Monitoring and Analyzing SSDP DDoS Amplification Attacks

An Empirical Study of Reflective Amplification Traffic Using Honeypots

Tim Guldenmundt | t.m.j.guldenmundt@student.tudelft.nl

Supervisor: Harm Griffioen

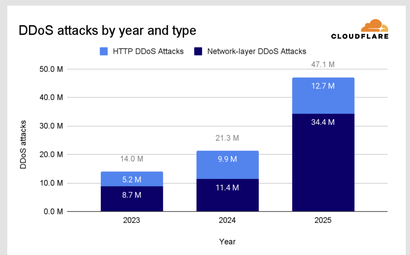
Delft University of Technology

Abstract

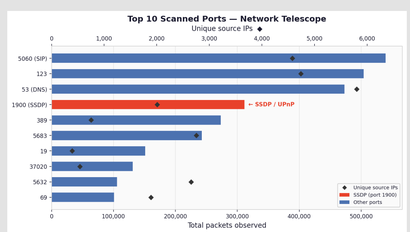
DDoS attacks are a mayor threat to modern day internet infrastructure. The Simple Service Discovery Protocol (SSDP) is among the most abused protocols for amplification attacks. This research deploys a honeypot that emulates SSDP responses, to attract real-world attack traffic. The collected data is analyzed and used to answer the following question: How is the Simple Service Discovery Protocol abused for DDOS attacks in practice by adversaries? The results give an updated view of the SSDP DDoS attacking landscape.

Introduction

Distributed Denial-of-Service (DDoS) attacks are one of the most damaging threats in networking, large attacks can take down entire network infrastructures. The scale and frequency of these attacks has been growing over the past decade. Modern DDoS attacks now regularly exceed 1TB/s in scale, with Cloudflare even reporting a DDoS attack of **31.4 TB/s** in late 2025.



A large part of these attacks is generated through so called amplification attacks. These attacks exploit publicly accessible servers to amplify their attack size. The **Simple Service Discovery Protocol (SSDP)** is one of the most abused protocols for these types of attacks. The figure below shows the most scanned ports, captured by the TU Delft network telescope. The large presence of request on port 1900 (used by SSDP) strongly suggest attackers are actively searching for misconfigured devices to use as amplification vectors.

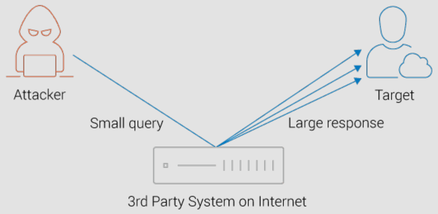


To study the strategies used by attackers in DDoS attacks abusing the SSDP, this research implements a honeypot to collect real world attack traffic in order to answer the following question: ***How is the Simple Service Discovery Protocol abused for DDOS attacks in practice by adversaries?***

Background

Amplification Attacks

In order to generate the biggest DDoS attack possible, attackers often make use of amplification attacks. Attackers send spoof the IP of the victim and send small requests to a publicly accessible server, which in turn send a much larger response back to the victim. In extreme cases this can amplify the attack by more than 100x.



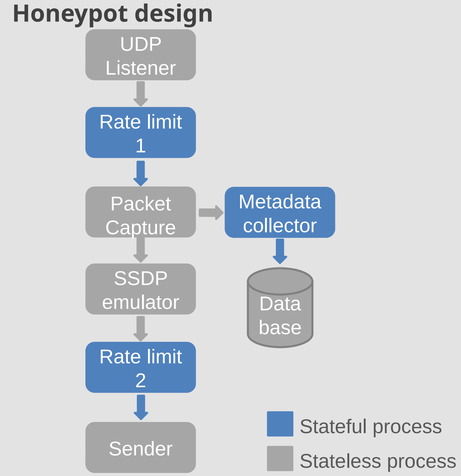
SSDP

The Simple Service Discovery Protocol is a discovery protocol used by devices to automatically discover each other on a network. Devices listen for M-SEARCH requests and respond with a description of their service. When exposed to the internet, these devices can be exploited by attackers in DDoS amplification attacks

DDoS Honeypots

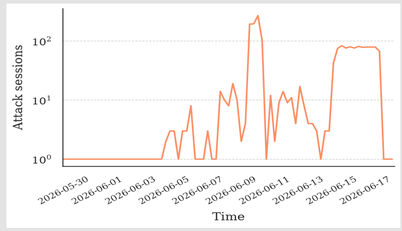
DDoS honeypots are systems that are specifically designed to emulate a vulnerable system to attract and log attack traffic. Honeypots are intentionally designed to only implement the minimum functionality to appear legitimate but not provide any real service. Almost all traffic to a honeypot can therefore be assumed to be malicious.

Honeypot design

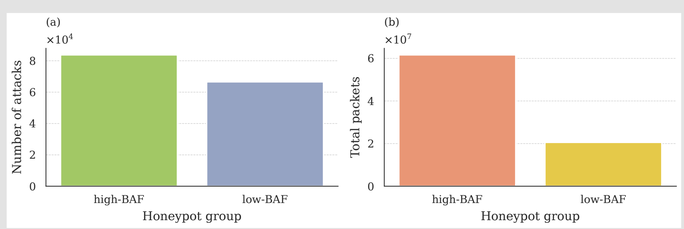


Results

The logged requests to the honeypot system are classified into attack sessions using an attack classification algorithm. In total the system received **84,532,921** requests, and detected **1,852** attacks. The graph below shows the total amount of attacks detected during the measurement period.



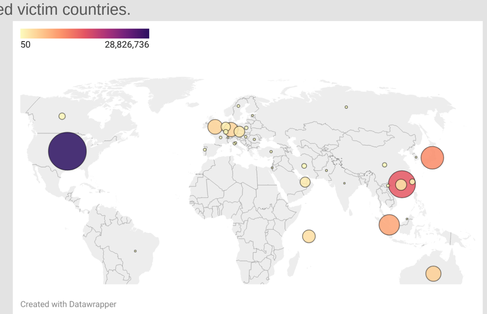
To test wether adversaries prefer devices with a higher amplification rate, the honeypot IP's were divided into two distinct groups. The low-BAF group responded with 1329 Bytes, and the high-BAF group responded with 4616 Bytes. The graph below shows the difference between these two groups in detected attack session, and total attack traffic



Furthermore, this research looked at the amount of attacks targeting more than 1 source IP within a **/24** subnet, also known as carpet bombing attacks..

Attack type	Count	Percentage
Single-source (= 1)	426	23.0%
Multi-source (> 1)	1 426	77.0%
Total	1 852	100%

Lastly, this study performs a victim analysis based on the detected attacks. Part of this analysis was taking a look at the countries of the victim IP's. Below a heat map visualizing the most targeted victim countries.



Conclusion

Based on the results from this research, several conclusions can be made:

Adversaries prefer high-amplification reflectors.

The results show that the group of IP addresses responding with a larger response are used more often by attackers during their attacks. The difference in total packets is substantially bigger than the difference in attacks. This could have two explanations:

1. Attackers use high amplification reflector more intensively in their attacks, but do not exclude the lower reflectors altogether.
2. Only the attackers responsible for the largest attacks make a selection based on amplification factors.

Carpet bombing is becoming the default strategy for SSDP DDoS attacks.

The results show that most attacks target more than one IP withing a **/24** subnet (77.0%). This is a notable increase compared to previous research, suggesting that carpet bombing is becoming the default strategy for most attacks.

Victims are concentrated in a small section of countries and industry sectors.

Within the 1,852 detected attacks, only 325 unique victims were targeted. Most of the attacks were targeted at the United States of America, which is not surprising as they own the largest share of the global network infrastructure .

Attack duration and request rate vary widely.

The attack duration and request rate measured by this research both included extreme outliers. The distribution of attack durations showed an increase in attacks around 30s, 60s, 120s and 300s. Furthermore the median request rate was found to be significantly lower that the request needed for successful DDoS attacks. This could indicate that attackers use large sets of amplifiers for their attacks.

Future work

The results of this research leave several directions open for future research. Future research could:

1. **Take a closer look at the attack classification algorithm.**
   Future research could investigate its flaws, and could try to present a better alternative.
2. **Investigate the differences between different amplification protocols.**
   The results of this study are purely based on a single amplification protocol. The results might not be consistent with other protocols.
3. **Look more closely at the effectiveness of carpet bombing strategies against current defense systems.**
   Since carpet bombing strategies seem to be the norm, understanding their effectiveness could aid in updating the current defenses.
4. **Revisit this research's questions with a longer measurement period.**
   The measurement period of 17 days from this research is relatively short, and could overlook larger patterns altogether.