On the Collateral Damage during Blackholing at Internet Exchange Points

Marcin Nawrocki, advised by Matthias Wählisch
Freie Universität Berlin, Berlin, Germany
Email: {marcin.nawrocki, m.waehlisch}@fu-berlin.de

***Abstract*—DDoS attacks are a major threat to the Internet infrastructure and end-user systems. This type of attack is currently mitigated by remotely-triggered Blackholing (RTBH), which also drops legitimate traffic, i.e., introduces collateral damage. We motivate a comprehensive characterization of RTBH events at Internet Exchange Points. Results of this research project will help to advance fine-grained filter mechanisms at the inter-domain level.**

I. Research Problem

Denial of service (DoS) attacks are a major threat to both Internet operators and end-users. A DoS attack attempts to exhaust resources of its target in order to disrupt the availability of Internet services. Typically, this is accomplished by simply flooding the target with a high volume of superfluous data packets (volumetric attack).

A common mitigation technique is remotely-triggered blackholing (RTBH). The victim domain announces the IP-prefix under attack using BGP to their direct peers by tagging the update with a well-known blackholing community. Blackholing announcements might propagate to other domains which leads to a global mitigation. Peers that receive RTBH announcements drop all traffic destined to the victims prefix. RTBH has become a popular DDoS mitigation strategy at IXPs [1]. By using the routeserver as a multiplexer, the victim sends a single RTBH announcement to reach all other IXP members.

Although RTBH is a fast, cost-efficient and effective mitigation solution, it faces a significant drawback. Since *all* traffic to the victim is dropped, the victim becomes unreachable. From a user-perspective, RTBH and a successful DDoS attack cannot be distinguished. We refer to unnecessarily dropped user traffic as collateral damage.

The goal of this thesis is to quantify collateral damage during DDoS attacks as observed by two IXPs. To the best of our knowledge, related work only offers anecdotal evidence for collateral damage. We provide a comprehensive analysis of all events for a sufficiently long measurement period.

II. Research Objectives and Methodology

A. Flow Data Sources

We propose the utilization of IXP flow data to quantify collateral damage due to RTBH. We use two IXPs as vantage points to improve visibility, a regional and a large international IXP. The data is sampled and consists of network and transport layer header information as well as parts of the application header for one of the IXPs.

B. Detecting DDoS Periods

Detecting DDoS attacks accurately is challenging. Most approaches are based on monitoring the volume of traffic in the attacked network. Internet measurements platforms such as telescopes (e.g., CAIDA) or honeypots (e.g., AmpPot) can be used to infer attacks on other networks [2].

We infer periods when a DDoS occurs by using a private data set from one of the IXPs that logs all blackholing time ranges. We assume that DDoS attacks and blackholing are closely related [3]. We further correlate this list with data from Internet measurements platforms to highlight differences, i.e., which IXP members did not activate RTBH despite a measured DDoS attack.

C. Advances of State of the Art

Results of this research project will help to advance fine-grained filter mechanisms at the inter-domain level (BGP Flowspec [4], Stellar [5] *etc.*). However, fine-grained filtering is only an useful addition if (*i*) DDoS traffic and legitimate traffic differ substantially in their features (*ii*) the fine-grained signalling and filtering mechanism is able to express such features.

In addition to the statistical evaluation of flow properties, we will describe the operational status quo of RTBH. This includes measuring RTBH frequency and reaction time to DDoS by the victim and detecting other reasons for RTBH. Furthermore, we check how many peers accept and implement the RTBH and if they do so selectively by victim or event.

Table I
FREQUENCY OF BLACKHOLING EVENTS BASED ON THE DURATION OF RTBH.

Blackhole Duration [s]	Median # Packets	# Blackholes
$0 < d \leq 10^0$	3	5
$10^0 < d \leq 10^1$	3	20
$10^1 < d \leq 10^2$	4	74
$10^2 < d \leq 10^3$	4	755
$10^3 < d \leq 10^4$	9	606
$10^4 < d \leq 10^5$	19	437
$10^5 < d \leq 10^6$	5	86
$10^6 < d \leq 10^7$	4.5	70
$10^7 < d \leq 10^8$	293.5	6

D. Practical Challenges

Measurements at IXPs for inter-domain security face some open challenges. IXPs forward very large volumes of data, hence analysing it can be expensive in terms of resources and time. Furthermore, data sampling leads to blurred results and makes a comparison across various IXPs difficult if different sampling strategies are deployed. Since we correlate data form several infrastructures with multiple devices, we have to carefully consider clock skews.

The Internet is an ever-changing network. This means, that the analysis is affected by hourly, diurnal, and even weekly traffic patterns and sudden traffic peaks. However, unusual traffic peaks are not necessarily malicious and a RTBH does not always indicate an ongoing DDoS attack.

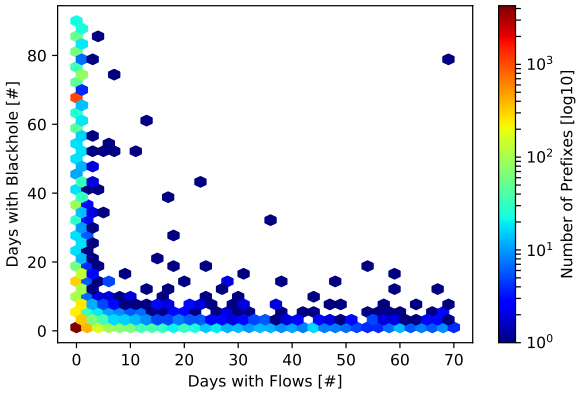
IXPs are legally bound to not release private information about their members. We will have to anonymize and aggregate our results while not limiting the significance of the results.

III. PRELIMINARY RESULTS

We present preliminary, operational results from two IXPs. We use a list of RTBH events covering 6 months from an IXP and compare this list with flow data from a second reference IXP.

We classify all RTBH events by duration. Then, we count the number of RTBH events and calculate the median number of sampled packets per event for each class. The results are shown in Table I. The majority of blackholes lasts between 10^2 and 10^5 seconds. These events are likely used as a short-term DDoS mitigation strategy. However, we also find very short-lived and always-on RTBH. Overall, there is no correlation between the blackhole duration and observed packets.

Figure 1. Number of destination prefixes with sampled traffic and active blackholes per day at the reference IXP.



In order to compare legitimate and malicious traffic patterns, we identify prefixes with traffic outside of blackholing periods. For each blackholed prefix, we count the number of distinct days on which it was blackholed and on which we sampled traffic to it (independently of RTBH). We present the results in Figure 1. The overall traffic frequency does not correlate with the blackhole usage. In particular, RTBH is uncommon for prefixes which receive daily traffic. Such prefixes probably offer widely-used services that are only protected by RTBH as a last resort. A detailed traffic analysis for these cases remains open for future work as well as an analysis including flow data from the second IXP.

REFERENCES

[1] C. Dietzel, A. Feldmann, and T. King, "Blackholing at ixps: On the effectiveness of ddos mitigation in the wild," in *International Conference on Passive and Active Network Measurement*. Springer, 2016, pp. 319–332.

[2] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, and A. Dainotti, "Millions of targets under attack: a macroscopic characterization of the dos ecosystem," in *Proceedings of the 2017 Internet Measurement Conference*. ACM, 2017, pp. 100–113.

[3] M. Jonker, A. Pras, A. Dainotti, and A. Sperotto, "A first joint look at dos attacks and bgp blackholing in the wild," in *Proceedings of the Internet Measurement Conference 2018*. ACM, 2018, pp. 457–463.

[4] N. Hinze, M. Nawrocki, M. Jonker, A. Dainotti, T. C. Schmidt, and M. Wählisch, "On the potential of bgp flowspec for ddos mitigation at two sources: Isp and ixp," in *Proceedings of the ACM SIGCOMM 2018 Conference, Posters and Demos*. ACM, 2018, pp. 57–59.

[5] C. Dietzel, G. Smaragdakis, M. Wichtlhuber, and A. Feldmann, "Stellar: Network attack mitigation using advanced blackholing," in *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*. ACM, 2018, pp. 152–164.