Investigating the Amplification Potential of Common UDP-Based Protocols in DDoS Attacks across Belgium and Luxembourg

Vlad-Petru Nitu[1] (V.P.Nitu@student.tudelft.nl), Georgios Smaragdakis[1] (Responsible Professor), Harm Griffioen[1] (Supervisor)
[1]EEMCS, Delft University of Technology, The Netherlands

1. Motivation

- Most amplification attacks are based on the **UDP (User Datagram Protocol) protocol**, which are connection-less, and thus allow source address IP spoofing (modifying the source IP address as the victim's IP address) [1].
- **DNS, NTP** and **Memcached** [2]: most used protocols in amplification attack, hitting ranges of **Tbps (Terabits Per Second)** [3], [4].

2. Preliminaries

1. Protocols

- **DNS (Domain Name System)** - the "phonebook of the Internet", mapping domain names to IP addresses [5].
- **NTP (Network Time Protocol) -** widely used by computers to synchronise clocks on the Internet.
- **Memcached** protocol is a distributed memory-caching system.

2. Cyberattacks Terminology

- **Amplifier** - internet-connected server that receives a small request and answers with large response.
- **Amplification Attack** [6] – attacker spoofs the source IP address and sends a small request to the amplifier, resulting in a large volume of traffic directed back to the victim.
- **DDoS (Distributed Denial-of-Service) -** cyberattack in which the attacker disrupts a victim's machine by exhausting its resources or network in a *distributed* fashion.
- **EDNS0** - a DNS extension that allows the transfer of UDP packets larger than 512 bytes.
- **EDNS0 Buffer Size** - the maximum size of a DNS packet that a DNS resolver or server can handle using *EDNS0*.
- **DNS Flag Day 2020 [7] -** an initiative that proposed several recommendations for improving the security in DNS, such as setting the EDNS Buffer Size to 1,232.

3. Metrics

- **Bandwidth Amplification Factor (BAF)** [8]

$$BAF = \frac{len(UDP\ payload)\ amplifier\ to\ victim}{len(UDP\ payload)\ attacker\ to\ amplifier} \quad (1)$$

References

[1] Microsoft Security Blog, (2023, May 16). "Anatomy of a DDoS amplification attack". Accessed on May 15, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/05/23/anatomy-of-ddos-amplification-attacks/
[2] Cybersecurity and Infrastructure Security Agency (CISA), "UDP-Based Amplification Attacks," Jan. 2014, Accessed on May 8, 2024. [Online]. Available: https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks
[3] C. Cimpanu, "AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever," ZDNET, Jun. 22, 2020. [Online]. Accessed on May 1, 2024. [Online]. Available: https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
[4] S. Kottler, "February 28th DDOS incident report - the GitHub blog," The GitHub Blog, Mar. 01, 2018. Accessed on May 1, 2024. [Online]. https://github.blog/2018-03-01-ddos-incident-report/
[5] Cloudflare, "What is DNS? — How DNS works," Accessed on May 8, 2024. [Online]. Available: https://www.cloudflare.com/learning/dns/what-is-dns/
[6] Cloudflare, "DNS Amplification DDoS Attack", Accessed on April 23, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/
[7] "DNS Flag Day 2020," The Cloudflare Blog, May 19, 2021. Accessed on May 15, 2024. [Online]. https://blog.cloudflare.com/dns-flag-day-2020
[8] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," in Proceedings 2014 Network and Distributed System Security Symposium
[9] H. Griffioen et al., "Scan, Test, Execute: Adversarial Tactics in Amplification DDoS Attacks," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security

3. Research Questions

1. How to **identify potential amplifiers** in the networking infrastructure of Belgium (BE) and Luxembourg (LU)?
2. How to **estimate the amplification factor** for identified amplifiers?
3. Which **parameters affect the attack's success**? *Compare* observations with my research peers.

4. Contributions

1. Provide a framework to **find amplifiers** that run DNS, NTP and Memcached in the wild**.**
2. **Audit BE and LU network landscape**, estimating the BAF of vulnerable systems and identify those susceptible to application-layer loops.
3. Reflect on results and define **success factors** for attacks on these protocols [9], as well as proposing **how to mitigate** such vulnerabilities.
4. Analyse **correlation between parameters** that influence attacks.

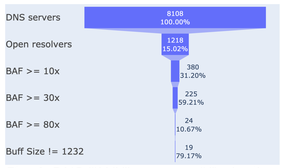

Fig. 1. DNS ("ANY" query on ".") pipeline.

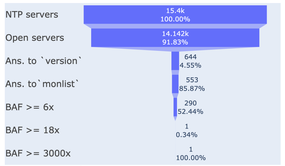

Fig. 2. NTP pipeline.

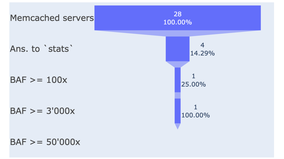

Fig. 3. Memcached pipeline.

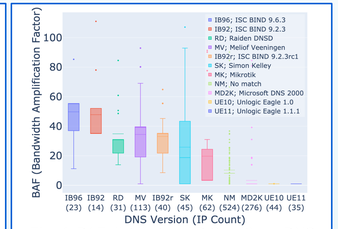

Fig. 4. BAF distribution (IP Count) per DNS Version ("ANY" on ".").

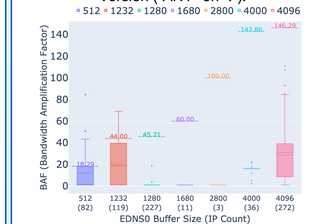

Fig. 5. BAF distribution (IP Count) per EDNS0 Buffer Size ("ANY" on "."). Threshold is the maximum BAF for a properly configured server.

5. Methodology

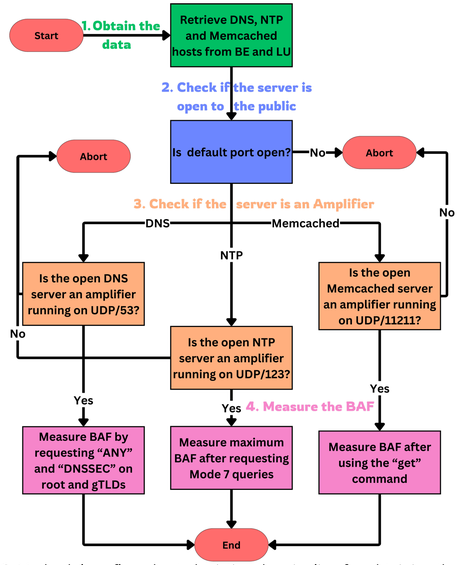

Fig. 6. Methodology flow chart, depicting the pipeline for obtaining the data, checking if a server is open, checking if the server is an amplifier, and then measuring its BAF for a specific strategy.

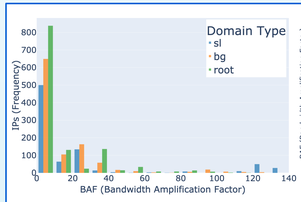

Fig. 7. BAF distribution for "ANY" queries in DNS, for domains: "sl.", "bg." and root (".").

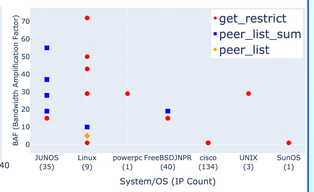

Fig. 8. BAF distribution (IP Count) per System/OS in NTP. Different Mode 7 queries are depicted with different colours and symbols.

6. Unexpected Observations

- **There are 4/119 (3.36%) DNS servers that do not properly follow the DNS Flag Day 2020 recommendation** ("lying" when advertising the buffer size: even though EDNS0 Buffer Size is set to 1,232, they still answer on UDP with messages larger than the threshold) [Fig. 5].
- **NTP servers** running the *JUNOS* and *Linux* seem the most vulnerable [Fig. 8]. We also found an NTP server running Linux achieving **3800x.**
- **We found one highly-vulnerable Memcached server** that answer on UDP/11211 [Fig. 3], even after the renowned GitHub attack [4].

7. Results

- **Unlogic Eagle DNS** servers are not vulnerable [Fig. 4].
- DNS "ANY" query resolving domain "sl." peaks at **BAF 132.09** [Fig. 7].
- There are **plenty of amplifiers in *BE* and *LU***, being *misconfigured* (DNS) or *not patched* (by running old, vulnerable versions, for NTP and Memcached).
- **DNS Version** and **EDNS0 Buffer Size** are strongly correlated factors; DNS Versions that advertise buffer sizes of 4,096 produce large BAFs.
- **Vast majority (96%) of NTP servers** are not responsive to Mode 7 (Private) queries [Fig. 2]. None of the **Cisco NTP** servers is vulnerable [Fig. 8].
- We observe 15 DNS and 33 NTP **application-level layer loops**, respectively.

8. Recommendations

- **Properly configure DNS servers**, by restricting "ANY" queries, setting EDNS0 Buffer Size to 1,232, switch to TCP if response size exceeds the buffer's size.
- **Upgrade NTP and Memcached to latest versions**. This way, Mode 7 queries (such as "monlist") will be disabled by default in NTP, and Memcached will not be exposed on the UDP port.

9. Limitations

- **Dataset** does not include all the servers in Belgium and Luxembourg (limited to Censys' and Shodan's databases).
- **A worldwide study / more extensive dataset** would be more conclusive on the patterns observed in the vulnerability of the servers.
- **Many other protocols** may be used in real amplification attacks, which were not in the scope of our research (SNMP, CharGen, etc).
- **Obtained BAFs are lower bounds**, as there may exist other query strategies that maximise the amplification factor.

10. Conclusion

- **Vulnerable DNS servers** should be manually hardened; **Vulnerable NTP** and **Memcached servers** should be upgraded to the latest versions.
- Generally, vulnerable NTP and Memcached servers **produce larger BAFs** than vulnerable DNS servers.