A First Joint Look at DoS Attacks and BGP Blackholing in the Wild

Mattij Jonker  
University of Twente  
m.jonker@utwente.nl

Aiko Pras  
University of Twente  
a.pras@utwente.nl

Alberto Dainotti  
CAIDA / UC San Diego  
alberto@caida.org

Anna Sperotto  
University of Twente  
a.sperotto@utwente.nl

ABSTRACT
BGP blackholing is an operational countermeasure that builds upon the capabilities of BGP to achieve DoS mitigation. Although empirical evidence of blackholing activities are documented in literature, a clear understanding of how blackholing is used in practice when attacks occur is still missing.

This paper presents a first joint look at DoS attacks and BGP blackholing in the wild. We do this on the basis of two complementary data sets of DoS attacks, inferred from a large network telescope and DoS honeypots, and on a data set of blackholing events. All data sets span a period of three years, thus providing a longitudinal overview of operational deployment of blackholing during DoS attacks.

CCS CONCEPTS
• Networks → Denial-of-service attacks; Network measurement; Routing protocols; • Security and privacy → Security services;

KEYWORDS
Denial-of-Service; DDoS Mitigation; BGP; Blackholing

ACM Reference Format:

1 INTRODUCTION
Volumetric Denial-of-Service (DoS) attacks have rapidly increased in frequency and intensity over the last years. In previous work, we found an average of thirty thousand attacks daily, with intensities ranging from a mere nuisance to severe [1]. Thanks to so-called Booters [2], DoS has also become available "as-a-Service", allowing the layman to launch attacks powerful enough to saturate 1-10 Gbps links. The full potential of attacks has arguably yet to be seen and Leverett et al. [3] estimate the upper bound of distributed reflection and amplification attacks to be above 100 Tbps.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

IMC ’18, October 31-November 2, 2018, Boston, MA, USA
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5619-0/18/10… $15.00
https://doi.org/10.1145/3278532.3278571
2 DATA SETS

In this paper, we consider two DoS attack events data sets and one data set of BGP blackholing events. All data sets cover the same period, from March 1, 2015 through March 5, 2018.

2.1 DoS Attack Events

The DoS data sets contain various attack types, measured by established and complementary data sources.

Randomly and Uniformly Spoofed Attacks – The first data set on DoS attacks is inferred from backscatter packets that reach the UCSD Network Telescope [13] (UCSD-NT). The UCSD-NT is a largely-unused but routed /8 network operated by University of California, San Diego. It passively collects unsolicited traffic resulting from, among others, scans, misconfigurations, and backscatter from Denial-of-Service attacks. The UCSD-NT covers approximately 1/256 of the IPv4 address space. This means that a randomly and uniformly selected IPv4 address has an approximate probability of 1/256 to fall within UCSD-NT’s address space. Randomly and uniformly spoofed attacks are often visible at the UCSD-NT as these attacks typically involve backscatter to a substantial number [1, 12] of spoofed IPv4 addresses. To infer attacks we use the classification methodology described by Moore et al. [12]. For each attack we register, among others: the attack’s target, i.e., intended victim – apparent from the backscatter packets; the attack’s (observed) beginning and end times; and a measure of attack intensity based on backscatter packet rate.1 Further details on the implementation can be found in Jonker et al. [1].

Reflection and Amplification Attacks – The second data set on DoS attacks is inferred in honeypots running AmpPot [14]. In reflection and amplification attacks, requests with a specifically spoofed source address are used to trigger reflectors to send unrequested response packets. The address is set to be that of the intended victim and the responses are typically considerably larger than the requests (i.e., there is amplification). AmpPot emulates various protocols known to be abused in this type of attack, such as NTP, DNS and CharGen [15]. During an attack, the attacker sends requests – apparently coming from the intended victim – to AmpPot. AmpPot records these requests and registers various information about each attack, such as: the target – apparent from the source address spoofed in the requests; a measure of attack intensity based on the request rate; and the attack’s (observed) beginning and end times. We use data from 24 AmpPot instances.2 It has been shown that this number of AmpPot instances is sufficient to register most reflection attacks on the Internet. Further details on AmpPot can be found in Krämer et al. [14].

The UCSD-NT data set includes spoofing attacks that directly target the victim. The AmpPot data set, differently, reports on indirect (reflected) attacks. As such, the two data sets complement each other. The data sets, however, do not cover attacks in which packets are sent without any form of source IP address spoofing. Table 1 summarizes the data sets in terms of attack events, targets and involved ASNs.

2.2 Blackholing Events

We obtain a data set of inferred blackholing events from publicly available BGP routing data, using a measurement system that we implemented on the basis of the methodology described by Giotas et al. [11].

Public BGP data – We use data from two projects that offer public BGP data: (1) University of Oregon’s RouteViews Project (RV) [16]; and (2) RIPE NCC’s Routing Information Service (RIS) [17]. Both these projects gather Internet routing data from globally dispersed collectors that peer with one or multiple routers.3

Blackholing Communities – Within the BGP data, we look for BGP announcements tagged with a community that is likely to signal a blackholing request. Giotas et al. [11] created a dictionary of such communities by applying natural language processing to resources where blackholing communities are likely to be documented (e.g., in Internet Routing Registry (IRR) records). We use a copy of this dictionary, which provides us with 288 as: value community tags, for 251 blackholing providers, using 74 distinct values (e.g., 666).4

Inferring Blackholing Events – We implemented a measurement system in Python that utilizes pyBGPStream, a Python interface to the BGPStream framework for BGP data analysis [18]. Because of our focus, we do not consider prefixes less specific than /24, since these are not commonly blackholed [11, 19]. We do infer blackholing activity incrementally, by analyzing BGP updates, and do not parse a full RIB dump at the beginning of the observation period.5 To create our data set, we analyze data from 36 BGP collectors.6 Each event in the data set contains, most notably: the blackholed prefix, a start time (i.e., activation time), an optional end time (i.e., deactivation time), a list of collectors on which prefix-related activity was observed7, and the matched communities.

Table 1: Denial-of-Service data from UCSD-NT and AmpPot for March 1, 2015 – March 5, 2018. We find 28.14 M attacks, targeting 8.58 M unique IP addresses.

<table>
<thead>
<tr>
<th>source</th>
<th>#events</th>
<th>#targets</th>
<th>#ASNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT</td>
<td>15.89 M</td>
<td>2.94 M</td>
<td>29750</td>
</tr>
<tr>
<td>AmpPot</td>
<td>12.25 M</td>
<td>6.03 M</td>
<td>28425</td>
</tr>
<tr>
<td>Combined</td>
<td>28.14 M</td>
<td>8.58 M</td>
<td>36939</td>
</tr>
<tr>
<td>Joint</td>
<td>447.6 k</td>
<td>0.18 M</td>
<td>9218</td>
</tr>
</tbody>
</table>

Table 2: Blackholing data set inferred from public BGP data for March 1, 2015 – March 5, 2018. We infer 1.3 M blackholing events, involving 146193 prefixes.
A First Joint Look at DoS Attacks and BGP Blackholing in the Wild

Table 3: Blackholed Denial-of-Service attacks. This is the first large-scale empirical observation of DoS events and corresponding blackholing mitigation: 456 k of the 28.16 M attack events in our data sets are blackholed (1.62%), which involves 0.81% of all uniquely targeted IP addresses.

<table>
<thead>
<tr>
<th>source</th>
<th>#attack events</th>
<th>#targets</th>
<th>#ASNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT</td>
<td>214.9 k (1.35%)</td>
<td>34.5 k (1.17%)</td>
<td>1732</td>
</tr>
<tr>
<td>AmpPot</td>
<td>241.0 k (1.97%)</td>
<td>47.5 k (0.79%)</td>
<td>2197</td>
</tr>
<tr>
<td>Combined</td>
<td>456.0 k (1.62%)</td>
<td>69.7 k (0.81%)</td>
<td>2543</td>
</tr>
<tr>
<td>Joint</td>
<td>18.4 k (4.12%)</td>
<td>5.7 k (3.25%)</td>
<td>800</td>
</tr>
</tbody>
</table>

Table 4: Blackholing events that follow (an observed) Denial-of-Service attack in the UCSD-NT or AmpPot data sets, as well as for attacks in either. We match 363.0 k of 1.30 M blackholing events with attacks (27.8%).

<table>
<thead>
<tr>
<th>attack source</th>
<th>#blackholing events</th>
<th>#prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT</td>
<td>159.9 k (12.3%)</td>
<td>20.6 k (14.1%)</td>
</tr>
<tr>
<td>AmpPot</td>
<td>306.4 k (23.5%)</td>
<td>33.5 k (23.0%)</td>
</tr>
<tr>
<td>Combined</td>
<td>363.0 k (27.8%)</td>
<td>45.2 k (30.9%)</td>
</tr>
</tbody>
</table>

Interestingly, for the 447.6 k attacks jointly launched against the same target (Table 1) that we observe in our DoS data sets, we find 18.4 k (4.12%) to be blackholed. This involves 3.25% (5.7 k) of unique target IPs, which, compared to 0.81%, leads us to believe that more serious attacks (i.e., those in which we observe the combination of multiple attack types) are more likely to be blackholed.

Our comparison of data sets also allows us to shed some light, for the first time, on the popularity of randomly-spoofed and reflection attacks compared to other DoS attacks (e.g., unspoofed) for which so far the research community has not been able to provide data on a global scale [1]. Table 4 shows we find 159.9 k blackholing events preceded by a randomly spoofed attack, and 306.4 k preceded by a reflection attack. This means that we match 27.8% of all 1.30 M (Table 2) blackholing events in our data set with attacks.

While, this preliminary result does not allow us to infer the fraction of different categories of attacks, it highlights that together randomly-spoofed and reflection attacks represent a significant share of the attacks that operators dealt with in the last three years.

Figure 1: Time until blackholing is activated. The distribution of the time between the start of attacks and the start of blackholing, for attacks in the UCSD-NT and AmpPot data sets. Almost half of all blackholed attacks (44.4%) see blackholing activated within a minute.

More than half of all blackholed attacks see mitigation activated within a matter of minutes. Figure 1 shows the time it takes for blackholing to be activated. For any blackholed attack in the data sets, we analyze the delay between the start of the attack and the start of the associated blackholing event. For joint

timestamps encountered in BGP announcements and withdrawals. A blackholing event can be activated through a prefix announcement with a blackholing community set, and deactivated either through re-announcement without a blackholing community set, or through a prefix withdrawal. We presume consistent propagation characteristics between announcements and withdrawals.

The 2 collectors that did not provide us with any blackholing events are RV’s KIXP and NAPAfrica. The latter was added in February 2018 and thus only overlaps with our observation period for about a month. In fact, RIPE NCC’s RIS and RouteViews know a total of 43 collectors combined at current. BGPStream indexed 41 of them while we ran our analysis, of which we considered only 36 as 4 were not active during the studied period (rcc02, rcc06, rcc08 and rcc09), and 1 is IPv6 only (route-views6).

This can occur if the event is inferred from BGP events on multiple collectors.

We will show that blackholing is often triggered well within the hour following an attack’s start time.

BGP collects, AmpPot instances, and the UCSD-NT infrastructure synchronize time through NTP. Notwithstanding, BGP timestamps are based on when the collector receives an update – not when the origin AS requested blackholing. Moreover, marginal time deviations may occur depending on where the BGP collector is in relation to the blackholing provider.
blackholed attacks – which may not see the randomly spoofed and the reflection attack start at the same time – we assume that the attack component that had started earlier in time triggered the blackholing event. To account for this assumption, we pick the longer mitigation delay for our analysis.\textsuperscript{12,13} Nearly half of blackholed attacks (44.4\%) see the blackhole activated within one minute, and 84.2\% see activation within ten minutes. Such times suggest the use of automated detection and mitigation. Only for 0.02\% of blackholed attacks it takes longer than six hours for blackholing to be activated.

![Figure 2: The distribution of the time between the end of attacks in the AmpPot data set, and the end of correlated blackholing events. In 74.8\% of blackholed reflection attacks, the blackholing is withdrawn in three hours or less after the attack stopped. In some cases, however, blackholing is left active for days after.](image)

Often blackholing mitigation lasts way beyond the attack duration. Figure 2 shows the time between the end of blackholed attacks in the AmpPot data set and the end, i.e., deactivation time, of the associated blackholing event.\textsuperscript{14} We show that for 74.8\% of blackholed attacks the blackhole is deactivated within three hours after the end of the attack. 96.1\% of blackholed attacks see deactivation within 24 hours, meaning that for 3.9\% it may take multiple days. These results suggest lack of automation in recovery from blackholing, and highlight that its side-effects (completely blocking any traffic reaching the victim) extend beyond the duration of the attack, i.e., a sort of self-inflicted DoS. Later in this section we provide some results about the potential impact of blackholing on different type of infrastructure.

We see evidence that less intense attacks are also mitigated. The UCSD-NT data set contains a measure of attack intensity (\textit{pps}_\text{max}), expressed in terms of the maximum number of backscatter packets per second observed. Figure 3 shows the overall distribution of intensities in the UCSD-NT data set, as well as for blackholed attacks only. 64.6\% of blackholed attacks (gray curve) have an intensity not greater than 100\textit{pps}_\text{max}, which corresponds to an approximate attack traffic volume of 300 Mbps.\textsuperscript{15} This applies to 91.1\% of all attacks (black curve), which confirms the intuition that attacks for which mitigation is observed are likely to be stronger.\textsuperscript{16} More importantly, a non-negligible percentage of blackholed attacks have low intensity. Specifically, 13.1\% see an intensity of at most 1ppsmax (3 Mbps). First, this result shows that operators mitigate – with such an extreme measure as blackholing – even less intense randomly spoofed attacks; which raises the question of what is the minimal effort needed by an attacker in order to induce the victim to recur to “shut down” an IP address for a certain period of time. In addition, this is the first time we are able to confirm (on a large scale) that even the smallest attack intensities inferred through a methodology based on indirect and partial observation of DoS phenomena but largely used in literature (Moore et al.\textsuperscript{[12]}) are relevant, since they trigger mitigation. Finally, this result underpins the validity of the surprisingly large number of DoS attacks we discovered in a recent work\textsuperscript{[1]}, contributing to the bigger picture, and it provides a reference threshold to be used in the context of monitoring and situational awareness.

The analysis of blackholed reflection attacks yields similar results. The AmpPot data set contains an intensity measure (\textit{rps}_\text{avg}), expressed in terms of the average number of requests per second, e.g., DNS queries.\textsuperscript{17} The top five reflector protocols in the AmpPot data are: (1) NTP \textapprox{} 40.7\%, (2) DNS \textapprox{} 25.6\%, (3) CharGen \textapprox{} 22.6\%, (4) SSDP \textapprox{} 8.3\%, and (5) RIPv1 \textapprox{} 2.6\%. We consider only these protocols and note that they are used in all but 0.2\% of AmpPot attacks. Figure 4 shows the intensity per protocol for the top five reflection attack protocols for all AmpPot attacks as well as for those that are blackholed ((1) NTP \textapprox{} 45.0\%, (2) DNS \textapprox{} 33.9\%, (3) CharGen \textapprox{} 11.2\%, (4) SSDP \textapprox{} 7.5\%, and (5) RIPv1 \textapprox{} 2.1\%). We here too show that operators also mitigate less intense reflection attacks (e.g., 4.9 ppsavg for fewer than 50\% of blackholed SSDP-based reflection attacks). We also confirm the intuition that mitigated attacks are likely to be stronger\textsuperscript{18}.

\textsuperscript{11}In doing so we favor the risk of introducing “longer-than-actual” over “shorter-than-actual” times when estimating the delay with which blackholing starts. In other words, we pick an upper bound for the mitigation delay. It should be noted that we can only do this for joint attacks that we recognize as such, meaning that we cannot account for attack components that we do not observe (Section 2.1). However, based on our observations of randomly spoofed attacks and reflection attacks, joint attacks are relatively rare.

\textsuperscript{12}We analyzed the start time differences between attack components of the 18.4k joint blackholed attacks in our data (Table 3) and find that 85.54\% see the attack start spaced less than 40 minutes apart.

\textsuperscript{13}Blackholing ‘truncates’ the attack end times in UCSD-NT data, which is why we do not analyze deactivation delays for randomly spoofed attacks.

\textsuperscript{14}We assume 1500-byte packets and account for UCSD-NT’s 1/256 address space coverage, i.e., observing 1 backscatter packet for every 256 uniformly spoofed packets.

\textsuperscript{15}In previous work we showed that stronger attacks lead to quicker outsourcing to DDoS Protection Services – another form of mitigation\textsuperscript{[1]}.\textsuperscript{16} Wepon honeypots are part of a larger set of amplifiers. The attack intensity depends on all amplifiers involved, and honeypots cannot know the extent of involvement. By a best-effort guess, the number of amplifiers will not vary significantly among attacks for the same reflection protocol\textsuperscript{[5]}. We thus consider the intensity per protocol.
on average. Specifically, between all AmpPot attacks and those blackholed, the median rates for SSDP, DNS and CharGen increase with 0.8, 6.6 and 11.5 $rps_{avg}$ respectively. RIPv1 and NTP reflection see stronger increases, by 55.5 and 329.9 $rps_{avg}$, respectively.

Given that attacks of various intensities can be launched jointly against the same target, one could hypothesize that a less intense attack will only be mitigated by a target – with such an extreme measure as blackholing – if it is joined by a high-intensity attack. We analyzed the intensity components in the 18.4k joint blackholed attacks in our data (Table 3). 9.82% of the joint randomly spoofed attacks have an intensity in the 25-th percentile (which corresponds to an intensity of up to 2.55 $rps_{max}$). About a fifth of these attacks, 20.54%, were joined with a reflection attack that falls in the 12.5-th percentile of its respective, i.e., protocol-specific intensity distribution (e.g., up to 13.2 $rps_{avg}$ for NTP). 40.71%, 68.39% and 86.79% of the aforementioned randomly spoofed attacks were joined with reflection attacks that have an intensity in, respectively, the 25-th, 50-th or 75-th percentile. The presence of low-intensity combinations in joint blackholed attacks corroborates that less intense attacks are also mitigated with blackholing.

The blackholing communities we observe reflect actual traffic filtering. Figure 5 shows the duration distributions of all attacks and of blackholed attacks, for the AmpPot data as well as the UCSD-NT data. For reflection attacks (upper plot), the duration of attacks goes up for those for which we observe blackholing, with 41.6% of blackholed attacks lasting ten minutes or longer, against 29.2% for all attacks. This confirms the intuition that mitigated attacks are more substantial also in terms of duration. For randomly spoofed attacks, however, 64.5% of blackholed attacks last ten minutes or shorter, against 55.5% of all attacks (lower plot). The duration thus decreases. This might seem counter-intuitive at first, but we note that an effective blackhole will drop all target-destined traffic, including the packets that trigger backscatter. Consequently, the attack end time observed through backscatter may not reflect the actual time at which the attack stopped. In fact, none of the blackholed attacks last longer than 3.2h in our data. On the other hand, the end time observed in a reflector honeypot does not necessarily change as the result of effective mitigation, because the honeypot can still receive spoofed requests, even in the event where the victim no longer receives any traffic. The asymmetric increase and decrease in duration thus confirms that the BGP communities we observe reflect actual blackholing activity.

Loss of service may affect Web sites, mail exchangers and name servers. We observe a total of 228.1M Web sites for March 1, 2015 – March 5, 2018 (1100 days), and 38.76M and 7.62M unique mail exchanger and name server names for January 22, 2017 – March 5, 2018 (407 days).

The blackholing communities we observe reflect actual traffic filtering. Figure 5 shows the duration distributions of all attacks and of blackholed attacks, for the AmpPot data as well as the UCSD-NT data. For reflection attacks (upper plot), the duration of attacks goes up for those for which we observe blackholing, with 41.6% of blackholed attacks lasting ten minutes or longer, against 29.2% for all attacks. This confirms the intuition that mitigated attacks are more substantial also in terms of duration. For randomly spoofed attacks, however, 64.5% of blackholed attacks last ten minutes or shorter, against 55.5% of all attacks (lower plot). The duration thus decreases. This might seem counter-intuitive at first, but we note that an effective blackhole will drop all target-destined traffic, including the packets that trigger backscatter. Consequently, the attack end time observed through backscatter may not reflect the actual time at which the attack stopped. In fact, none of the blackholed attacks last longer than 3.2h in our data. On the other hand, the end time observed in a reflector honeypot does not necessarily change as the result of effective mitigation, because the honeypot can still receive spoofed requests, even in the event where the victim no longer receives any traffic. The asymmetric increase and decrease in duration thus confirms that the BGP communities we observe reflect actual blackholing activity.

Loss of service may affect Web sites, mail exchangers and name servers. We observe a total of 228.1M Web sites for March 1, 2015 – March 5, 2018 (1100 days), and 38.76M and 7.62M unique mail exchanger and name server names for January 22, 2017 – March 5, 2018 (407 days).
 temporary loss of use of the victim IP address, in some cases even beyond the attack duration, we explore the impact blackholing may have on the availability of services by considering data from OpenINTEL. OpenINTEL is an active DNS measurements platform [20] that measures daily snapshots of the DNS by querying all domain names under Top-Level Domains (TLDs) for their Resource Records (RRs). This includes IP addresses of: (i) www labels, (ii) mail exchanger (MX), and (iii) authoritative name servers (NS). We use these records to map Web sites, mail and name servers to blackholing events.

We use data for the three generic TLDs: .com, .net, and .org, which cover 50% of the global namespace [21]. Table 5 summarizes the data. We note that the Web site data spans the full DoS and blackholing data sets, but MX and NS data is shorter as the functionality to resolve these records was added to OpenINTEL later (on January 22, 2017).

Table 6 summarizes the blackholing correlation. 754k Web sites map to blackholing (0.33% of 228.1M). Of unique MX and NS names, 154k (0.40% of 38.76M) and 9994 (0.13% of 7.62M) map to blackholed prefixes.

Infrastructure can be redundantly hosted, i.e., have multiple IP addresses. We investigate this by studying the presence of non-blackholed IP address records and find that, respectively, 87.4%, 98.0% and 98.6% of the names found (cf, ratio in Table 6) do not have an alternative IP address at the time of blackholing. It follows that these services may become – and remain for extended time – unavailable when blackholing is left active and no IP address change takes place. We note that Mail Transfer Agents (MTAs) typically try to resend mails for days, meaning that an unreachable mail exchanger may incur a (hefty) delay rather than a full loss of service. When name servers cannot be reached, the domain names for which they are authoritative may become unreachable – something also influenced by DNS redundancy and caching mechanisms (e.g., TTL settings). A thorough characterization of loss of service requires extensive additional measurement – some to be performed on-the-fly while the event is happening, which we started instrumenting and leave as future work.

4 RELATED WORK

Several approaches to DoS mitigation have been proposed in literature [22, 23]. However, it is only with the analysis in Jonker et al. [4] that a first characterization of the adoption of DoS mitigation solutions was measured at scale. Giottas et al. [11] present a comprehensive characterization of BGP blackholing activity, based on BGP data. Dietzel et al. [24] and Chatzis et al. [25] emphasize that IXP’s play a key role in deploying blackholing. Our contribution focuses instead on correlating DoS attacks and blackholing events.

DoS attacks have been the subject of detailed studies [26]. A large-scale, measurement-based characterization of DoS attacks at the macroscopic scale is only given, however, in Jonker et al. [1], with an analysis of reflection and randomly spoofed attacks over a two-year period. The paper also retraces the major steps in DoS analysis, from the seminal paper by Moore et al. [12]. DoS characterization has been carried on based on diverse data sources. While the work in Moore et al. focuses on the analysis of backscatter, Krämer et al. [14] and Thomas et al. [27] focus on DoS attacks as seen from a set of amplification honeypots. Santanna et al. [2] and Krupp et al. [28] analyze DoS attacks generated by Booters, while Wang et al. [29] analyze Botnet-related attacks. The focus of this paper is not on DoS attacks per se, but on the relation between DoS attacks and blackholing.

5 CONCLUSIONS

This study compares, on a global scale, DoS attacks with BGP blackholing events, revealing insights about the operational deployment of blackholing as a DoS mitigation strategy. Based on our analysis, we argue that BGP blackholing defense mechanisms can react extremely fast, thus appear to be highly effective at protecting the network involved. However, some blackholing events last far longer than the duration of the related attack, thus being very hard on the services and systems involved. Our preliminary results also highlight that, to further understand the impact of blackholing, more data is needed, e.g., on-the-fly DNS measurements triggered once a blackhole is announced. Such measurements will shed light on aspects such as which networks are fully taken offline by a blackhole and which services benefit from blackholing but subsequently migrate to a different IP address to ensure service continuity. Finally, this study contributes to a better understanding of the whole DoS ecosystem: (i) it validates and reinforces some findings from our previous work [1], and (ii) it adds other pieces to the puzzle of the bigger picture of DoS attacks (attacks, defenses, impact, etc.).

ACKNOWLEDGMENTS

This work is part of the NWO: D3 project, which is funded by the Netherlands Organization for Scientific Research (628.001.018). This research was made possible by OpenINTEL, a joint project of the University of Twente, SURFnet, and SIDN. This material is based on research sponsored by Air Force Research Laboratory under agreement number FA8750-18-2-0049. This work used the Extreme Science and Engineering Discovery Environment (XSEDE), which is supported by National Science Foundation grant number ACI-1053575. This work was supported by National Science Foundation grant CNS-1730661. We are grateful to Christian Rossow and Johannes Krupp for sharing AmpPoT data. We thank our shepherd and the anonymous reviewers for their valuable feedback.

The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.
REFERENCES


