Estimating the Amplification Factor of Three Common Protocols in DRDoS Attacks

A Quantitative Analysis on the Weaponisation of Hosts Located in Greece

Rareș Toader[1] (R.A.Toader@student.tudelft.nl) Georgios Smaragdakis[1] (Responsible Professor) Harm Griffioen[1] (Supervisor)

[1]EEMCS, Delft University of Technology, The Netherlands

1. Introduction

- **Distributed Reflection denial-of-service attack (DRDoS)** - a malicious actor uses public servers to *reflect traffic* to a a target victim [1].

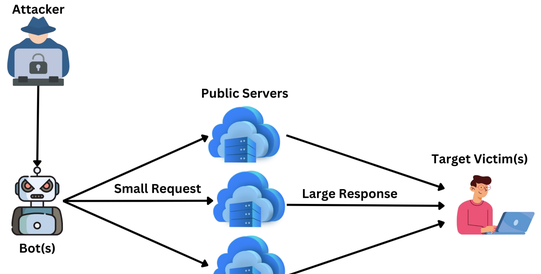

Fig. 1. Overview of a DRDoS attack.

2. Background

- **Domain Name System (DNS) -** forms the critical infrastructure that allows mapping of *domain names to IP addresses* [2].
- **EDNS0 (Extension Mechanisms for DNS)** allows for larger DNS packet sizes (≥ 512 bytes) [5].
- **Network Time Protocol (NTP) – synchronises clocks** between computers over a network [3].
- **Memcached** is a distributed memory **caching** system, primarily used to increase the **performance** of dynamic **web applications** [4].
- **BAF** - *the bandwidth amplification factor*, an important **metric** in the context of **DRDoS** attacks [1].

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

3. Research Questions

- To what extent can hosts that run **DNS**, **NTP** or **Memcached** and are located in **Greece** be weaponised in ***amplification attacks***?
- What **factors** make a server a more potent **amplification vector**?
- Are **NTP** and **DNS** hosts from Greece vulnerable to **looping attacks**?

4. Methodology

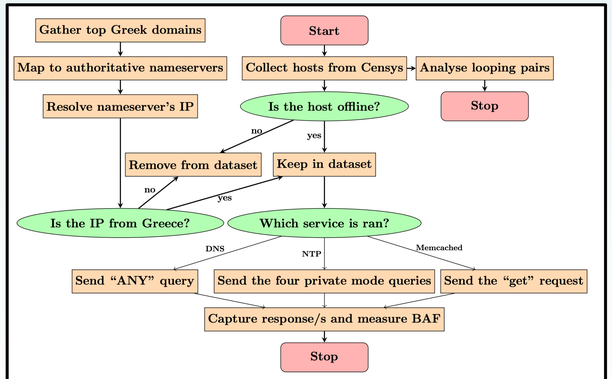

Fig. 2. Flow diagram of our experiments.

References

[1] 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. [Online]. Available: https://www.ndss-symposium.org/ndss2014/programme/ amplification-hell-revisiting-network-protocols-ddos-abuse/
[2] "What is a DNS Amplification DDoS Attack?" Cloudflare, https://www.cloudflare.com/en-gb/learning/ddos/dns-amplification-ddos-attack/.
[3] "What is an NTP Amplification DDoS Attack?" Cloudflare, https://www.cloudflare.com/en-gb/learning/ddos/ntp-amplification-ddos-attack/.
[4] "What is a Memcached DDoS Attack?" Cloudflare, https://www.cloudflare.com/en-gb/learning/ddos/memcached-ddos-attack/.
[5] J. Damas, M. Graff, and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))." RFC Editor, RFC 6891, 2013. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6891
[6] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing." RFC Editor, RFC 2827, 2000. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2827.html
[7] J. Abley, O. Gudmundsson, M. Majkowski, and E. Hunt, "Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY." RFC Editor, RFC 8482, 2019. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8482
[8] "DNS flag day 2020." DNS Flag Day, https://www.dnsflagday. net/2020/.

5.Results

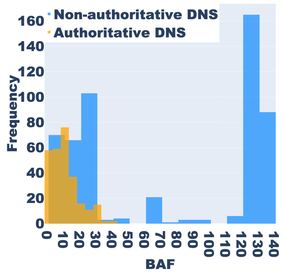

Fig. 3. Comparison of BAF (DNS).

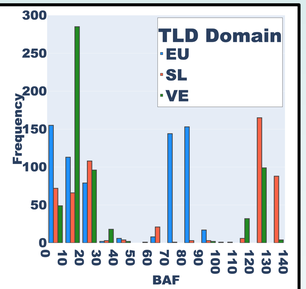

Fig. 4. BAF for DNS per domain.

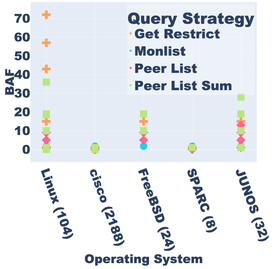

Fig. 5. BAF per OS (NTP).

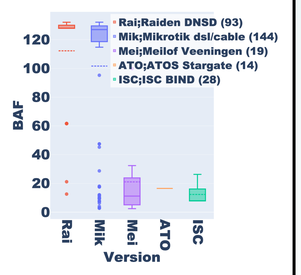

Fig. 6. BAF per DNS software.

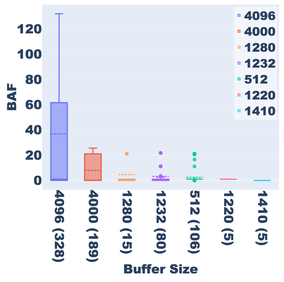

Fig. 7. BAF per buffer size.

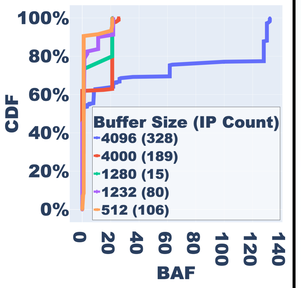

Fig. 8. CDF of BAF per buffer size.

6. Findings

- **265** *DNS servers* respond with a **BAF > 80**, leading to a cumulative BAF of 33,695.
- **Authoritative NS** – harder to weaponise (Fig. 5).
- **Domains** influence DNS amplification (Fig. 4).
- **45%** of *DNS servers* choose a value ≥ **4096** bytes for the **EDNS0 buffer size**, and **30%** of them achieve a **BAF > 100** (Fig. 8).
- **Two DNS implementations** achieve high BAFs, **70%** of the top **250** hosts run one of them (Fig. *6)*.
- **MikroTik DNS** and **Raiden DNSD** set a default value of 4,096 for the buffer size.
- **DNS** and **NTP** hosts from Greece form **7** potential loops.

7. Conclusion

- For ISPs - implement **network ingress filtering** (BCP38) [6].
- Patch **NTP** and **Memcached** hosts to secure versions.
- **Restrict** "ANY" queries (RFC8482) [7].
- Properly configure **buffer sizes** [8].

8. Limitations

- Other vulnerable protocols – **omitted**.
- Our results - ***lower bound*** of what an attacker could achieve **in the wild**.
- A **worldwide study** is *required* to confirm or contradict observed patterns.