tb/s bandwidth** [1] [2], enough to disrupt large networks.
- **Detection is difficult** due to the legitimate appearance of traffic and spoofed IPs. Studied protocols: DNS, NTP, Memcached.
- **Identifying parameters of large amplifiers** can aid the development of tools to detect exploitable networks before their deployment.

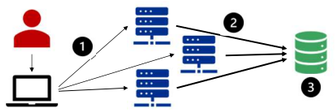

Figure 1: The concept of amplification attacks. An attacker sends spoofed requests to vulnerable amplifiers which in turn send their large responses to the victim.

1. The attacker sends requests with a spoofed IP address to amplifiers;
2. Servers unknowingly respond with large responses to the victim's spoofed IP address;
3. The victim's network gets overwhelmed with all the traffic.

2. BACKGROUND

- **An amplification attack** needs a protocol that can be weaponized and a server to reflect amplified traffic [3], causing disruption.
- **Amplification is measured** by the Bandwidth Amplification Factor (BAF). Higher BAF means more traffic can be generated.
- **Protocols that can be weaponized** use User Datagram Protocol (UDP) communication, necessary for IP spoofing, and produce large responses.
- **Domain Name System** (DNS): a simple query-response protocol that provides a naming system for resources on the internet.
- **DNS servers use buffers**, whose size is the maximum length of a response that is allowed to be sent over UDP. **The old default is 512 bytes**, but the Extension Mechanisms for DNS expanded it to **4096 bytes**. The recommendation is 1232 bytes [4] [5].
- **Network Time Protocol** (NTP): used to synchronize time between time servers and clients on the network. Supports debug requests producing large responses.
- **Memcached:** an in-memory data store. Stores arbitrary values under keys making any server communicating over UDP susceptible to amplification.

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

Figure 2: The formula used to calcluate the Bandwidth Amplification Factor.

3. RESEARCH QUESTION

How **estimating the amplification factor** and necessary **parameters for successful attacks** in Swedish network infrastractures can **improve the detection** of exploitable systems?

- How to identify potential amplifiers and estimate the amplification factor?
- What parameters affect the attack's success?
- How can identified factors detect infrastructure vulnerable to abuse?

4. CONTRIBUTIONS

- **Many DNS servers** are shown to **exceed 50, 75, and 100 BAF**, with recursive resolvers being larger amplifiers.
- **EDNS buffer size**, **DNSSEC**, and **'ANY' query** identified to influence amplifier likelihood.
- **We show query types** causing the highest amplification, with correlation to servers' **OSes and versions**.
- **NTP servers are mostly secure** against the **'monlist' attack** but provide amplification with other debug commands.

5. METHODOLOGY

- **IPs collected** from the Censys database and **domain name resolution** for DNS servers.
- Different requests per protocol sent to **trigger large responses**.
- **BAF measured** using the formula in Figure 2.

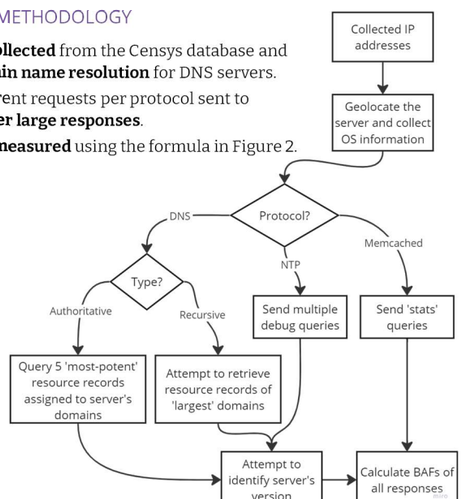

Figure 3: Simplified methodology: steps performed for each type of a server to obtain final results.

6. RESULTS

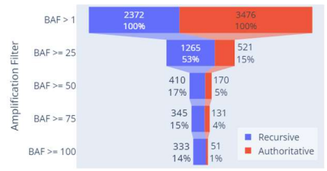

Figure 4: DNS - distribution of servers based on the BAF produced.

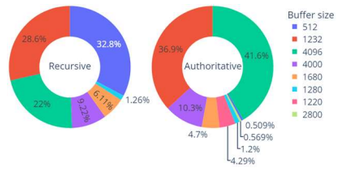

Figure 5: DNS - distribution of EDNS buffer sizes indicated by at least 10 servers

Figure 6: DNS – BAFs recorded per indicated ENDS buffer size.

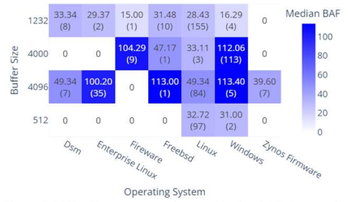

Figure 7: DNS – Heatmap showing the Median BAF of recursive resolvers across EDNS buffer sizes and operating systems.

Protocol	n	%	BAF all	BAF 50%	BAF 10%
DNS_{NS}	3,476	N/A	15.13	25.28	61.48
DNS_{OR}	2,372	5.63%	36.46	59.20	113.79
NTP	445	0.91%	95.01	173.48	772.20

Table 1: BAF per protocol. n is the number of servers with amplification larger than 1 and % represents the fraction of amplifiers compared to all active servers. all shows the average BAF of all amplifiers, 50% and 10% represent the average BAF of servers that were in the top 50% and top 10%, respectively, when compared for the largest amplification.

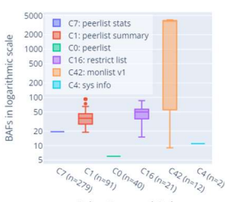

Figure 8: NTP – Recorded BAFs larger than 1 per debug command.

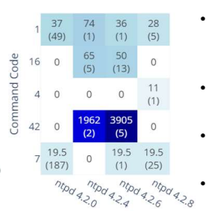

Figure 9: NTP – Heatmap showing the Median BAF across NTP versions and command codes.

- **NTP servers** provide the largest amplification; **DNS authoritative servers** are the largest group;
- **Many recursive resolvers** return all data for large domains (**BAF >= 100**);
- **The recommended 1,232-byte buffer size is common** but not most popular among DNS servers;
- **Most large amplifiers** use **4,000- and 4,096-byte** buffers;
- **Enterprise Linux and Windows OSes** found on large amplifiers;
- **'monlist' is uncommon** (12 servers) **but produces large BAF**. Other debug commands (0, 1, 7, 16) also amplify;
- **'monlist' found on NTP versions** before ntpd 4.2.7 where it was disabled by default;
- **Most amplifiers run old NTP versions** (below 4.2.8);
- **No Memcached servers** with UDP enabled found.

7. LIMITATIONS

- **Project's time constraints:** a limited number of scans;
- Scans from **one vantage point:** possibly limited view of the network;
- **DDoS prevention mechanisms are not reflected** in this study;
- **DNS servers' versions** may be **inaccurate**;
- **Not all servers** identified with a **buffer size, operating system, or version**: some results may be biased.

8. RECOMMENDATIONS

- **DNS servers' buffer size** should be set to 1,232 bytes with truncation and switching to TCP enabled;
- **DNS servers** should disable or limit the **'ANY' query**;
- **Better configuration** of recursive resolvers needed;
- **Recursive resolvers** could select authoritative servers based on **minimal responses**;
- **NTP servers** should disable **debug mode**;

9. CONCLUSION

- **This study investigated amplifiers in Sweden** and **attempted to identify parameters** responsible for their high amplification;
- **We hope to facilitate the detection** of vulnerable servers and **help correctly configure new servers** before their deployment;
- **DNS servers with 4,000 and 4,096 bytes buffers** and **cryptographic signatures** are more like to be large amplifiers;
- **Default settings of specific OSes and versions** may not represent latest recommendations;
- **NTP amplifiers may gradually decrease** as most of them run on old versions;
- **More work needed on fingerprinting servers** and **identifying vendors** who release software without complying with best practices;

REFERENCES

[1] 'Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date', ZDNET. Accessed: Jun. 19, 2024. [Online]. Available: https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/

[2] 'Famous DDoS attacks | Biggest DDoS attacks'. Accessed: Jun. 19, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

[3] C. Rossow, 'Amplification Hell: Revisiting Network Protocols for DDoS Abuse', in Proceedings 2014 Network and Distributed System Security Symposium, San Diego, CA: Internet Society, 2014. doi: 10.14722/ndss.2014.23233.

[4] P. Špaček and O. Surý, 'DNS Flag Day 2020', DNS flag day. Accessed: Jun. 12, 2024. [Online]. Available: https://www.dnsflagday.net/2020/

[5] G. C. M. Moura, M. Müller, M. Davids, M. Wullink, and C. Hesselman, 'Fragmentation, Truncation, and Timeouts: Are Large DNS Messages Falling to Bits?', in Passive and Active Measurement, vol. 12671, O. Hohlfeld, A. Lutu, and D. Levin, Eds., in Lecture Notes in Computer Science, vol. 12671. , Cham: Springer International Publishing, 2021, pp. 460–477. doi: 10.1007/978-3-030-72582-2_27.