Quantifying TCP SYN DDoS Resilience: A Longitudinal Study of Internet Services

Harm Griffioen
Hasso Plattner Institute for Digital Engineering
University of Potsdam
Potsdam, Germany
harm.griffioen@hpi.de

Christian Doerr
Hasso Plattner Institute for Digital Engineering
University of Potsdam
Potsdam, Germany
christian.doerr@hpi.de

***Abstract*—One of the most prevalent attacks in the Internet are TCP SYN floods, during which a massive number of malicious connection requests is being sent to a victim that will eventually use up all of the server's resources. In order to make these attacks more difficult to track back and defend against, SYN floods are typically injected with spoofed source addresses, which provides the interesting side effect that an "echo" of ongoing attacks becomes visible through the resulting background noise.**

This paper provides a longitudinal study of this Internet backscatter received at more than 65,000 IP addresses over a period of 5 years, which allows us to quantify the types of victims that are attacked, the attack duration and intensity, and whether services collapse under the load – thereby providing an insight into the resilience of services provided publicly on the Internet. Our findings show that DDoS attacks have significantly changed in type and magnitude within this relatively short period of time, however we also see that Internet services by-and-large co-evolved with the increased threat landscape and become increasingly better provisioned, yet at a rate insufficient to keep up with the growth of attacks.

I. Introduction

One of the earliest and still most common type of attacks on Internet services are distributed denial-of-service (DDoS) attacks. DDoS attacks are typically launched in one of two ways: first, a victim gets flooded by a large volume of unwanted data, hereby clogging the available bandwidth of the target so that legitimate users may no longer be served. Or second, the adversary sends a massive number of requests to the victim, with the goal of exhausting some finite resource such as the maximum number of connections, system memory, or interrupts. If the attacker can inject them at a rate faster than the target can service them, and the victim has no means of differentiating legitimate requests from malicious connection attempts to discard them preemptively, the server under attack will eventually succumb to the load.

An easy and thus very widely adopted technique for resource exhaustion attacks are TCP SYN floods, which accounted for 82.43% of DDoS attacks in Q2 of 2019 [1] and are thus a significant portion of the DDoS attack space. Here, clients pretend to initiate a TCP connection by sending a TCP SYN packet to a server. Following the protocol specification, the server reserves some memory to handle the connection and acknowledges the attempt with a TCP SYN/ACK, which a legitimate client would complete with a TCP ACK frame. In a typical TCP SYN flood, the malicious clients such as infected computers under the control of an adversary do not close the handshake, thereby leaving the connection open, eventually exhausting the possible number of concurrent connections the server can handle. To make the attack even more difficult to counter, SYN floods furthermore spoof the source IP addresses of the request, which makes it highly difficult for the server to tell friend from foe to for example selectively discard requests.

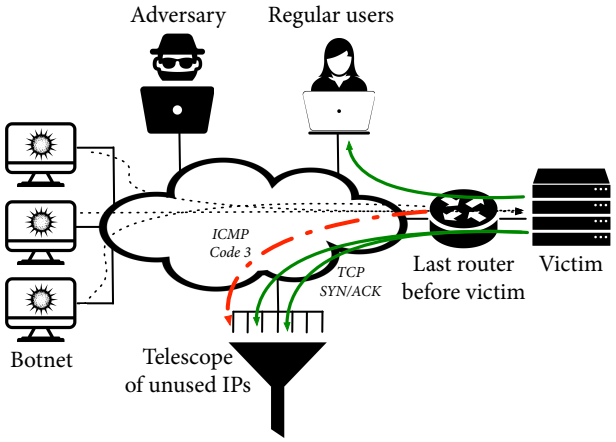


Fig. 1: Due to IP address spoofing, the TCP SYN/ACKs from the victim and ICMP status codes are delivered random addresses in the Internet and thus provide insight into the attack

As part of the attack, TCP SYN/ACKs are now delivered to those hosts whose addresses have been spoofed in the request. As shown in figure 1, this so-called backscatter hence provides a real-time view of the targets currently under attack with this method, which we collect by monitoring a unconnected, publicly routable IP addresses, frequently referred to as a network telescope. While the returned backscatter already allows us to determine the victim and quantify the volume of the attack [2], the Internet Protocol suite (IP) contains the ability to return status codes to the sender, for example if the delivery of a

ISBN 978-3-903176-28-7

message fails. Of particular importance for this paper is the ICMP type 3 message, which gets returned by the destination's gateway if the final destination has become unreachable, for example as currently being overloaded as part of an attack. The resulting ICMP backscatter thus allows a quantification when and how often Internet services fail as part of a DDoS attack and how they were able to handle the load.

While studies of the Internet's resilience either focus on structural, topological analyses [3] of the Internet or specific case studies of DDoS attacks [4], a broad quantification of the resilience of web sites across the entire Internet is challenging to do at scale and has not been done. In this paper, we address this gap specifically for the case of TCP SYN flood attacks. Using an unused IP address block as a telescope, we quantify attacks, their victims and specifically the tipping points in a longitudinal study over the last 5 years. Specifically, we make the following four contributions:

- We track the development of this type of resource exhaustion attacks from 2015 to 2019. We find that common services like HTTP, HTTPs or SSH get attacked most often, however attacks on these services are rarely successful.
- We show that most successful TCP SYN flood attacks occur at services run on non-privileged ports such as game servers or an application gateway service, and see that attacks almost exclusively target servers (such as a game server) and not the actual end users.
- We demonstrate that professional shared hosting environments are not per se more resilient against DDoS attacks than dedicated hosts or even home networks. Adversaries seem to adjust their flood volume to the capabilities of the server infrastructure.
- We find clear evidence that adversaries increase their attack capability and attacks get bigger by the year across the entire spectrum. At the same time, the resilience of Internet services does not keep pace with this capability upgrade, and we find a statistically significant trend that services collapse faster each year.

The remainder of this paper is structured as follows: section II provides an overview of related work and previous findings of DDoS attacks in the Internet. Section III discusses the data collection and preparation process used in this paper, as well as the statistical confidence intervals of the DDoS estimations made in this paper. Section IV discusses the resilience of Internet hosts by service provided, and links their ability to withstand attacks to operational and geographical factors. Section V discusses how the technique described in this paper can be scaled to assess DDoS attacks even in the absence of ICMP backscatter. Section VI provide a longitudinal view at the Internet ecosystem and discusses trends in attacks and resilience over time. Section VII summarizes and concludes our work.

II. Related Work

Capturing backscatter to estimate worldwide denial-of-service attacks has been done by various other papers, and was first introduced by Moore et al. [5] in 2006. It is used by various studies to analyze protocol based attacks, in which resources of the victim are exhausted [6], [2]. To classify such protocol based attacks, Moore et al. created flows in which packets originating from one IP address were grouped if the inter-arrival time of packets were less than 5 minutes. The authors removed flows with a size of less than 100 packets, a total duration of the flow smaller than one minute, and flows that did not cover multiple IP addresses of their network telescope, in order to remove flows caused by misconfigurations from the dataset.

Wustrow et al. [7] monitored Internet backscatter at multiple /8 subnets and considered, in addition to attack streams, scanning and misconfigurations in the backscatter. To classify attacks, the authors define packets with the SYN+ACK, RST, RST+ACK or ACK flag set as backscatter. Another study by Blenn et al. [2] defined backscatter as only the packets with the SYN+ACK and RST flags, as the TCP protocol [7] states that a server should only respond with these flags on initial request.

Apart from using network telescope, research has investigated DDoS attacks using a variety of techniques. Kramer et al. [8] propose Amppot to measure amplification DDoS attacks, which has consequently been used in a variety of studies [9], [10], [11]. Next to Amppot, the authors of [12] propose another system to capture these amplification attacks, and use it to measure 1000 days of Internet attacks.

Blenn et al. [2] introduced a method leveraging backscattered ICMP packets to quantify whether a server falls over. In normal operation, a server responds with a SYN+ACK when a request is received on an open port. However, in case the server is unable to process the request, the server or a router in-between will generate an ICMP destination unreachable frame (ICMP type 3) unless this functionality is switched off. By monitoring for these ICMP packets, the authors are able to estimate the attack size needed to successfully DDoS a server. The results show that the distribution of servers sending these ICMP packets is long tailed, with the most resilient servers sustaining floods of well over 100 Mbps before falling over. The paper also shows 85% of recorded attacks have a speed of 10 Mbps or lower, which is in some cases already sufficient.

Apart from the work of Blenn et al., the resillience of Internet services remains a largely untouched topic in the literature, where the large focus is on quantification of DDoS attacks. In this work, we quantify the resilience of Internet services using the methodology in [2] over a period of five years, in order to estimate the ongoing threat arising from TCP protocol attacks.

III. Data Collection

We conduct this study based on two datasets. First, backscatter as received by a network telescope, which we then augment by passive DNS data to pinpoint the domain name and the type of hosting setup under attack. This section briefly outlines both.

A. DDoS Backscatter

The primary dataset used for this study are unsolicited packets collected by a large network telescope of 65,000 IP

addresses. Such a telescope consists of unused but publicly routed IP addresses, collecting unsolicited traffic sent to the IP address. As the addresses are not connected to any client machines, two types of data are received by this setup: first port scanning traffic where remote parties probe which ranges are in use and at which IP addresses hosts and services are active, and second backscatter reflections that are delivered as the attacker spoofed the telescope's IP addresses during an attack. Separating these two is however easy, and we follow the standard practice [7] of labeling TCP SYNs as port scanning, and TCP SYN/ACK as well as TCP RST packets as backscatter. As UDP does not maintain a connection state and is thus not subject to the same type of resource exhaustion attack as TCP is, we consider it as out of scope for this study.

As during the time frame of our longitudinal study between 2015 and 2019 more than 29 TB of raw network traffic was collected by the telescope, we selected 3 months from the start of each year for analysis, which reduces the data volume yet given the plethora of attacks still provides reliable results. During the observation period, we saw a total of 14,091,088 attacks targeting 4,712,322 unique IPs. These attacks backscattered 1,674,433,469 packets towards the telescope.

As we are interested in the characterization of attacks, we group TCP SYN/ACK and ICMP packets received across the telescope into a single attack, if the backscatter originates from the same victim IP and all attack packets were targeting the same port. Given the relatively large size of the telescope, the analysis provides some tight estimation on the overall size of IP spoofed TCP SYN floods. Using the method described in [2], we find the error margin in over- or underestimating the attack volume based on the telescope in use to be below 1%, and since we are sampling from a statistically significant share of the IPv4 space we can also reliably approximate the DDoS start and end times based on when we observe the first and last packet from a victim in our range. If no packet with the same parameters has been received for more than 10 minutes, we mark the DDoS as terminated. Given the size of our network range, these parameters mean that we record TCP SYN attacks as long as they are larger than 2 kBps. While an adversary could run TCP SYN floods from its own source IP addresses, this would make the attack easy to attribute and mitigate, as packets from a limited number of origins could be trivially filtered out. In practice thus, adversaries spoof source IP addresses, and if in the worst case packets originate from the entire IPv4 space, source-based filtering is no longer a feasible defense. While in theory it could be possible that adversaries spoof attack packets with any IP addresses but ours in the telescope – which would mean that these attacks would not backscatter to us and thus be part of our dataset –, such selected spoofing has not been described in the literature to date.

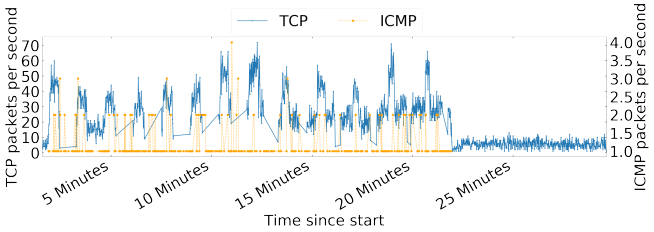
B. Passive DNS Lookups

While the backscatter received in the telescope tells us the IP address of the victim, it does not provide direct insights into the potential victim and the type of server that is attacked. We hence use passive DNS lookups as an auxiliary dataset, and resolve the domain names hosted at a particular IP address during the time frame when the IP address was sending us backscatter. If we find a one-to-one match of a domain name to a server (in other words, only one type of domains – e.g., bank.com and bank.ca – no unrelated records are hosting there), we classify the domain as a dedicated hosting setup. This is also the case of the domain is hosted by multiple IP addresses in a load-balancing configuration. If no domain names point to a particular IP address, we classify it as non-professional (home) hosting server. If a large number of domain names point to the IP address under attack, we refer to the attacked server as a shared hosting provider, which in this case provides the disadvantage that it is not possible to see which domain name and client exactly was the target.

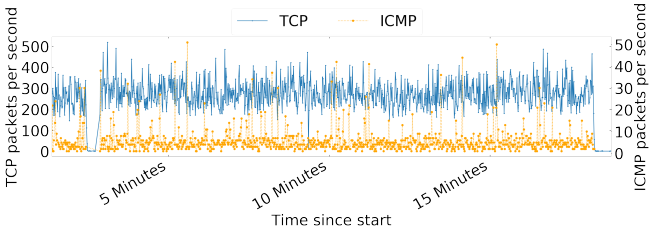
IV. Quantifying Service Resilience through SYN/ACK and ICMP Backscatter

The backscattering of TCP SYN/ACKs from the victim and ICMP type 3 – Destination unreachable – packets from the victim's gateway provides interesting insights into the nature and result of a SYN flood DDoS attack. For this work, we focus on two different ICMP type 3 responses, those sent by the gateway and those sent by the host. RFC 792 [13] specifies that packets with ICMP error code 1 may be sent if the gateway determines that the host is unreachable, and error code 3 when the host determines that the requested port unreachable. If we observe TCP SYN/ACK packets shortly before receiving ICMP packets, these destination unreachable packets with error code 1 or 3 show that the service is temporarily not responsive. Figure 2 shows packet captures of three different DDoS targets that are able to deal with the incoming packet floods with different degrees of success. In blue we see the volume of TCP SYN/ACK frames pouring into the telescope range, in yellow the volume of ICMP Destination Unreachable notifications. As we see in subfigure (a), this particular website is targeted by a large volume of connection requests which causes it to collapse in regular intervals. During this time, incoming SYNs are responded by the gateway as shown in yellow, until the server has recovered and again begins to service requests, only for this cycle to repeat. Note in subfigure (a) that at some point the successful DDoS attack stops, while another one continues, which is however below the capacity threshold of the service and causes no harm.

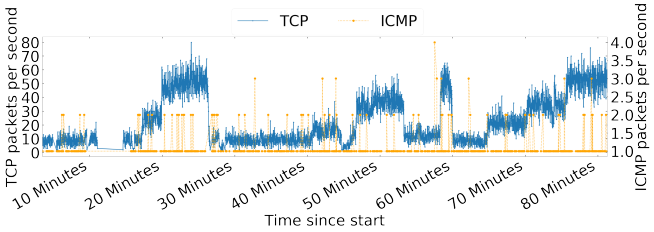
Attacks do not have to result in a complete breakdown of a service. At the boundary when the processing queue starts to become saturated with requests, we see the type of behavior shown in subfigure (b). Here the website continues to process connection requests, but occasionally becomes unresponsive for very short periods of time. In this figure, approximately one in every 52 request is responded by the router. From these two behaviors, the onset of packet drops and the full outage, we can derive an estimate of the available capacity and resilience of the



(a) Service intermittently stifled by SYN flood



(b) Service with package drops, but continuing operation



(c) Service largely unaffected by the SYN flood

Fig. 2: The combination of SYN/ACKs and ICMP backscatter reveals how a service continues to operate under a DDoS attack

service, which in the following are called the fallover point. In the vast number of cases, especially services such as HTTP(s) or SSH, SYN floods have almost no measurable impact on the ability of a victim to service its clients. Subfigure (c) shows such an example, where after no effect the DDoS intensity first increases and the attack is then stopped, before another attempt is launched later again. In the following, we will investigate the resilience of Internet services to TCP SYN DDoS attacks from 2015 to 2019, and investigate if and how the ability of sites to withstand these attacks has changed over these 5 years.

A. The Resilience of Services

DDoS attacks are common place, we record on average more than 30,000 of them every day. Out of these, only vanishingly few get actually recognized by their users or receive public attention for example in media reporting, which typically only happens if well-known services collapse or a new record gets broken that makes this attack newsworthy. As can be seen in the cumulative density plot of figure 3 where we aggregated the overall attack volume (which we can approximate due to the size of the telescope and random source IP spoofing) by year, most attacks are actually very small in size. Across the five years of observation, 50% of all attacks were smaller than 11,000 to 20,000 packets per second depending on the year,

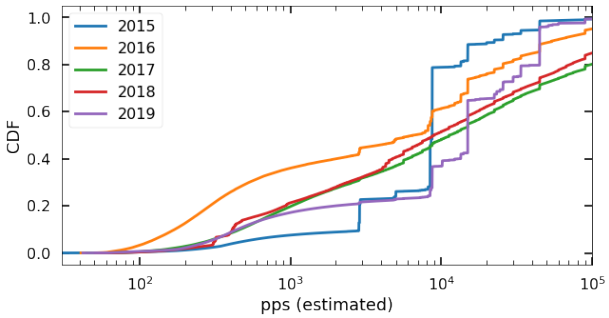


Fig. 3: Attack intensity for all attacks per year, no clear trend is visible in the overall attack traffic

which works out between 0.41 and 0.76 MBps of estimated attack volume. While this number seems small as opposed to the large numbers reported in the media, recall that this particular attack is not aimed at congesting the line, but rather to exhaust the resources on the host itself. Only a tiny fraction of attacks reach considerable volume, in 2019 for example 1% of attacks were larger than 25 Gb/s. Although some fluctuation exists between different years, we do not see a clear trend towards a drastic increase in TCP SYN flood volume, at least when we look at the entirely landscape of attacks. When it comes to peak volume, that is the largest or 0.1% largest attacks recorded during a calendar year, we find a statistically significant growth ($p<0.05$) in size of these largest attacks.

The reason that the dominance of small attacks in the distribution of attacks is relatively unknown can probably be linked to observation bias. As coverage in the media and Internet venues would typically only occur when DDoS attacks are “noteworthy” in that they broke some record or hit an important service, attacks that do not meet these criteria or are directed at small services with few users would easily go by unnoticed.

One aspect where this can also be seen is the type of ports targeted in attacks and the degree they collapse under load. Table I shows the ten least resilient services, as measured by the percentage of attacks in which a particular service stopped responding and backscattered ICMP Destination Unreachable packets. For comparison purposes, we also include the common – and commonly attacked – services telnet, HTTPs, HTTP and SSH. As can be seen in the table, the overwhelming number of attacks hit well-known ports, however services hosted at higher ports (thus, applications run by the user and not system services) are much more likely to fall over in an attack. These ports are non-standardized with respect to applications by the IANA, and are hence labeled as “Unknown”. The general ranking of victim services and their fallover rate is a remarkable stable pattern over the entire 5 year observation period.

Not only is there a skew in terms of which ports are targeted, but we also see that the success of attacks highly depends on the type of service under attack. Popular commercially used services such as HTTP or SSH are almost never impacted, here

TABLE I: Attacked ports ranked by percentage of successful attacks. Attack rates are estimated using the method in [2]

Rank	Port	Service [14]	Successful (%)	Total attacks	Total hosts	Estimated Avg. pps (x10^4)	Estimated pps on fallover (x10^4)	Avg. fallover duration (seconds)
1	56900	Unknown	9.37	215	190	10.70	10.44	3769
2	64711	Unknown	8.48	100	100	1.87	1.97	1484
3	18090	FIFA Manager 10	4.07	140	140	15.75	6.97	976
4	9094	Citrix NetScaler	3.75	406	401	10.21	18.92	1304
5	25565	Minecraft	3.67	6847	4605	12.33	9.11	12155
6	20121	Unknown	2.88	75	75	0.09	0.033	4915
7	57125	Unknown	2.87	65	36	14.36	9.73	57
8	9978	XYBRID RT Server	2.76	444	359	302.52	214.46	88
9	20101	Soldier of Fortune 2	2.75	64	28	0.24	0.04	2983
10	20163	Unknown	2.73	54	27	0.06	0.05	8254
61	2323	Telnet	1.39	166	154	21.01	5.76	3979
364	443	HTTPs	0.44	67,131	27,139	9.47	14.67	4196
1382	80	HTTP	0.04	8,952,149	2,864,452	2.01	9.45	3512
1444	22	SSH	0.01	1,735,748	137,020	1.07	6.46	2590

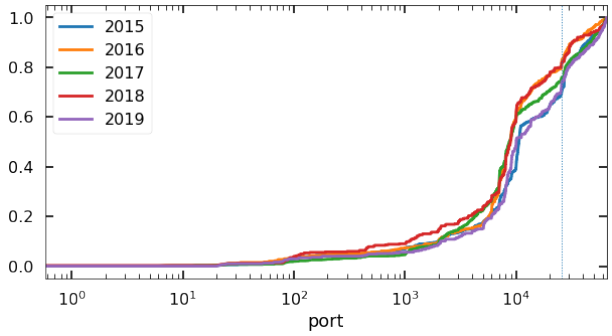


Fig. 4: CDF of the port distribution sending ICMP packets, normalized by the total number of attacks received by the port, the vertical line is located on the default port used by Minecraft

the success rate is way below one per mille, while games and a number of services run outside of the range of well-known ports collapse as often as one of fifty attacks or more. It is interesting to note that the average attack volume matches the average fallover point especially for high port services. For instance, we observe that for port 56900 hosted applications become inoperative on average when hit with a SYN flood of 10.44 $\cdot$ 10^4 packets/second (pps). The average attack volume follows this average fallover level very closely with 10.7 $\cdot$ 10^4 pps. This match of attack volume to fallover level appears as a consistent picture across all "Unknown" services. In contrast to this, game servers and telnet devices are attacked much more intensively than necessary, while for common standardized services the average attack volume is significantly smaller than necessary for services to collapse.

This dominance of non-standard services in the victim population can further be seen in figure 4 which plots a cumulative density function of the ratio of victims that fall down with ICMP backscatter over the number of all attacks received on a particular port. This normalization is essential given the hefty skew in attack traffic that was already visible in table I, and a visualization as a CDF helps to see the minuscule contribution of the plethora of high port numbers (which are randomly selected and the signal is thus spread out over hundreds of ports, compared to the well-known ports 80, 443 or 22 where the bulk of HTTP/HTTPs/SSH services are reachable). As can be seen in the figure, most of the service collapses happen on non-privileged ports ($>$ 1024). These correspond to services spun up by users, however the relatively little share of dynamic ports ($>$ 49152) show that the bulk of attacks is directed at services, not users of services. In other words, TCP SYN floods predominantly target the operator of a game server, and only to a lesser degree the players connecting to it.

It is curious to see in table I that the average attack duration that results in a fallover is comparatively long. As can be seen in the table, average attack durations in case of a successful outcome on the order of 30 or 60 minutes are the norm. The only large outliers are ranks 7 and 8, which accomplish the objective typically in less than 1.5 minutes, in these cases the attack volume is also significantly larger in absolute numbers and also 50% larger than necessary with respect to the average fallover levels. As a rule of thumb, the higher an attack intensity is, the shorter the attack lasts.

B. Victim Characteristics

The large difference in attack volume and percentage of services that send ICMP backscatter demonstrates a large heterogeneity across DDoS victims. For instance, the comparatively large share of high ports would at first sight suggest home users and non-professional operators as prime targets. In the following, we will thus characterize the victim population.

In order to send a DDoS, one needs to know the destination. A target could be addressed based on a domain name, or based on the IP address of the target machine. A first glance it would seem logical that the most effective modus operandi would be to use the domain name. First, if a service is distributed over multiple machines a DDoS on a domain name (with a sufficient low TTL or a round robin resolution) would target all of the servers, and second, if a host collapses under a DDoS or is

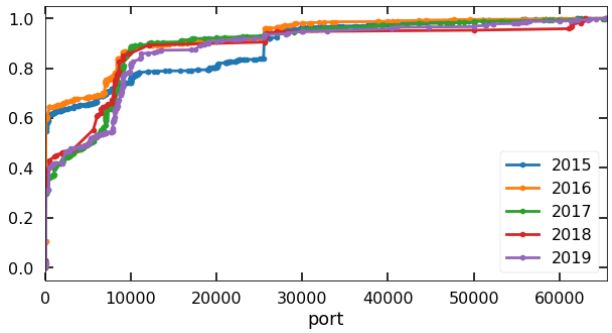


Fig. 5: Number of domains hosted on services sending ICMP

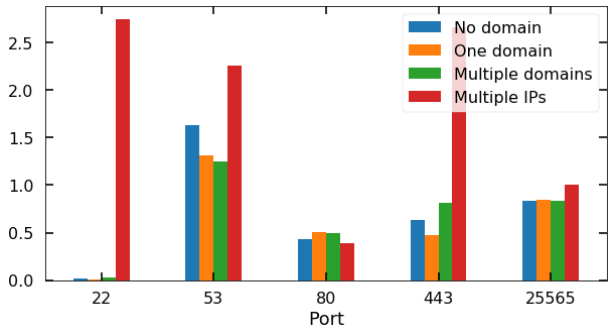
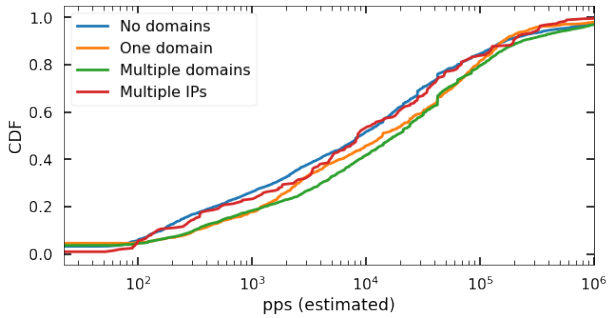
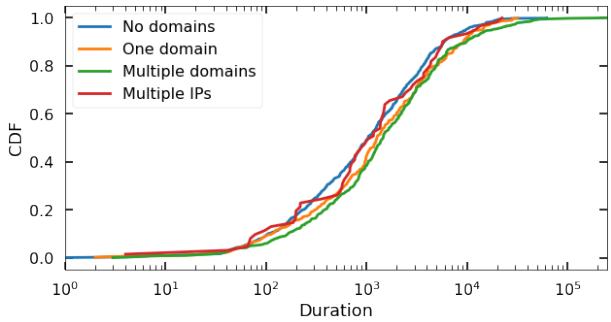


Fig. 6: Relative amount of packets received on popular ports



(a) Speed of attack



(b) Duration of attack

Fig. 7: Speed and duration of an attack before a service falls over, grouped by category

moved somewhere else attacking the domain name would move the SYN flood to the new location as well.

In order to investigate whether adversaries were attacking victims by proxy based on domain name or directly by IP address we made use of passive DNS. For the observation period, we looked up for all remote IP addresses that were sending us backscatter all domain names that resolved just before or while the attack was ongoing to that particular IP address according to a passive DNS provider. As we know which port was attacked, we can link the addressing method to the particular service in the crosshair. Figure 5 shows the number of domains linked to a particular host under attack as a function of the targeted service. The plot visualizes this again as a CDF to meaningfully show the distribution in the presence of a drastic distribution skew and large spread across many high user ports. As can be seen in the plot, less than 30% of domains are linked to hosts attacked on ports 10,000 or above, and only a fraction of a percent are linked to hosts where we receive backscatter from a port that would be dynamically bound by an application. If we compare this to the distribution of attacked services in figure 4, we see that attacks on these user-run services seem to be very specific, and directly target individual machines.

While this could imply that especially non-professionally administered systems are less well provisioned, configured and hence more likely to fall down, this hypothesis does not hold globally. While categorizing by the type of service is one way to assess "professional" usage, a more precise way will be to look at the number of different domain names pointed at a particular IP address. After all, merely running a web server does not imply professional or non-professional activity, as this could be operated and monitored by a professional hosting company. Such a company could however operate a large number of web sites on the single server. Alternatively, a bank would host their web page not at a single server, but also multiple hosts across which it load balances. We thus categorize victims by the number of domains that point to a particular IP: (a) an IP with a large number of domains implies some shared hosting, (b) an IP exclusively dedicated to a particular domain name, (c) a set of IPs that are all hosting a particular domain in a load sharing configuration, and (d) a server to which no domains point. Figure 6 shows the backscatter by these categories for five commonly attacked ports, normalized for each port to the relative distribution of attacked targets. As we see in the figure, environments with a lot of resources dedicated to hosting a service suffer from significantly different attacks, but for select services slight differences exist between these categories of service provisioning.

Given this classification of victims, we do see that adversaries show a slight, yet significant difference in the way they perform DDoS depending on the type of target. Figure 7 shows cumulative density function plots of the speed and the duration of SYN flood attacks before a service falls over, with the targets grouped together by the categorization discussed above.

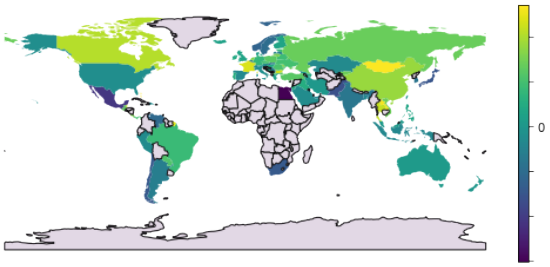


Fig. 8: Proportional fallover rate by country, normalized by the number of IP addresses located in a country. A value of 0 indicates that the country has an average fallover rate, +1 is a higher rate, and -1 a lower rate

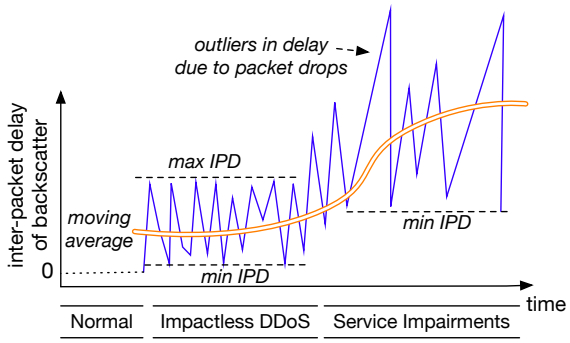


Fig. 9: Concept of DDoS outage estimation based on shifts in the inter-packet delay of backscatter

In figure 7(a), we see that hosts which do not host any domain are targeted at a slightly lower attack rate than shared and dedicated hosting servers. Subfigure (b) however shows that there is almost no difference in the duration of the attacks until service collapse, thus, adversaries compensate for more resilient services by higher attack power. This can be partially explained by looking back at figure 2 where we showed the behavior of services during attack. While in figure 2(a) a service stopped being responsive altogether, also in figure 2(b) the service will be impaired and show some partial on/off behavior. This impairment might be seen as a sufficiently successful outcome by the attackers.

Also in terms of geography, we are able to observe differences. Figure 8 visualizes the proportional rate at which services collapse, normalized by the total number of IP addresses located within a country. A value of 0 means that during SYN floods as many services go offline as we would expect based on the number of IP addresses that are located within that country. Values of +1 mark a positive deviation from this global expectation, meaning that a larger percentage of hosts collapsed in this country compared to the worldwide average. A value of -1 means a more resilient deployment, and countries where not sufficient attack data has been collected are colored in grey. Overall, we see a number of hotspots. For example, countries with a slower average Internet connectivity according to the global index of speedtest.net [15] such as Mongolia, Thailand or New Guinea experience drastically higher outages than countries such as North America, Europe or Japan with higher average Internet access speeds. Previous work pinpointed a significant share of DDoS activity directed at Chinese websites [8], [16], [17], indeed we see countries such as China or Russia experiencing more DDoS activity and higher fallover rates in our longitudinal study than we would statistically expect.

V. Beyond ICMP

Until now, we have established DDoS attacks and service outages based on the backscattering of TCP SYN/ACKs and ICMP type 3 messages. However not all networks enable ICMP status messages and there are networks that actively filter them out. It is however possible to do some approximation of the DDoS progression based on rate differences in SYN/ACK backscatter, which we will discuss in the following.

Imagine an attack on a victim web server where the network drops ICMP status messages. After the onset of the attack, the telescope would receive TCP SYN/ACKs as backscatter. If the spoofed source IPs are randomized, the inter-arrival time will however follow a Gaussian distribution, with the mean equal to the fraction of the IPv4 space monitored by the telescope. Furthermore, if two consecutive spoofed IPs are both from the telescope range – which in our case happens with a probability of 1 in 65,000 – we obtain the momentary attack speed from the minimum inter-packet delay (IPD) threshold. When the DDoS attack speed increases and is beginning to cause outages in the server, we will experience outliers in the IPD of the interceding backscatter. As individual requests go unserviced, we "miss" individual packets that would have been directed at the telescope. This is noticeable in gaps and this spike in maximum inter arrival time, leading to an increase in the mean of IPD distribution, as well as possibly a general increase in the minimum inter-packet delay if the service responds generally slower. Figure 9 visualizes this schematically. We can thus characterize service impairments during a DDoS attack, if (a) we receive backscatter approximately at a constant rate, (b) we observe spikes in IPD due to drops of "our" packets, and (c) the distribution mean increases measured as a moving average. We experimentally validated this hypothesis and measurement technique in the lab, using a TCP SYN flood on an Ubuntu victim host. As the TCP SYN flood increases and approaches critical, we indeed see an increase in IPD prior to a collapse of the service.

Figure 10 shows a selection of ICMP-less DDoS attacks detected by this method, with a moving average across 250 packets and the triggering condition that the mean IPD has to increase a factor of 10 above the previous average. In the top level corner of the figure, we see exact the behavior depicted in the theoretical model of figure 9. After 4 hours of backscatter, the inter-packet delay in blue sharply increases, as can be seen by the moving average in orange, while at the same time we

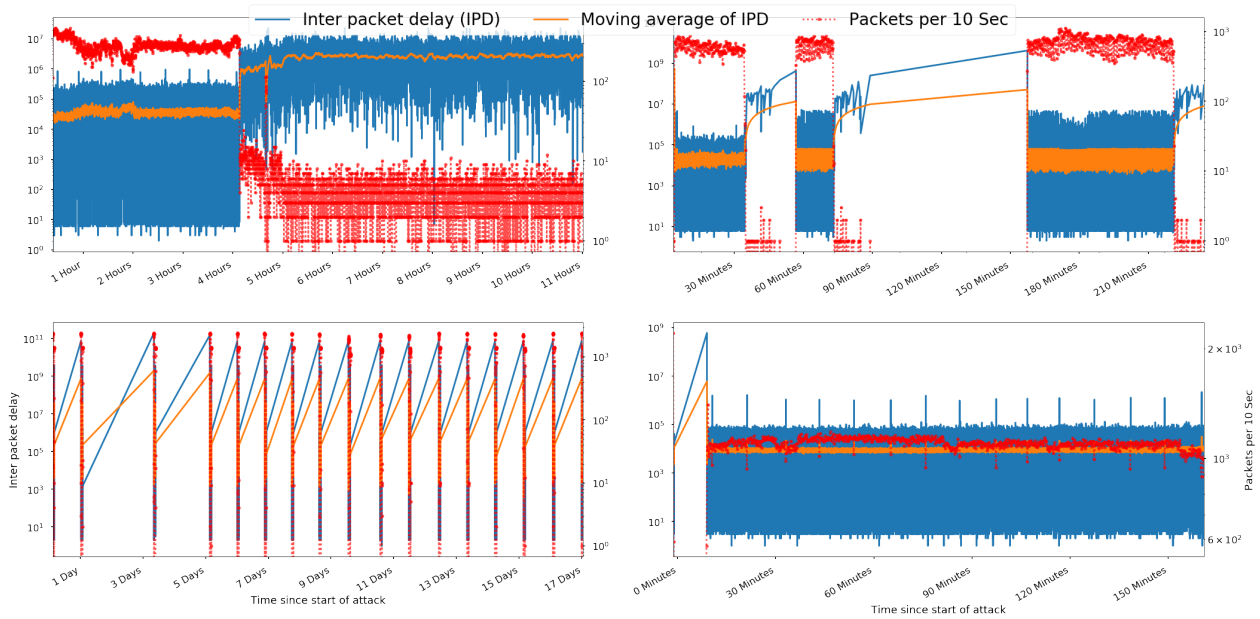


Fig. 10: DDoS attack fallover based on inter packet delay observed in a network telescope. The first image shows a continuous attack where the server fell over after 4 hours. The second and third images show attacks that stop after crippling the server, and attack again to cripple the server. The final image shows sustained load on a server without a major outage

experience "lost" packages. The number of incoming packets (in red) drops and highly fluctuates: while before the service impairments the telescope received every single packet, now packet drops occur randomly and even in consecutive bursts.

Overall, we have found that services collapse in 5.39% of all TCP SYN flood DDoS attacks without the emergence of ICMP backscatter. We find no structural difference in terms of targeted ports, in case of attacks that fail with and without ICMP status messages. While one would intuitively imagine DDoS attacks to be a mere flood of packets that starts at some point and endure for a certain period, we find that in 26% of the cases TCP SYN floods to be pulsed. Examples of this behaviors are shown in the top right and bottom left corner of figure 9, where the DDoS is sent as a finite burst and stops as soon as the service is crippled only to pick up again later on, in contrast to a continuous speed attack in the bottom right. We find that those attackers that closely monitor the victim and operate in bursts to be vastly more successful in technique: those attacks following a burst pattern are able to topple over the target in 40% of the attacks, whereas in continuous attack modes the percentage of successful attacks is only 4.9%.

VI. Service Resilience over Time

When we look at the progression of DDoS attacks over the past years, we see a continuous increase in peak attack volumes [18]. While peak volumes are an important datapoint for the total capacity planning of DDoS mitigation providers, in the following we will investigate whether attack speeds increase in the case of the most occurring attack vector, TCP SYN floods.

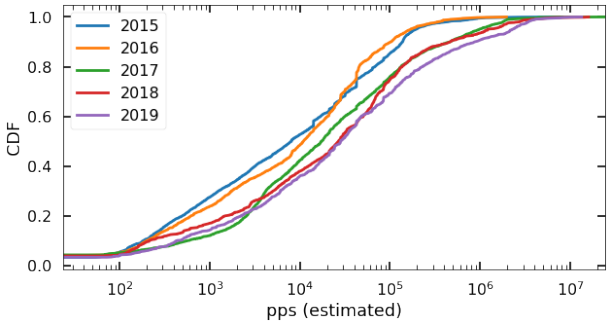


Fig. 11: Estimated attack intensity required for a server to fall over, grouped by year. The figure shows a trend in which services become more resilient, as more attack power is needed to cripple the server

Figure 11 shows a cumulative density function of the attack volume required for an attack to be successful (measured in total packets/second part of the attack), for each of the 5 year observation period. We see a clear, and surprisingly linear progression. Not only do TCP SYN floods need to be larger in general, also the entire attack spectrum simply shifts to the right. In other words, all attacks (and in extension actors) have to roll out bigger guns every year and continuously deploy more attack capacity across. We find a strong statistically significantly correlation between the median attack intensity (pps) and the year ($r = 0.9773$, $p < 0.05$), as well as the average attack intensity (pps) and the year ($r = 0.9637$, $p < 0.01$). While the intensity required for an attack to be successful shifts, the

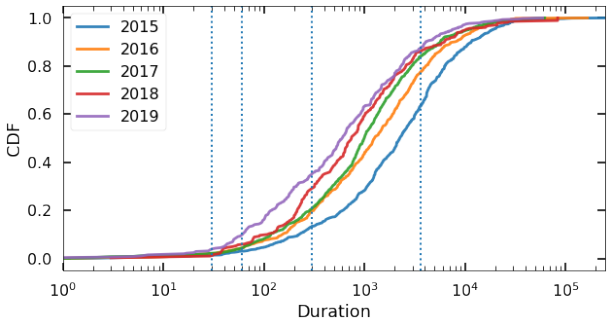


Fig. 12: Time before a server fell over, grouped by year. The figure shows a trend in which servers fall over faster. Lines mark attacks of respectively 30 sec, 60 sec, 5 min and 1 hour

overall attack intensity does not (figure 3), showing that a large portion of attacks will be unsuccessful. This also means that the general increase in the DDoS threat landscape is not just the result of new attacks and major instances such as [19], but occurs across the board.

When we look at the duration that victims were under attack before a service finally fell over, we observe the exact opposite trend. As can be seen in figure 12, not only does the average duration until collapse decrease each year in the 5 year study period, but we also see a general decrease in resilience across the entire spectrum. The median duration until collapse as a strong significant correlation with the year ($r = -0.923$, $p < 0.05$). This is somewhat surprising. On the one hand, the availability of many DDoS protection services, it is now comparatively easy for service operators to shield themselves from TCP SYN floods. On the other hand, the fact that we see a shift across the entire distribution means that not only simple, home-grown game servers do not get more resilient, also professionally managed and run hosts did not seem to improve much within our observation period. Whatever gains in defense were accomplished, seemed to have been entirely consumed by the adversaries' increase in attack ability.

Although services can absorb more and more packets year by year before they collapse in the DDoS, we surprisingly do not find any statistically significant differences by the type of victim, as defined above with shared or dedicated hosters compared to domain-less servers. DDoS protection does not exclusively seem to be rolled out in professional environments, but across the entire spectrum, if at all.

VII. Conclusion

In this paper, we have done a longitudinal analysis of TCP SYN flood attacks on Internet services between 2015 and 2019. Based on backscatter of SYN/ACKs and ICMP status code 3 messages, we are able to track the intensity of the attack as well as characterize how the targeted host fared with the incoming packet flood.

Although the majority of attack target will known ports such as HTTP or SSH, we find that these attacks are rarely successful. Instead, it is mostly user-hosted applications that are prone to collapse. Surprisingly, we find no clear difference into the resilience of services based on how they are hosted. Hosts providing service for a large number of domains – a typical shared hosting environment – are no more resilient than dedicated machines, and only a slight but not significant difference exists to machines unconnected to domain names, a typical home environment. We can trace this back to the fact that adversaries adjust their attack speed depending on the service connectivity: servers with many domains experience a larger attack volume than home hosting, meaning that in the end both types of deployment collapse comparatively equally.

Worrying is the fact that we observe a clear trend to higher attack volumes in every year of our 5 year study. Every year, not only peak volumes grow, but the entire spectrum of attacks gets more powerful. While services overall can digest larger incoming packet floods each year before falling down, these increases in service resilience do not keep pace with the increase in attack power, and we notice that year-by-year the time necessary for a TCP SYN flood to bring down an Internet host steadily decreases.

References

[1] "Kaspersky DDoS report." https://securelist.com/ddos-report-q2-2019/91934/.
[2] N. Blenn, V. Ghiette, and C. Doerr, "Quantifying the spectrum of denial-of-service attacks through internet backscatter," in *ARES*, 2017.
[3] E. G. Coffman Jr, Z. Ge, V. Misra, and D. Towsley, "Network resilience: exploring cascading failures within bgp," in *Allerton Conference on Communications, Computing and Control*, 2002.
[4] G. C. Moura, R. d. O. Schmidt, J. Heidemann, W. B. de Vries, M. Muller, L. Wei, and C. Hesselman, "Anycast vs. DDoS: Evaluating the November 2015 root DNS event," in *IMC*, 2016.
[5] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *TOCS*, vol. 24, no. 2, pp. 115–139, 2006.
[6] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS attacks: trends and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.
[7] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, "Internet background radiation revisited," in *IMC*, pp. 62–74, ACM, 2010.
[8] L. Krämer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, K. Yoshioka, and C. Rossow, "Amppot: Monitoring and defending against amplification ddos attacks," in *RAID*, pp. 615–636, Springer, 2015.
[9] C. Rossow, "Amplification hell: Revisiting network protocols for DDoS abuse," in *NDSS*, 2014.
[10] A. Noroozian, M. Korczyński, C. H. Gañan, D. Makita, K. Yoshioka, and M. van Eeten, "Who gets the boot? analyzing victimization by ddos-as-a-service," in *RAID*, pp. 368–389, Springer, 2016.
[11] 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 *IMC*, pp. 100–113, ACM, 2017.
[12] D. R. Thomas, R. Clayton, and A. R. Beresford, "1000 days of UDP amplification DDoS attacks," in *eCrime*, pp. 79–84, IEEE, 2017.
[13] J. Postel, "Rfc 792 - internet control message protocol," tech. rep., Internet Engineering Task Force, 1981.
[14] Retrieved from www.speedguide.net.
[15] "Global internet speed index." https://www.speedtest.net/global-index.
[16] S. Mansfield-Devine, "The growth and evolution of DDoS," *Network Security*, vol. 2015, no. 10, pp. 13 – 20, 2015.
[17] S. Mansfield-Devine, "DDoS: threats and mitigation," *Network Security*, vol. 2011, no. 12, pp. 5 – 12, 2011.
[18] "Netscout report." https://www.netscout.com/report/.
[19] V. Ghiette and C. Doerr, "How media reports trigger copycats: An analysis of the brewing of the largest packet storm to date," in *WTMC*, 2018.