DDoS Mitigation: A Measurement-Based Approach

Mattijs Jonker, Anna Sperotto, and Aiko Pras
University of Twente, Enschede, The Netherlands

***Abstract*—Society heavily relies upon the Internet for global communications. Simultaneously, Internet stability and reliability are continuously subject to deliberate threats. These threats include (Distributed) Denial-of-Service (DDoS) attacks, which can potentially be devastating. As a result of DDoS, businesses lose hundreds of millions of dollars annually. Moreover, when it comes to vital infrastructure, national safety and even lives could be at stake. Effective defenses are therefore an absolute necessity. Prospective users of readily available mitigation solutions find themselves having many shapes and sizes to choose from, the right fit of which may, however, not always be apparent. In addition, the deployment and operation of mitigation solutions may come with hidden hazards that need to be better understood. Policy makers and governments also find themselves facing questions concerning what needs to be done to promote cybersafety on a national level. Developing an optimal course of action to deal with DDoS, therefore, also brings about societal challenges. Even though the DDoS problem is by no means new, the scale of the problem is still unclear. We do not know exactly what it is we are defending against and getting a better understanding of attacks is essential to addressing the problem head-on. To advance situational awareness, many technical and societal challenges need still to be tackled. Given the central importance of better understanding the DDoS problem to improve overall Internet security, the thesis that we summarize in this paper has three main contributions. First, we rigorously characterize attacks and attacked targets at scale. Second, we advance knowledge about the Internet-wide adoption, deployment and operational use of various mitigation solutions. Finally, we investigate hidden hazards that can render mitigation solutions altogether ineffective.**

***Index Terms*—Denial-of-Service, DDoS, attacks, mitigation, Internet measurement**

I. Introduction

Our primary communications fabric is under siege. The evolution of the Internet has had a revolutionary impact on modern society. What started as a technology to interconnect educational institutes, research centers and alike has – over the past three decades or so – taken over global communications. The Internet has become an integral part of modern society, tying into, among others, commerce, technology and entertainment. As we have a dependency on the Internet for communication, its availability – taken for granted by many – is of vital importance. Although critical components of the Internet were originally designed with resilience in mind, the stability and reliability of the Internet are nowadays continuously subject to deliberate threats, including devastating DDoS attacks. A rigorous characterization of the DDoS phenomenon, and of countermeasures to mitigate the associated risks, is missing and faces many analytic challenges. The thesis addresses precisely this open issue, by taking a measurement-based approach to characterizing attacks and mitigation solutions. Our work advances situational awareness and demonstrates our ability to inform Internet research, network operations and policy makers about the growing DDoS threat.

978-1-7281-4973-8/20/$31.00

A. DDoS Attacks

Over the past decades, DDoS attacks have rapidly increased in terms of occurrence and intensity, steadily becoming one of the largest threats to the stability and reliability of the Internet.

As the name suggests, Denial-of-Service attacks are used by attackers to achieve denial of service. In essence, this entails cutting a networked service off a network, i.e., the Internet, by any means possible. The motivations of attackers can vary wildly, including – but certainly not limited to – creating a distraction from other malicious activity (e.g., masking data theft [1], [2]), hacktivism (e.g., politically motivated attacks) [3], [4], or cyber-extortion (e.g., threatening banks to take down e-banking applications unless a ransom is paid) [5].

Successful attacks can have ripple effects, create cascading failure, and potentially have an immense impact on the Internet [6]. Self-evidently, in the face of the DDoS threat, effective defenses are an absolute necessity.

B. Mitigation Solutions

The upsurge of the DDoS problem has prompted the development of diverse mitigation solutions and has led to a booming market for commercial products. Generally speaking, on the one hand, defending against attacks is better done closer to the source, before attack traffic converges and starts doing harm. On the other hand, detection is generally better done closer to the target, where harm is done. Because of this, various proven solutions are inter-domain, meaning that telemetry information for detection as well as reactive control measures for mitigation are exchanged across organizational boundaries. Quantitative knowledge of the adoption of mitigation solutions on the Internet is limited. In addition, an understanding of how they are deployed and operated when operators are faced with attacks is missing.

C. Hidden Hazards

Even though mitigation solutions are readily available, there is a potential disconnect between the ease of setup and the expertise of users. Solution providers stand to benefit from offering a low adoption barrier. Often they try to capitalize rapid product (or service) deployment, because that is what is needed in times of crisis (i.e., when attacked). But what are the potential pitfalls that users others than seasoned network operators and security engineers face when using certain

mitigation technologies? Are there hidden hazards that can render solutions ineffective?

D. Challenges

There are many challenges when it comes to DDoS mitigation, including but not limited to: *(i)* challenges in knowing exactly what it is we are defending against; and *(ii)* challenges relating to the adoption and operation of mitigation solutions. The thesis shows from its outset that a basic challenge that we are faced with concerns data. Acquiring and developing diverse (raw) data sources to methodologically study the DDoS problem constitutes a challenge in itself. We contribute significantly towards overcoming these challenges.

E. Approach

The approach we take is measurement-based. We use large-scale passive and active measurements from diverse vantage points all over the world, to gather a variety of independent data types. Given the challenge of processing such data, we fuse, derive, and analyze data sets by applying Big Data Analytics. In the process, we identify and verify, where applicable, pre-existing methodologies to measure, and devise new measurement methodologies along the way where necessary.

F. Contributions

By successfully fusing data we: *(i)* unveil eye-opening statistics about global attack activity; *(ii)* gain insights into the Internet-wide adoption of mitigation solutions as well as operational practices of users; and *(iii)* lay bare and investigate the undesirable side effect of mistakes in deployment and operation. In addition, we further validate existing methodologies (i.e., our work complements previous validation efforts), and make some of our data available to the research community.

In terms of knowing what we are defending against, we present a large-scale characterization of attacks. We reveal the massive scale of the DDoS problem. Our characterization accounts for nearly *21* million attacks and we show, among others, that one-third of all `/24` networks estimated to be active on the Internet have suffered at least one attack during a recent, two-year observation period. We also advance our understanding of the adoption and operation of mitigation solutions. We focus on two inter-domain solutions in particular, cloud-based protection services and BGP blackholing, and reveal global trends in adoption as well as operational practices. Finally, our work underpins that mistakes are made in deployment and operation, which arguably leave some operators and users with a false sense of security. Our work also corroborates the notion that attackers can seize on such mistakes as an opportunity to bypass defenses.

G. Organization

The rest of this paper is organized as follows. In § II we outline the primary data sources that we identified, developed, and used. We present our characterization of attacks in § II-A. In § IV we shift our attention to mitigation solutions. Next, in § V, we present our analysis of hidden hazards concerning these solutions. Finally, we summarize our work in § VI.

II. Data Sources

A. Data on (D)DoS Activity

We identified two distinct data sources that provide global indicators of (D)DoS activity. First, the UCSD Network Telescope (UCSD-NT), which captures evidence of DoS attacks that involve randomly and uniformly spoofed IP addresses. And second, AmpPot honeypots, which capture reflection and amplification DoS attacks – an attack type that involves specifically spoofed IP addresses.

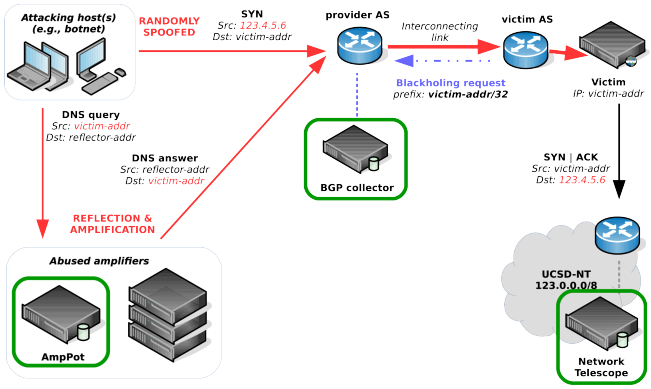

Fig. 1. A bird's-eye view on the measurement systems' placement for three of our data sources. Specifically, attacks data and blackholing observation.

Randomly Spoofed Attacks The UCSD-NT is a largely-unused yet routed `/8` network operated by the University of California, San Diego. [7] Network telescopes, i.e., darknets, passively collect unsolicited traffic – resulting from scans, misconfigurations, bugs, and backscatter from Denial-of-Service attacks, etc. – sent to routed regions of the address space that do not contain any hosts.

Figure 1 shows (follow the red lines atop) how network telescopes pick up (D)DoS backscatter. The example attack shown is a `TCP SYN` flood attack, which involves the first packet type from a three-way TCP handshake. The source IP address in these packets is set to a randomly spoofed IP address by the attacker. The victim may, provided that its link is not (yet) saturated by the attack, upon receipt of a `SYN` packet, answer with a handshake response, i.e., a `SYN|ACK`. If the spoofed address is within the network telescope's address space, the response packet will be sent to the telescope (rather than to the actual source of the attack packet), where the packet can be collected and analyzed.

We implemented the detection and classification methodology described by Moore et al. [8] to identify randomly spoofed attacks in the UCSD-NT data. We describe this process and the data source in more detail in our IMC 2017 paper [9].

The UCSD-NT covers approximately *1/256* of the IPv4 address space. This means that any sizable attack, i.e., one that involves many packets with randomly and uniformly spoofed IP addresses, is likely to be visible on this darknet.

Reflection and Amplification Attacks Our second data source on attacks is provided by the AmpPot project. This

novel and open-source honeypot aims to track reflection and amplification attacks by mimicking reflectors. To be appealing to attackers, AmpPot emulates several protocols known to be abused in reflection attacks. This way, AmpPot can be found by attackers scanning for reflectors and be "abused" in subsequent attacks, which can be inferred and logged.

Figure 1 also shows (follow the red line down) how AmpPot is positioned to log attempts at reflection. In this particular example, a forged DNS query is sent to the honeypot, enabling it to infer the reflection attack. We refer the reader to the paper by Krämer et al. for more information on AmpPot [10].

Both attack data sources provide target IP addresses, which can be augmented with metadata to study target characteristics. We use *NetAcuity Edge Premium Edition* data [11] to add geolocation information. And we use *Routeviews Prefix-to-AS mappings* data [12] to add BPG routing metadata.

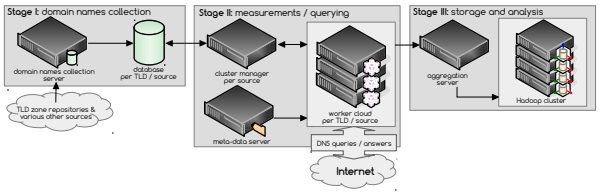

Fig. 2. The OpenINTEL measurement and analysis architecture.

DNS Measurement Data The UCSD-NT and AmpPot data sets contain targeted IP addresses. To evaluate the potential impact of attacks using Web sites as a measure we need a historical mapping between IP addresses and Web sites. To obtain this mapping we use active DNS measurement data from the OpenINTEL project, which is a large-scale, active DNS measurement platform that collects daily snapshots of the content of the DNS [13]. It builds snapshots by structurally querying all the domain names under a full zone, i.e., Top-Level Domain (TLD), for a set of Resource Records (RRs). OpenINTEL covers a large number of TLDs. The resulting measurement data notably include domain name to IP address mappings (i.e., `A` records).

We are among the OpenINTEL founders and have been actively involved in its develoment and operation from the get-go. Unsurprisingly, we use OpenINTEL data for other purposes too (more on this later). We also rely on the OpenINTEL architecture to fuse and analyse diverse data.

Figure 2 shows a glimpse of the architecture. Stage I is for zone (i.e., TLD) collection. Stage II relates to daily measurements. And stage III relates to data storage and analysis.

Inferring the Use of Protection Services The use of DDoS Protection Services (DPS) involves using the DNS or BGP to divert network traffic. OpenINTEL measures the DNS records on which various DNS-based diversion mechanisms rely. This allows us to devise a methodology to infer DNS-based diversion from OpenINTEL data. In particular, we infer DPS use from `A`, `CNAME` and `NS` records. To infer BGP-based network traffic diversion, we consider BGP routing information. To this end we supplement IP address records in OpenINTEL data with autonomous system numbers. We do this analogously to how we augmented attack target IP addresses in UCSD-NT and AmpPot attacks data. The full details of our methodology are described in our IMC 2016 paper [14]. Take note that protection services can be used in an *always-on* or *on-demand* fashion.

Inferred Use of BGP Blackholing We infer BGP blackholing events from publicly available BGP routing data, using a custom, extensible measurement system, implemented on the basis of the methodology described by Giotsas et al. [15]. We use data from two projects: *(i)* University of Oregon's *RouteViews Project (RV)*; and *(ii)* RIPE NCC's *Routing Information Service (RIS)*. Within the BGP data, we look for BGP announcements tagged with a community that is likely to signal a blackholing request. Figure 1 shows blackholing activity (the dashed blue line originating from the victim's AS) can be inferred through data from BGP route collectors. Each blackholing event in our data contains, most notably: *(i)* the blackholed prefix; *(ii)* the activation time; and *(iii)* an (optional) deactivation time. For further details we refer the interested reader to our IMC 2018 paper [16].

source	#events	#targets	`#/24s`	`#/16s`	#ASNs
UCSD-NT	12.47 M	2.45 M	0.77 M	31057	25990
AmpPot	8.43 M	4.18 M	1.72 M	41678	24432
Combined	20.90 M	6.34 M	2.19 M	43041	32580

TABLE I
DoS ATTACK EVENTS DATA. WE CONSIDER TWO YEARS OF DATA FROM UCSD-NT AND AMPPOT.

start	#days	source	#Web sites	#data points	size
2015-03	731	`.com`	173.7 M	1045.9 G	23.5 TiB
		`.net`	21.6 M	121.0 G	2.8 TiB
		`.org`	14.7 M	90.7 G	2.1 TiB
		Combined	210.0 M	1257.6 G	28.4 TiB

TABLE II
ACTIVE DNS DATA SET. WE USE TWO YEARS OF DNS DATA COLLECTED BY THE OPENINTEL PLATFORM TO INFER WEB SITES AND ASSOCIATED IP ADDRESSES FOR THE `.COM`, `.NET`, AND `.ORG` GTLDS.

III. CHARACTERIZATION OF ATTACKS

To characterize Internet-wide attack activity, we analyze two data sets built from the previously identified data sources on DoS activity. Both data sets cover a two-year period (March 1, 2015 – February 28, 2017) and complement each other in terms of the attack types accounted for.

Table I summarizes both data sets. Together, our data sets account for nearly *21* million attacks, targeting *6.34* M unique IP addresses, over a two-year period. We observe a total of *2.19* M unique `/24` network blocks that host at least one target, which is about a third of the ∼*6.5* M `/24` blocks recently estimated to be active on the Internet [17], [18].

We identify Web sites that are potentially affected by attacks by looking for `A` records on `www` labels that, at the time of a given attack, mapped to the attacked IP address. We use a

subset of the TLDs that OpenINTEL measures. Specifically, we use data for the three generic TLDs (gTLDs) `com`, `net`, and `org`, which combinedly cover roughly *50%* of the global domain namespace. Table II shows the details of the data set. We infer *210* M Web sites in total.

We find Web site associations associations on *572* k of the *6.34* M unique target IP addresses in the attacks data. This means that of uniquely targeted IP addresses, at least *9%* host one or more Web sites.

We frequently observe that multiple Web sites share an attacked IP address. As a consequence, an attack on a single IP can potentially affect millions of Web sites simultaneously. Upon further analysis, we find that many target IP addresses belong to large hosters, each mapping up to millions of Web sites. In extreme cases, we find a single attack involves potentially up to *3.6* M Web sites. And over the two years considered, almost two-thirds (*64%*) of *210* M inferred Web sites were hosted on IP addresses targeted by attacks. For more details on our characterization of attacks and attacked targets we refer the curious reader to the paper on which this section is based (or our thesis) [9], [19].

IV. Adoption and Operation of Mitigation

The thesis covers two inter-AS mitigation solutions: cloud-based protection services and BGP blackholing.

Cloud-based protection services We study leading providers of cloud-based mitigation, focusing on all nine protection services listed in the 2015 *Forrester Wave* report [20].[1] Specifically, Akamai, CenturyLink, Cloudflare, DOSarrest, F5 Networks, Incapsula, Level 3, Neustar, and Verisign. We study growth in use over a 1.5-year period and consider users (i.e., Web sites) under the three gTLDs: `com`, `net`, and `org`.

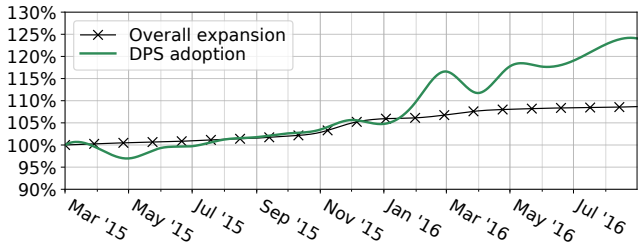

Fig. 3. Growth of DPS use in 50% of the DNS (`com`, `net`, and `org`)

Figure 3 shows the combined growth of the nine providers relative to the start of our data set. The overall expansion of the zones involved is also shown. A trend in the adoption of DPSs becomes apparent. We observe that DPS use has grown by 1.24× over 1.5 years, which exceeds the overall expansion of the considered namespace (1.09×). For this analysis we smoothed out peaks and troughs in usage by taking the median combined customers count over a window of several weeks.

We also learned that a large contribution to the user base and adoption of DPS providers is made by third parties, examples of which are Web hosters and domainers. Some of these larger players activate or deactivate protection for millions of domains from one day to the next. We also learn how protection services are used in terms of, e.g., the use of optional authoritative nameserver protection. The full details of our analyses can be found in our paper [14].

We also investigated the extent to which having been under attack influences DPS adoption. After being targeted by a DoS attack, operators may start outsourcing protection to a DPS. From our data on DPS use we can analyze if, and when, Web sites adopted a DPS. In § III we already linked attacks and Web sites. If we fuse these data sets we can see which attacks lead to adoption. We refer to this process as *migration*.

We investigated the effect of attack characteristics on migration. Figure 4 shows the cumulative distribution functions of the days it took Web sites to migrate, respectively for Web sites attacked with *any* intensity (slowest CDF), and with intensities in the *95-th*, *99-th*, *99.9-th* percentiles of the normalized attack intensity distribution. Comparing these CDFs highlights a drastic reduction of the latency between an attack and the effected site migrating to a DPS. Evidently, the intensity of an attack event strongly correlates with migration to a DPS, specifically in terms of speed, which intuitively suggests a sense of urgency in mitigating DDoS damage and risks. We refer the reader to [9] for our full investigation.

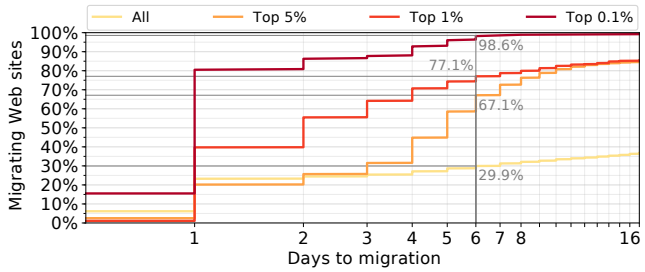

Fig. 4. Migration delay for percentiles of the normalized attack intensity.

BGP blackholing We shift our focus to BGP blackholing. Our blackholing data set, created as described in § II, covers a three-year period, starting March 2015. Table III provides a summary.

collectors	#events	#prefixes	#origins	#AS paths
34	1.30 M	146193	2682	31493

TABLE III
Blackholing data set inferred from public BGP data.

We jointly analyze our attacks and blackholing data to find *"blackholed attacks"*. We match attacked target IP addresses against blackholed prefixes and require the attack's start time to precede the blackhole's activation by at most 24 hours. This allows us to study how operators behave when faced with attacks. We will highlight some of the findings from the thesis in the remainder of this section.

Figure 5 shows the time it takes for blackholing to be activated. Nearly half of blackholed attacks (*44.4%*) see the blackhole activated within one minute, and *84.2%* see activation

[1] An advisory market research company that follows an open methodology.

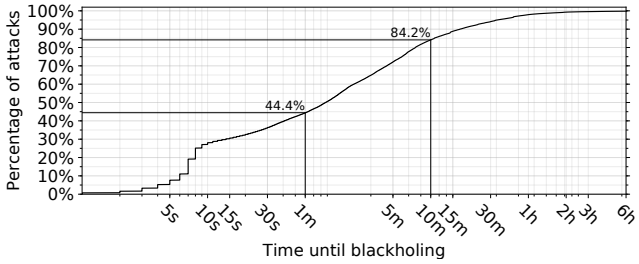

Fig. 5. The distribution of time between the start of attacks and of blackholing, for blackholed attacks in the UCSD-NT and AmpPot data sets.

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.

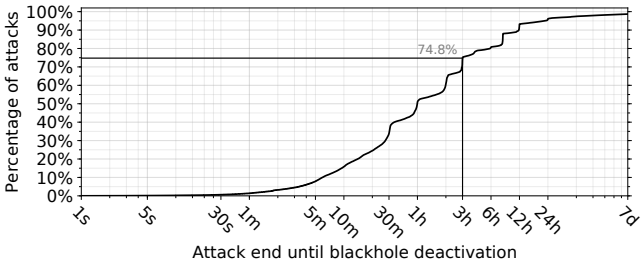

Fig. 6. The distribution of the time between the end of attacks in the AmpPot data set, and the end of correlated blackholing events.

Figure 6 shows the time between the end of blackholed attacks in the AmpPot data set and the deactivation time of the associated blackholing event.[2] For *96.1%* of blackholed attacks, deactivation follows within 24 hours. For *3.9%* it may thus take multiple days. These results suggest lack of automation in recovery from blackholing, and highlight that its side-effects (completely blocking *any* traffic destined to the blackholed prefix) extend beyond the duration of the attack, thereby arguably amounting to a self-inflicted DoS.

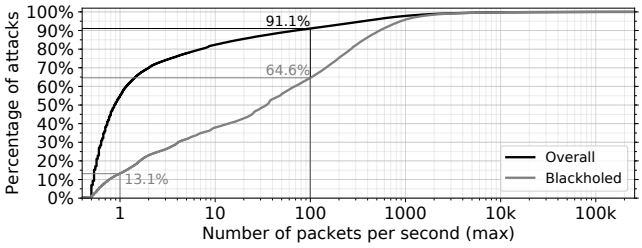

Fig. 7. The intensity distribution for all attacks in the UCSD-NT data set (black curve), as well as for those that are blackholed (gray curve).

The UCSD-NT data set contains a measure of attack intensity (pps_{max}), expressed in terms of the maximum number of backscatter packets per second observed. Figure 7 shows the distribution of these intensities for all attacks as well as for the blackholed attacks only. *64.6%* of blackholed attacks (gray curve) have an intensity up to *100* pps_{max}, which corresponds to an approximate attack traffic volume of *300* $Mbps$. This applies to *91.1%* of all attacks (black curve). A non-negligible percentage of blackholed attacks have a low intensity. Specifically, *13.1%* see an intensity of at most *1* pps_{max} (*3* $Mbps$). This result shows that operators mitigate – with such an extreme measure as blackholing – even less intense randomly spoofed attacks; which raises the question of how little effort attackers need to do to get operators to self-inflict a DoS. Our analysis of blackholed attacks in the AmpPot data set yields similar results. We refer the reader to our paper for these and other findings that we cannot cover here [16].

[2]Blackholing "truncates" the attack end times in UCSD-NT data, which is why we do not analyze deactivation delays for randomly spoofed attacks [16].

V. Hidden Hazards with Mitigation Solutions

We here highlight and quantify a major drawback of using cloud-based protection services: the fact that attackers my bypass and render ineffective protection as a result of so-called "origin exposure."

As first discussed in § II, protection services require *traffic diversion*. That is, traffic must be routed through the security infrastructure of a protection service. Figure 8 shows a schematic of how this works when the DNS is used.

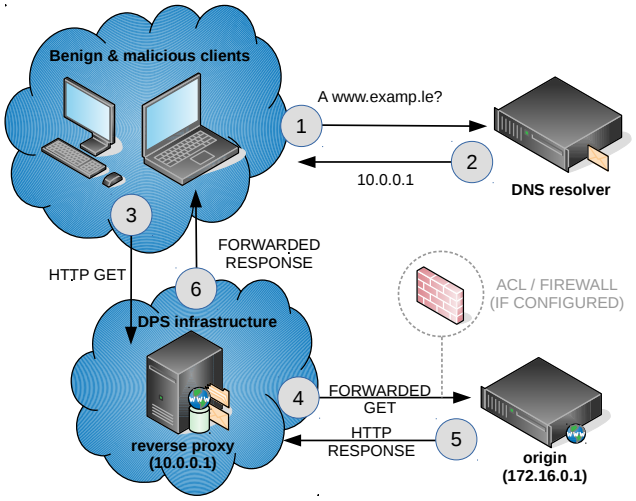

Fig. 8. Schematic of DNS-based network traffic diversion

The origin of a service for which protection is outsourced (e.g., a Web server's actual IP address) should be known only to the protection service. This is because traffic should go through the *reverse proxy* (see Figure 8). There are various "vectors" through which the origin IP address can be learned. In terms of DNS configuration, this boils down to leaving traces of the origin in DNS configuration, or having it exposed through historic DNS data (which OpenINTEL provides). We investigate various DNS-based vectors, a detailed description of which can be found in our CNSM 2017 paper [21]. We use these vectors and OpenINTEL data to find *candidate* IP addresses for the origin of Web sites that are on the Alexa Top 1M list and use cloud-based protection. We consider Web sites under the protection of eight out of the nine protection services from § IV (CenturyLink did not support DNS-based

diversion). With candidate addresses in hand, we attempt to bypass protection by sending a HTTP request directly. We then compare the resulting HTTP content with that retrieved through a regular request (i.e., through the reverse proxy). We use a DOM-tree comparison method based on the tree-edit distance algorithm by Zhang and Shasha, which counts the number of edit operations (inserts, deletes, and substitutions) to get from one tree to another. we find for *40.5%* of all Web sites considered that protection can be bypassed. This comes down to 4408 out of 10884 Web sites.

We also matched exposed Web sites with our attacks data and found that the origin of 843 of 4408 Web sites were attacked after they had started oursourcing protection to a DPS. This comes down to *19%* of all exposed Web sites. These findings underpin that correct management and configuration are needed to ensure effective use of protection services.

VI. Summary

The upsurge of DDoS attacks has left many – ranging from individual operators to governments – questioning how to best deal with the DDoS problem. What exactly are we defending against? How are mitigation solutions operated in practice? And which hazards with mitigation solutions do operators, i.e., end users, need to be wary of? These questions are among many to understandably ask. At the start of the thesis we identified various challenges surrounding such questions, some of which are more *technical* in nature, and some of which are more of a *societal* nature. We set out to focus mostly on technical challenges and the absence of scientific reporting at scale on the topic of DDoS attacks was a driving force behind the thesis.

This paper highlights some of the results of our thesis. Specifically, we summarize select findings from our rigorous characterization of attacks and attacked targets, our studies of the adoption and operation of diverse mitigation solutions, and our investigation into mistakes made in operation and deployment that can render mitigation solutions altogether ineffective.

It is important to note that our work would not have been possible were it not for various preexisting data sources that we identified, some of which are summarized in this paper. Even with diverse data from global Internet measurement infrastructures in hand, fusing and further processing it to, e.g., study attacks and mitigation at scale, is not a straightforward matter. But our successes in doing so led to novel insights and paved the way for further contribution.

In the thesis we also show that overcoming technical challenges puts societal contribution within reach. More specifically, our research efforts enabled us to inform policy makers and regulators dealing with societal questions, in addition to the research community and network operators. We feel this validates our work further and gives meaning to it beyond its scientific contributions.

References

[1] A. Garg, J. Curtis, and H. Halper, "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security*, vol. 11, no. 2, pp. 74–83, 2003.

[2] B. Krebs, "DDoS Attack on Bank Hid $900,000 Cyberheist," https://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/, February 2013.

[3] T. Jordan and P. Taylor, *Hacktivism and cyberwars: Rebels with a cause?* Routledge, 2004.

[4] D. E. Denning, "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy," *Networks and netwars: The future of terror, crime, and militancy*, vol. 239, p. 288, 2001.

[5] R. A. Paulson and J. E. Weber, "Cyberextortion: an overview of distributed denial of service attacks against online gaming companies," *Issues in Information Systems*, vol. 7, no. 2, pp. 52–56, 2006.

[6] S. Hilton, "Dyn Analysis Summary Of Friday October 21 Attack," http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/, October 2016.

[7] "UCSD Network Telescope (UCSD-NT)," http://www.caida.org/projects/network_telescope/, 2010.

[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-service Activity," *ACM Transactions on Computer Systems*, vol. 24, no. 2, pp. 115–139, 2006.

[9] 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 *Proc. of the 2017 Internet Measurement Conference*, 2017, pp. 100–113.

[10] L. Krämer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, K. Yoshioka, and C. Rossow, "AmpPot: Monitoring and Defending Against Amplification DDoS Attacks," in *International Workshop on Recent Advances in Intrusion Detection*, 2015, pp. 615–636.

[11] D. Element, "Netacuity edge premium edition," http://www.digitalelement.com/solutions/netacuity-edge-premium.

[12] "Routeviews Prefix to AS mappings Dataset (pfx2as) for IPv4 and IPv6," http://www.caida.org/data/routing/routeviews-prefix2as.xml.

[13] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras, "A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, pp. 1877–1888, 2016.

[14] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras, "Measuring the Adoption of DDoS Protection Services," in *Proceedings of the 2016 ACM Internet Measurement Conference*, 2016, pp. 279–285.

[15] V. Giotsas, P. Richter, G. Smaragdakis, A. Feldmann, C. Dietzel, and A. Berger, "Inferring BGP Blackholing Activity in the Internet," in *Proc. of the 2017 Internet Measurement Conference*, 2017, pp. 1–14.

[16] M. Jonker, A. Pras, A. Dainotti, and A. Sperotto, "A First Joint Look at DoS Attacks and BGP Blackholing in the Wild," in *Proc. of the 2018 Internet Measurement Conference*, 2018, pp. 457–463.

[17] S. Zander, L. L. Andrew, and G. Armitage, "Capturing Ghosts: Predicting the Used IPv4 Space by Inferring Unobserved Addresses," in *Proceedings of the 2014 ACM Conference on Internet Measurement Conference*, 2014.

[18] P. Richter, G. Smaragdakis, D. Plonka, and A. Berger, "Beyond Counting: New Perspectives on the Active IPv4 Address Space," in *Proceedings of the 2016 ACM Internet Measurement Conference*, 2016.

[19] M. Jonker, "DDoS Mitigation: A Measurement-Based Approach," Ph.D. dissertation, University of Twente, 2019, https://doi.org/10.3990/1.9789036548687.

[20] R. Holland and E. Ferrara, "The Forrester Wave™: DDoS Services Providers (Q3 2015)," Forrester Research, Inc., Tech. Rep., July 2015.

[21] M. Jonker and A. Sperotto, "Measuring Exposure in DDoS Protection Services," in *Proc. of the 13th International Conference on Network and Service Management (CNSM'17)*, 2017, pp. 1–9.