DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown

Daniel Kopp
DE-CIX

Matthias Wichtlhuber
DE-CIX

Ingmar Poese
BENOCS

Jair Santanna
University of Twente

Oliver Hohlfeld
Brandenburg University of
Technology

Christoph Dietzel
DE-CIX / MPI for Informatics

ABSTRACT

Booter services continue to provide popular DDoS-as-a-service platforms and enable anyone irrespective of their technical ability, to execute DDoS attacks with devastating impact. Since booters are a serious threat to Internet operations and can cause significant financial and reputational damage, they also draw the attention of law enforcement agencies and related counter activities. In this paper, we investigate booter-based DDoS attacks in the wild and the impact of an FBI takedown targeting 15 booter websites in December 2018 from the perspective of a major IXP and two ISPs. We study and compare attack properties of multiple booter services by launching Gbps-level attacks against our own infrastructure. To understand spatial and temporal trends of the DDoS traffic originating from booters we scrutinize 5 months, worth of inter-domain traffic. We observe that the takedown only leads to a temporary reduction in attack traffic. Additionally, one booter was found to quickly continue operation by using a new domain for its website.

CCS CONCEPTS

• **Networks → Network measurement**; **Denial-of-service attacks**; • **Social and professional topics → Computer crime**;

KEYWORDS

DDoS; Booter; Stresser; DDos-for-Hire; Internet Security; ISP; IXP

1 INTRODUCTION

The DDoS threat. Known for at least two decades [15], Distributed Denial-of-Service (DDoS) attacks have become a major security threat to the continuous operation of the Internet [20, 51, 58]. Their goal is to disrupt services by consuming more critical resources than available, e.g., computing power or network bandwidth. Beyond the web, modern DDoS attacks can overwhelm cloud services [50] or congest backbone peering links [48]. The motivation for launching attacks ranges from financial [9, 53], to political [4, 35], cyber warfare [19, 54], smoke screen for other attack types [33], and even teenagers attacking their schools [47]. To scale, DDoS amplification attacks [42, 43] abuse protocol design (flaws)—e.g., NTP, DNS, SNMP, and Memcached [2, 14, 37, 42]—where a relatively small request can trigger a significantly larger response (up to ×50 000). Spoofed source IP addresses [5, 6, 34, 36] allow traffic to be reflected to the target [55]. Thus, attacks are increasing in size and sophistication [1]. A few years back, the largest reported attacks peaked just below 300 Gbps [39, 40], whereas DDoS attacks have now reached the Tbps level [3, 26, 37, 58].

Booters as DDoS tool. DDoS-as-a-service providers, also referred to as *booters* or *stressers*, provide a simple web interface and enable anyone to launch attacks [21, 22] at a low cost of just $0-$5 [10, 11]. On the other end of the scale, booters also claim to *offer* large-scale attacks for hundreds of USD [10].

Booter-related work. An extensive body of research on booters is available. These studies cover multiple lines of research including analyses of (1) the booters' leaked databases [10, 21, 23], (2) booter attacks [8, 24, 47, 57], (3) victims of booters [38], (4) honeypots of servers commonly used for performing booter attacks [25, 52], (5) the usage of these honeypots for attribution purposes [31], (6) TLS certificates used by booters [32], (7) booter blacklists and their origins [12, 44, 46, 59], (8) the usage of these blacklists to understand the booter market [45], (9) ethical and legal aspects related to booters [16, 18], and (10) the impact of law enforcement operations on booters from a commercial perspective [7, 13].

Our contribution. In this first of its kind study, we shed light on an FBI led operation of 15 booter domains in December 2018 [29, 56]. Instead of analyzing the effect of a financial intervention, we take an empirical perspective on the impact of this event on the DDoS attack traffic observed through the lens of three major networks: tier-1 and tier-2 ISPs, and a major IXP.

Our study takes as its starting point the use of four popular booters to attack ourselves. This self-attack provides an up-to-date picture of booter capabilities and is the first study to investigate premium (VIP) services and their promises. We derive characteristics of these self-attacks to further investigate tier-1 and tier-2 ISP and IXP network traffic for DDoS attacks. We study spatial and temporal trends and present the existence and extent of DDoS attacks. This provides an overview of the current DDoS threat landscape. Finally, our study focuses on network traffic in the time frame of

Daniel Kopp, Matthias Wichtlhuber, Ingmar Poese, Jair Santanna, Oliver Hohlfeld and Christoph Dietzel

the FBI takedown, by applying the characteristics we learn from our self-attack approach and the investigation of network traffic of our vantage points. In summary, our major contributions are:

- We investigate the anatomy of a booter attack by launching attacks against our infrastructure. We were able to observe high attack traffic volumes of up to 20 Gbps.
- We present an overview of the current Internet threat landscape through the lens of three major networks: tier-1 and tier-2 ISPs and a major IXP. We observe constant DDoS attacks, at thousands of victims and traffic rates of up to 600 Gbps.
- We seize the unique opportunity to study the effectiveness of an FBI takedown targeting 15 booter services in December 2018. The takedown immediately reduced the DDoS amplification traffic to reflectors. However, it did not have any significant effect on DDoS traffic hitting victims or on the number of attacks observed.

2 VANTAGE POINTS

Our study is based on three vantage points—a major IXP, a tier-1 ISP, and a tier-2 ISP—that provide a unique perspective on DDoS attack traffic in the wild. None of the data sets contain any payload. In addition, we perform active measurements of large sets of domains within an observatory [17] to identify booter websites.

Major IXP. Anonymized and sampled IPFIX traces captured at a major Internet Exchange Point (IXP) between Oct. 27, 2018 and Jan. 31, 2019 with 834B flows were made available to us.

Tier-1 ISP. We obtained Netflow traces from all border routers (ingress only) of a tier-1 ISP. IP addresses are anonymized and filtered by protocol and port, resulting in 6.6B flows records for the period of Dec. 12 to Dec. 30, 2018. The trace contains traffic to *i)* fixed-line end-users, *ii)* cellular customers, and *iii)* transit traffic. Traffic from end-users and customers was not included.

Tier-2 ISP. The second ISP dataset was anonymized and filtered in the same way as the tier-1 ISP. However, ingress and egress traffic is available in this data, meaning that end-user and customer sourced traffic is included. This results in 470M flow records from Sept. 27, 2018 to Feb. 2, 2019.

IXP Observatory. To study booter properties by performing self-attacks, we set up and operate an IXP-based DDoS observatory. It comprises a measurement AS operated by us that is connected to an IXP via a 10GE link. The AS interconnection consists of multilateral peerings at the IXP and a transit link over the same physical interface. Data collection is performed directly at the IXP platform (sampled) and at the measurement AS itself (unsampled).

DNS and HTTPS observatory. To study the rise and fall of booter websites, we use weekly crawls of all ~140M .com/.net/.org domains by obtaining zone files and performing weekly DNS resolutions and HTTPS website snapshots during January 2018 until May 2019. The website snapshots enable us to identify booter websites.

3 BOOTER: A VICTIM'S PERSPECTIVE

We start by taking a victim's perspective to study the potential damage that booter-based DDoS attacks can (a) directly cause to their target (thereby updating earlier findings on booter attack characteristics [8, 24, 47, 57]) and (b) the collateral damage to Internet infrastructure caused by carrying attack traffic. We do so by purchasing services from popular booters to attack our dedicated

Booter	Seized	Time	NTP	DNS	CLDAP	mcache	non-VIP	VIP
A	✓	Apr, Aug	✓	✓	✓	✓	**$8.00**	$250
B	✓	Jun-Sep	✓	✓	✓	✓	**$19.83**	**$178.84**
C		Apr-May	✓	✓			**$14.00**	$89
D		May	✓	✓			**$19.99**	$149.99

Table 1: Booters used to attack our measurement AS. Booter services used for self-attack in Section 3 indicated in bold.

measurement infrastructure at an IXP between April and September 2018. This provides us with a unique picture of *current* booter service capabilities in the wild, and answers the question: How much DDoS traffic they generate in light of powerful Tbps-level attacks? Our study provides the first look into the abilities of booter services, e.g. different service packages, attack protocols and attack volumes. We utilize the self-attacks to identify characteristics to later discover DDoS attack traffic at our vantage points and provide conclusions about the DDoS traffic landscape.

3.1 Self-Attack Approach

Selected booter services. We select 4 popular booters (see Table 1) from the booter blacklist [46] based on their Alexa website rank (booter names anonymized). Two of the selected booters (*A* & *B*) were later seized by the FBI-led takedown. Three are still in operation (seized booter *A* started using a new website after the takedown). We purchase paid services from all booters including cheaper (non-VIP) and one more expensive premium package (VIP) from booter *B*. We use all booter services to launch attacks against our measurement infrastructure. However, for the remainder of this section we only consider attacks with relevant traffic volumes. These are mostly NTP based amplification attacks, whereas also CLDAP, DNS, and Memcached-based attacks are offered.

Attacking our infrastructure. For our analysis, we passively capture all traffic of the measurement platform. In addition, we obtain sampled flow traces of the IXP for traffic directed to our server and are therefore able to measure attack traffic exceeding the capacity of 10 Gbps. The BGP router of our measurement platform announces a /24 IPv4 prefix and peers with a transit provider and all IXP customers in a multilateral peering configuration via the IXP's BGP reflector [41]. This provides us with a similar network setup compared to small to medium-sized organizations connected to the Internet. For each attack, we select a new IP from our /24 prefix to isolate individual measurements and to not confuse different attacks within our traffic captures. We perform a post mortem analysis of the passively measured attacks and derive the attack traffic volume and their network properties (e.g., number of servers used for reflection, number of ASes handing over traffic).

Ethical considerations. We perform controlled DDoS experiments towards our measurement platform. To comply with measurements ethics we (a) inform and synchronize with national authorities regarding legal/ethical implications of buying booter services, (b) minimize payments to booter services by limiting the number of different booters and offered service plans we buy (indicated in bold in Table 1), (c) inform and synchronize with the IXP operator and upstream provider about attacks, (d) take precaution that sufficient network bandwidth is available to minimize the impact on other
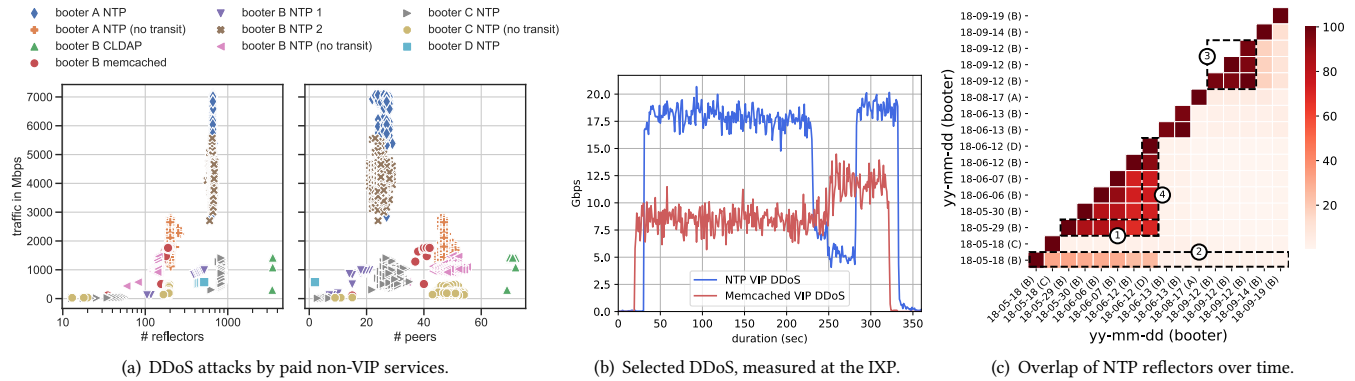
(a) DDoS attacks by paid non-VIP services.

(b) Selected DDoS, measured at the IXP.

(c) Overlap of NTP reflectors over time.

Figure 1: Measurements of Self-Attacks

IXP members, (e) use an experimental AS with no customer traffic, (f) utilize an unused /24 prefix that was allocated and announced only for the experiment, (g) are prepared to shut down the experimental AS and immediately stop attack traffic by withdrawing and blackholing the /24 in case of unexpected high traffic volumes or IXP members being negatively affected by our experiment (never occurred), and (h) minimize the experiment duration.

3.2 Self-Attack Observations

Attack traffic of non-VIP services. We show the results of 10 self-attacks on our measurement platform by non-VIP booter services in Figure 1(a). It depicts the received traffic volume per second (y-axis) for each attack. On the x-axis we display the number of observed reflectors (left plot) as well as with the number of neighboring ASes from which we receive the traffic (right plot). Each data point represents one second of a measurement. In terms of attack traffic volume, we find that during the attacks traffic levels of up to ~2000 Mbps are prevalent with a mean of 1440 Mbps but booters B and A peak at 7078 Mbps. These are the highest traffic levels reported during a non-VIP booter attack to date [47]. When we focus on the number of reflectors and peers from which the traffic is coming, we find that most booter attacks utilize between ~100 and ~1000 reflectors distributed over 20–55 peer ASes (avg. 346 and 27 respectively). However, when we instantiate booter B to use the connectionless LDAP (CLDAP) protocol the number of reflectors is 3519 distributed across 72 peer ASes. Thus, we learn that the protocol used for amplification affects the number of reflectors and IXP members transmitting traffic. Finally, we observe that NTP amplification attacks are the most potent attacks delivered by the booters included in our tests.

We next study how the attack traffic is handed over to our AS at the IXP, i.e., which fraction is received by transit and peering. To first study the maximum traffic that can be received via peering at the present IXP, we perform three attacks solely by using IXP peering and with *disabled transit* link (indicated as "no transit") in Figure 1(a). This enforces the usage of peering links even if the transit link would have been a better routing option. In this case, the number of individual IXP members (peers) sending traffic increases from below 30 to above 40 when the transit link is deactivated. While the handover traffic spreads over more peers, the absence the transit link limits the reachability of our AS. Consequently, we

receive less attack traffic, e.g., the NTP attack volume of booter A decreases from up to 7 Gbps to less than 3 Gbps (see Figure 1(a)). For NTP attacks with *enabled transit*, we receive most traffic through the transit link (avg. 80.81%) compared to the IXP peering (avg. 19.19%). Thus, the attack traffic volumes reported in Section 4 for the IXP will likely underestimate the true attack sizes as the traces do not contain the customers' transit links.

Attack traffic of VIP services. Booter services advertise higher priced premium services. For booter B, VIP offerings charge 178.84\$ compared to 19.83\$ and promise higher attack traffic rates of 80–100 Gbps instead of 8–12 Gbps for non-VIP services. We validate this claim and launch *two* VIP attacks from booter *B*. In Figure 1(b), we show that the NTP (blue line) and Memcached (red line) attacks generate traffic rates with a peak of about 20 Gbps and 10 Gbps, respectively (we configured both attacks to last for 5 min). The sudden drop in attack for the NTP traffic is due to a flapping BGP session with our transit provider due to the saturation of our measurement interface. Again, the majority of NTP traffic (80.81%) is delivered by our transit provider, the remaining 19.19% are received over the IXP peering. Interestingly, 45.55% of the IXP peering traffic (8.73% over all) is handed over by one AS while the median share per peer is 0.22%. Through the observations of the Memcached attack, we notice a shift of more traffic being transferred via the IXP peering (88.59%), while one member alone accounts for 33.58% of the total attack traffic. We assume that at this point in time this specific IXP member was exploited for Memcached amplification attacks. The observed traffic rates are significantly larger than the non-VIP booter attacks, but never reach the claimed bandwidth nor the advertised multiplication factors. Indeed, we experience only roughly 25% of the traffic rate compared to that which was advertised.

Amplification overlap. Next we study how the different booters are related and to what extent they share the same amplifiers. We focus on NTP amplification attacks and compare the sets of reflectors used for the attacks. Figure 1(c) depicts 16 independent self-attacks and the overlap of the NTP reflectors sorted by date. We find a stable set of reflectors for booter *B* with moderate churn of around 30% over a time frame of two weeks (1), which suddenly uses a new set of reflectors (for booter *B* from 18-06-12 to 18-06-13). We also observe a churning set of reflectors over a long period (2). The area number (3) shows same day measurements for one booter with a high overlap. This indicates a stability over short time frames
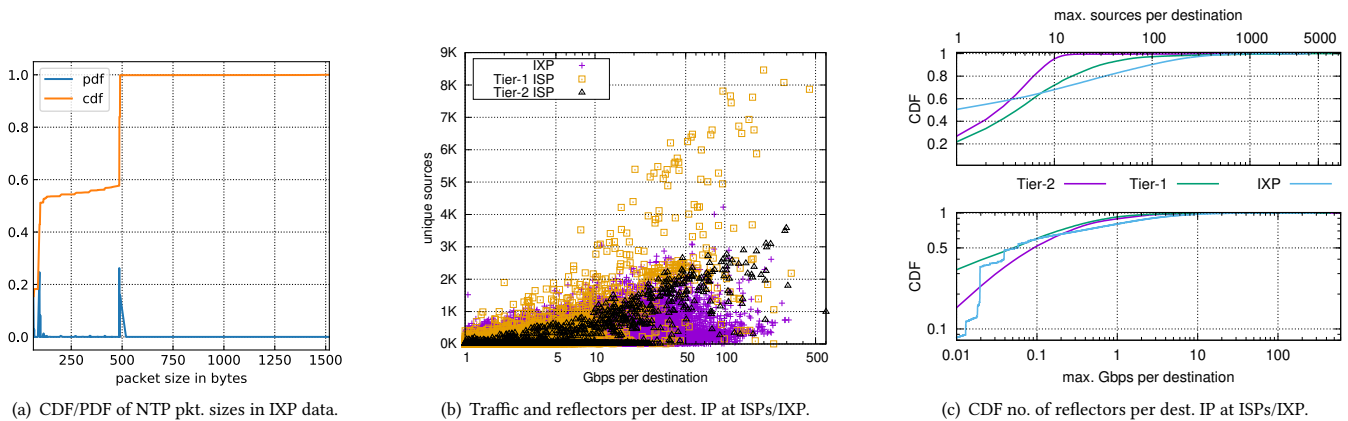
(a) CDF/PDF of NTP pkt. sizes in IXP data.

(b) Traffic and reflectors per dest. IP at ISPs/IXP.

(c) CDF no. of reflectors per dest. IP at ISPs/IXP.

Figure 2: Classification of NTP amplification attacks at ISPs and an IXP.

and allows us to conclude that this booter doesn't randomly select reflectors from a larger set of reflectors, but uses the same reflectors in this time frame. Moreover, reflectors occasionally overlap between booter services (4). Interestingly, the VIP and non-VIP services use the same set of reflectors. The difference in attack traffic is generated by a higher packet rate (5.3M pps compared to 2.2M pps). Noteworthy, the number of the reflectors used by booters is fairly low (in total 868) compared to the globally available set of potential amplifiers (e.g., 9M potentially usable NTP servers according to shodan.io on May 12 2019). From this analysis we conclude that identifying booter services by reflectors is difficult because the set of reflectors is overlapping between different booter services and a new set of reflectors is used suddenly. Ultimately, this makes it impossible to identify specific booter traffic at a later point in time by using the set of reflectors we learn from our self-attacks.

Takeaway. *Booters enable anyone to launch Gbps-scale DDoS for few dollars only. We measure higher attack volumes than previously reported (1.4 Gbps) [47], even with non VIP-services. We are the first to report the capabilities of a VIP booter services with attack traffic of up to 20 Gbps. These traffic volumes are sufficient to take down web services and significantly disturb the operation of inter-domain links and Internet infrastructure. We further find NTP-based amplification attacks to provide the most potent and reliable type of booter attacks. We believe this is because NTP amplifiers are more widespread and stable, while Memcached amplifiers focus on fewer networks, which in turn detect abuse more quickly and mitigate the problem.*

4 DDOS AMPLIFICATION TRAFFIC

Next, we study DDoS amplification traffic at our vantage points, i.e., a tier-1 & tier-2 ISP, and an IXP. We exclusively focus our discussion on NTP traffic, since most reliable booter-spawned attacks were executed over NTP. The following analysis highlights the prevalence of attack traffic at our vantage points and continues to define filtering criteria before we study the FBI takedown in the next section.

Basic NTP DDoS classification. In our self-attacks we observed amplified NTP packets to have a size of either 486 or 490 bytes (98.62% over all observed packets) due to monlist requests. To put this in context of a realistic NTP traffic mix, we show the distribution of NTP packet sizes at the IXP in Figure 2(a). We observe

an almost bimodal distribution of 54% of the NTP packets that are smaller than 200 bytes (likely benign traffic) and 46% that are larger (likely attack traffic). Thus, we define a threshold of 200 bytes as an optimistic classification criterion.

NTP amplification traffic in the wild. By applying our classification, we find 311*K* destinations (tier-1 ISP: 36*K*, tier-2 ISP: 95*K*, IXP: 244*K*) that receive NTP reflection traffic for the measurement time (see Section 2). We plot the destination IPs (victims) of the attack traffic in Figure 2(b). The plot shows the number of unique amplification sources (y-axis) and the max traffic level in Gbps over one minute (x-axis). The majority of traffic peaks (y-axis) are between 5 and 100 Gbps (avg. 2.64 Gbps). Notably, 224 victims receive more than 100 Gbps, 5 more than 300 Gbps of attack traffic—a single destination even up to 602 Gbps. Note that, as we learned in Section 3.2, attacks observed at the IXP can be significantly larger at the actual target.

Higher traffic rates often involve a higher number of amplifiers (sources): most destinations receive traffic from hundreds of amplifiers, some even from thousands (avg. 35). Outliers, particularly for the tier-1 ISP, receive traffic from up to ~8500 amplifiers.

We next study the max number of amplifiers per attack target (unique dest. IP) within one minute bins, shown as CDF in Figure 2(c) (top). Most targets receive traffic from less than 5 reflectors. For the tier-1 and the IXP about 70% receive traffic from less than 10. Interestingly, for the tier-2, 90% of the targets receive amplification NTP traffic from less than 10 amplifiers. For comparison, we depict the CDF of attack traffic peaks within one minute per target for all 3 data sets in Figure 2(c) (bottom). Only a fraction of 0.09 receives more than 1 Gbps peak traffic and at the IXP we see 158 targets receiving more than 100 Gbps. On the other hand, a majority of targets receive a negligible amount of traffic.

Extended NTP DDoS classification. We aim to identify NTP DDoS attacks with a low rate of false positives at the cost of false negatives. Thus, we extend our classification by excluding two more cases of false positives, the scanning or monitoring of NTP monlist [14] and the use of the NTP port by custom applications. Based on insights from our self-attacks in Section 3, we introduce two more filtering rules: (a) traffic to the target has to be larger than 1 Gbps and (b) has to originate from more than 10 amplifiers. Applying both rules reduces the number of NTP destinations by 78% ((a) 74%, (b) 59%). This results in a data set likely only containing NTP DDoS traffic.

Takeaway. *NTP-based DDoS traffic is prevalent at all three vantage points and can be classified using the proposed criteria. The observed attacks involve traffic rates of up to 600 Gbps—often generated by a large number of reflectors—during our observation period. The extent and size of DDoS attacks we observe raises the question of whether the takedown of booters has an effect on the attack traffic in general.*

5 FBI TAKEDOWN OF 15 BOOTERS

On December 19, 2018 the FBI seized the domains of 15 booter websites (e.g., critical-boot.com or quantumstress.net) [56]. All booters were tested by the FBI prior to the takedown and "the FBI determined that these types of services can and have caused disruptions of networks at all levels" [56]. Smaller seizures of single booter domains had occurred previously, e.g., the seizure of webstresser.org with more than 138k registered users by investigators in the U.S., U.K. and the Netherlands in 2018 [28]. Beyond domain seizures, booter users and operators can face legal actions [30], e.g., the operator of Titanium Stresser was sentenced to years in prison in 2017 [27]. Next we focus on studying the effects of the seizure on the overall DDoS attack traffic and take a first look on the domain ecosystem of booter websites.

5.1 Domain Perspective on Takedown

First, we take a control plane perspective on the available booter domains. We use weekly snapshots of all .com/.net/.org domains to identify booter websites by keyword matching following [46] (e.g., "booter", "stresser", "ddos-as-a-service"). This gives us an overview of booter domains before and after the takedown. We identified 58 booter .com/.net/.org domains by manually visiting and verifying each domain matching the keyword search. Using daily snapshots of the Alexa Top 1M list [49], we rank the identified booter domains by their median Alexa rank over each month, shown in Figure 3. Booter domains that were seized in December are highlighted. We observe the booter domains in the Alexa Top 1M to grow over time. Seized domains have a high Alexa rank but not the highest among all booter domains—notably they occasionally still appear in the top 1M list (likely as a result of press reports pointing to those domains). Thus, despite the seizure of 15 domains, many alternative booter sites exist. Following this, we select booter domains matching our keyword search after the takedown. In this way, we identified a new domain for the seized booter A that became active after the takedown and entered the global Alexa Top 1M list on December 22—just three days after the seizure of their old domain. The new domain was registered in June 2018 but remained unused until the takedown. Our account credentials registered with the seized domain still work with the new domain (at the time of this writing).

5.2 Traffic Perspective on Takedown

For studying any data plane effects of the recent FBI-led takedown in 2018 at our vantage points, we do a time series analysis of 122 days beginning at Sep. 30, 2018 and ending at Jan. 30, 2019, spanning the seizure of the domains on Dec. 19, 2018. We calculate the following metrics: (a) wt_{30}/wt_{40} a boolean metric indicating whether a one-tailed Welsh unequal variances test comparing the daily sum of packets 30/40 days before and 30/40 days after the takedown finds any significant difference at $p = 0.05$; (b) red_{30}/red_{40} a ratio
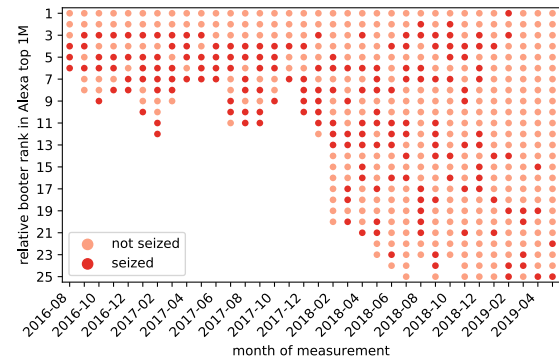

Figure 3: Booter domains in the Alexa Top 1M by rank.

of the daily average of sums of packets 30/40 days before and 30/40 days after the takedown. Using these metrics, we investigate any combination of suspicious protocol ports (NTP, Memcached, DNS, etc.) as source or destination port (to or from reflectors) for ingress and egress traffic. We start with a discussion of traffic *to* DDoS reflectors, as we found significant changes for this type of traffic.

Memcached traffic to reflectors. Memcached remains a popular attack vector due to its unsurpassed amplification factor. As Memcached is a AS-internal object caching daemon, it is not expected to appear in regular inter-domain traffic. Consequently, we assume that any UDP traffic with Memcached target port number 11211 is traffic flowing to a DDoS Memcached reflector and accept possible noise added by scanning or other applications using the port. We investigate the number of packets to Memcached reflectors for the IXP vantage point in Figure 4 (top). A statistically significant reduction can be found for the 30 day window (wt_{30}) as well as for the 40 day window (wt_{40}). The average daily number of packets after the takedown is 22.50% (red_{30}) and 27.72% (red_{40}) compared to before. A comparable and significant reduction was found for the tier-2 ISP as well (wt_{30}/wt_{40} =True, $red_{30} = 7.34\%$, $red_{40} = 4.99\%$).

NTP traffic to reflectors. NTP is a leading amplification vector due to the high number of open NTP reflectors. We compare traffic to NTP reflectors under the assumption that any traffic with UDP target port 123 is a spoofed packet for triggering an attack, i.e., including false negatives such as legitimate NTP requests. Even when accepting this unquantifiable amount of noise, we find significant reductions in traffic to NTP reflectors for the ISP vantage point (see 4, middle). After the seizure, the number of packets falls to 39.68% (red_30) and 26.97% (red_40) respectively. The same is true for the IXP vantage point (wt_{30}/wt_{40} =True, $red_{30} = 22.5\%$, $red_{40} = 27.72\%$).

DNS traffic to reflectors. Similar to NTP and Memcached, DNS is abused for DDoS as a reflector. However, separating the comparably large share of legitimate from illegitimate requests is difficult. Thus, our results for DNS request packets at the tier-2 ISP's vantage point (Fig. 4, bottom) are not as visually impressive as for other vectors. Nevertheless, we find a statistically significant reduction in traffic levels in both time windows (wt_{30}/wt_{40}). In the week after the seizure, DNS requests fall to a global minimum. The overall reduction is larger than 20% (red_{30}/red_{40}). No reduction could be found for the IXP vantage point.

No significant reduction in attack volumes or number of systems attacked. A surprising finding of this work is that we find significant reductions for traffic flowing *to* DDoS reflectors, but
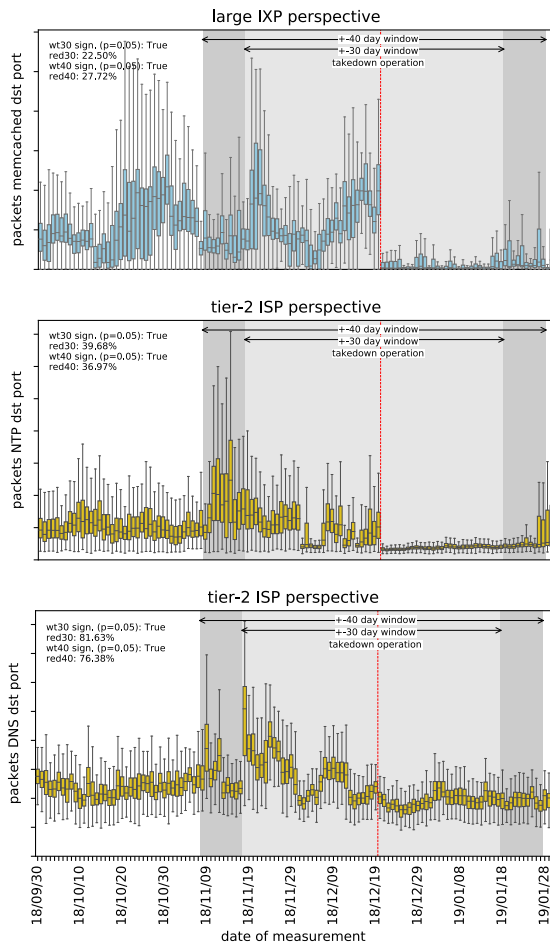
Daniel Kopp, Matthias Wichtlhuber, Ingmar Poese, Jair Santanna, Oliver Hohlfeld and Christoph Dietzel

Figure 4: Selected significant changes in traffic before and after the takedown; $wt30/wt40$**: significant lower packet counts at** $p = 0.05$ **when comparing 30/40 days before and after the takedown;** $red30/red40$**: ratio of daily mean 30/40 days before and 30/40 days after the takedown.**

no significant reduction in attack traffic *from* reflectors to victims, or in the number of systems attacked. In order to minimize the probability of false conclusions with respect to this finding, we use the knowledge of NTP DDoS traffic characteristics from Section 4 to compose a filter for the number of systems under attack (see Fig. 5). We isolate all IPs receiving NTP traffic with packets > 200 bytes packet size from more than 10 hosts with more than 1 Gbps traffic peak. We do not find a significant reduction in the number of systems attacked ($wt30/wt40$).

Takeaway. *The traffic patterns observed show a correlation with the FBI seizure. We find significant reductions in DDoS traffic to possible DNS, NTP, and Memcached reflectors after the takedown operation. Nevertheless, we could not find any significant reduction in traffic from reflectors to victims. To exclude false positives, we use our classification for NTP DDoS, which shows no significant reduction after the takedown in the systems attacked. We conclude that seizing the domains of booter websites does not improve the situation for DDoS victims, as the underlying infrastructure of reflectors remains online and can be utilized by third-parties without disruption.*
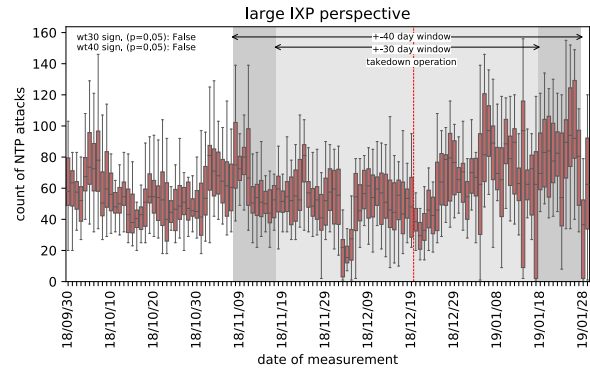

Figure 5: Systems under NTP DDoS attack per hour.

6 CONCLUSIONS

This paper studies for the first time the effect of booter-based DDoS attacks through the lens of a major IXP, a tier-1 ISP, and a tier-2 ISP—with a focus on the effects of an FBI-led takedown of 15 booter websites in Dec. 2018. By purchasing attacks against our own infrastructure from 4 popular booters, we study booter capabilities. The attack traffic levels generated by cheaper non-VIP services are considerably higher than reported in related work (avg. 1.4 Gbps) [47]. We are the first to report the capabilities of a premium (VIP) booter service that peaks at 20 Gbps while promising 60-80 Gbps. In our data sets, we observe NTP-based DDoS attack traffic to be prevalent at all three vantage points. The attacks observed involve substantial traffic rates of up to 600 Gbps. To study if booter takedowns of law enforcement agencies help to reduce the attack traffic, we analyze the effect of an FBI-led mass-seizure of 15 booter domains in Dec. 2018 on NTP, DNS, and Memcached-based DDoS attacks. We reveal that the takedown immediately had an effect on the DDoS amplification traffic especially towards reflectors. However, it did not have any significant effect on DDoS traffic hitting victims or on the number of attacks observed. This shows that seizing the seizing the domains of the booter websites is not enough as the underlying infrastructure of reflectors remains online and is utilized by third parties. Moreover, we found at least one booter to become active under a new domain shortly after the seizure, while the number of booter service domains in total increased over the measurement period despite the seizure. Our study aims to inform network operators to better understand the current threat-level, but also law enforcement agencies to recognize the need of additional efforts, e.g., to shut down open reflectors. Since our study is limited to technical parameters, the question arises whether this is sufficient to assess the health of the booter ecosystem. This motivates the need to better study the effects of law enforcement on the booter economy, e.g., on infrastructures, financing, or involved entities.

ACKNOWLEDGMENTS

REFERENCES

[1] AKAMAI. State of the Internet Security Report (Q4 2017). https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf, 2017.

[2] AKAMAI. State of the Internet Security Report (Attack Spotlight: Memcached). https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-attack-spotlight.pdf, 2018.

[3] ANTONAKAKIS, M., APRIL, T., BAILEY, M., BERNHARD, M., BURSZTEIN, E., COCHRAN, J., DURUMERIC, Z., HALDERMAN, J. A., INVERNIZZI, L., KALLITSIS, M., KUMAR, D., LEVER, C., MA, Z., MASON, J., MENSCHER, D., SEAMAN, C., SULLIVAN, N., THOMAS, K., AND ZHOU, Y. Understanding the Mirai Botnet. *USENIX Security Symposium* (2017).

[4] BBC. 'Hacking attacks' hit Russian political sites. http://www.bbc.com/news/technology-16032402, 2012.

[5] BEVERLY, R., AND BAUER, S. The spoofer project: Inferring the extent of internet source address filtering on the internet. In *Steps to Reducing Unwanted Traffic on the Internet Workshop, SRUTI'05, Cambridge, MA, USA, July 7, 2005* (2005).

[6] BEVERLY, R., BERGER, A., HYUN, Y., AND CLAFFY, K. Understanding the Efficacy of Deployed Internet Source Address Validation Filtering. In *Internet Measurement Conference (IMC)* (Nov 2009).

[7] BRUNT, R., PANDEY, P., AND MCCOY, D. Booted: An analysis of a payment intervention on a DDoS-for-Hire-Service. In *Workshop on the Economics of Information Security* (2017).

[8] BUKAC, V., STAVOVA, V., NEMEC, L., RIHA, Z., AND MATYAS, V. Service in denial—clouds going with the winds. In *International Conference on Network and System Security* (2015).

[9] BÜSCHER, A., AND HOLZ, T. Tracking DDoS Attacks: Insights into the Business of Disrupting the Web. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats* (2012).

[10] CARDOSO DE SANTANNA, J., DURBAN, R., SPEROTTO, A., AND PRAS, A. Inside Booters: an analysis on operational databases. In *IFIP/IEEE International Symposium on Integrated Network Management* (2015).

[11] CARDOSO DE SANTANNA, J., AND SPEROTTO, A. Characterizing and Mitigating the DDoS-as-a-Service Phenomenon. In *AIMS* (2014).

[12] CHROMIK, J., CARDOSO DE SANTANNA, J., SPEROTTO, A., AND PRAS, A. Booter websites characterization: Towards a list of threats. In *Brazilian Symposium on Computer Networks and Distributed Systems* (2015).

[13] COLLIER, B., THOMAS, D. R., CLAYTON, R., AND HUTCHINGS, A. Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks. In *IMC* (2019).

[14] CZYZ, J., KALLITSIS, M., GHARAIBEH, M., PAPADOPOULOS, C., BAILEY, M., AND KARIR, M. Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. In *ACM IMC* (2014).

[15] DITTRICH, D. The DoS Project's 'trinoo' distributed denial of service attack tool. https://staff.washington.edu/dittrich/misc/trinoo.analysis, 1999.

[16] DOUGLAS, D., SANTANNA, J., SCHMIDT, R., GRANVILLE, L., AND PRAS, A. Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire? *Journal of Information, Communication and Ethics in Society 15*, 01 (2017).

[17] HOHLFELD, O. Operating a DNS-based active internet observatory. In *ACM SIGCOMM Poster* (2018).

[18] HUTCHINGS, A., AND CLAYTON, R. Exploring the provision of online booter services. *Deviant Behavior 37*, 10 (2016).

[19] INTERFAX-UKRAINE. Poroshenko reports on DDoS-attacks on Ukrainian CEC from Russia on Feb. 24-25. https://www.kyivpost.com/ukraine-politics/poroshenko-reports-on-ddos-attacks-on-ukrainian-cec-from-russia-on-feb-24-25.html, 2019.

[20] JONKER, M., KING, A., KRUPP, J., ROSSOW, C., SPEROTTO, A., AND DAINOTTI, A. Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. In *ACM IMC* (2017).

[21] KARAMI, M., AND MCCOY, D. Rent to Pwn: Analyzing Commodity Booter DDoS Services. In *USENIX* (2013).

[22] KARAMI, M., AND MCCOY, D. Understanding the Emerging Threat of DDoS-as-a-service. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats* (2013).

[23] KARAMI, M., AND MCCOY, D. Understanding the emerging threat of ddos-as-a-service. In *LEET* (2013).

[24] KARAMI, M., PARK, Y., AND MCCOY, D. Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services. In *WWW* (2016).

[25] KRÄMER, L., KRUPP, J., MAKITA, D., NISHIZOE, T., KOIDE, T., YOSHIOKA, K., AND ROSSOW, C. AmpPot: Monitoring and Defending Against Amplification DDoS Attacks. In *International Workshop on Recent Advances in Intrusion Detection (RAID)* (2015), Springer, pp. 615–636.

[26] KREBS, B. KrebsOnSecurity Hit With Record DDoS. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos, 2016.

[27] KREBS, B. UK Man Gets Two Years in Jail for Running 'Titanium Stresser' Attack-for-Hire Service. https://krebsonsecurity.com/2017/04/uk-man-gets-two-years-in-jail-for-running-titanium-stresser-attack-for-hire-service/, 2017.

[28] KREBS, B. DDoS-for-Hire Service Webstresser Dismantled. https://krebsonsecurity.com/2018/04/ddos-for-hire-service-webstresser-dismantled/, 2018.

[29] KREBS, B. Feds Charge Three in Mass Seizure of Attack-for-hire Services. https://krebsonsecurity.com/2018/12/feds-charge-three-in-mass-seizure-of-attack-for-hire-services/, 2018.

[30] KREBS, B. 250 Webstresser Users to Face Legal Action. https://krebsonsecurity.com/2019/02/250-webstresser-users-to-face-legal-action/, 2019.

[31] KRUPP, J., KARAMI, M., ROSSOW, C., MCCOY, D., AND BACKES, M. Linking amplification DDoS attacks to booter services. In *International Symposium on Research in Attacks, Intrusions, and Defenses* (2017).

[32] KUHNERT, B., STEINBERGER, J., BAIER, H., SPEROTTO, A., AND PRAS, A. Booters and Certificates: An Overview of TLS in the DDoS-as-a-Service Landscape. In *2nd International Conference on Advances in Computation, Communications and Services, ACCSE* (2017).

[33] LAB, K. Research reveals hacker tactics: Cybercriminals use ddos as smokescreen for other attacks on business. https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business, 2016.

[34] LICHTBLAU, F., STREIBELT, F., KRÜGER, T., RICHTER, P., AND FELDMANN, A. Detection, Classification, and Analysis of Inter-domain Traffic with Spoofed Source IP Addresses. In *ACM IMC* (2017).

[35] MOHAMED, J. Daily Mirror: Hackers attack the Stock Exchange: Cyber criminals take down website for more than two hours as part of protest against world's banks. http://www.dailymail.co.uk/news/article-3625656/Hackers-attack-Stock-Exchange-Cyber-criminals-website-two-hours-protest-against-world-s-banks.html, 2016.

[36] MOORE, D., VOELKER, G., AND SAVAGE, S. Inferring Internet Denial-of-Service Activity. In *USENIX Security Symposium* (Washington, D.C., Aug 2001).

[37] MORALES, C. NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us. https://asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/, 2018.

[38] NOROOZIAN, A., KORCZYŃSKI, M., GAÑAN, C., MAKITA, D., YOSHIOKA, K., AND VAN EETEN, M. Who gets the boot? Analyzing victimization by DDoS-as-a-Service. In *International Symposium on Research in Attacks, Intrusions, and Defenses* (2016), Springer.

[39] PRINCE, M. The DDoS That Knocked Spamhaus Offline (And How We Mitigated It). https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/, 2013.

[40] PRINCE, M. Technical Details Behind a 400Gbps NTP Amplification DDoS Attack. https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/, 2014.

[41] RICHTER, P., SMARAGDAKIS, G., FELDMANN, A., CHATZIS, N., BOETTGER, J., AND WILLINGER, W. Peering at Peerings: On the Role of IXP Route Servers. In *ACM IMC* (2014).

[42] ROSSOW, C. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. *NDSS* (2014).

[43] RYBA, F. J., ORLINSKI, M., WÄHLISCH, M., ROSSOW, C., AND SCHMIDT, T. C. Amplification and DRDoS Attack Defense–A Survey and New Perspectives. *arXiv preprint arXiv:1505.07892* (2015).

[44] SANTANNA, J., DE VRIES, J., DE O. SCHMIDT, R., TUNCER, D., Z. GRANVILLE, L., AND PRAS, A. Booter list generation: The basis for investigating DDoS-for-hire websites. *International journal of network management 28* (Jan 2018).

[45] SANTANNA, J., SCHMIDT, R., TUNCER, D., SPEROTTO, A., GRANVILLE, L., AND PRAS, A. Quiet dogs can bite: Which booters should we go after, and what are our mitigation options? *IEEE Communications Magazine 55*, 7 (2017).

[46] SANTANNA, J. J., D. O. SCHMIDT, R., TUNCER, D., DE VRIES, J., GRANVILLE, L. Z., AND PRAS, A. Booter blacklist: Unveiling DDoS-for-hire websites. In *International Conference on Network and Service Management (CNSM)* (2016).

[47] SANTANNA, J. J., VAN RIJSWIJK-DEIJ, R., HOFSTEDE, R., SPEROTTO, A., WIERBOSCH, M., GRANVILLE, L. Z., AND PRAS, A. Booters – An analysis of DDoS-as-a-service Attacks. *IFIP/IEEE International Symposium on Integrated Network Management* (2015).

[48] SC MEDIA UK. OVH suffers 1.1Tbps DDoS attack. https://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/532197/, 2016.

[49] SCHEITLE, Q., HOHLFELD, O., GAMBA, J., JELTEN, J., ZIMMERMANN, T., STROWES, S. D., AND VALLINA-RODRIGUEZ, N. A long way to the top: Significance, structure, and stability of internet top lists. In *ACM IMC* (2018).

[50] SIPGATE. The Sipgate DDoS Story. https://medium.com/@sipgate/ddos-attacke-auf-sipgate-a7d18bf08c03, 2014.

[51] TECHNOLOGIES, A. 2018 State of the Internet / Security: A Year in Review. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/2018-state-of-the-internet-security-a-year-in-review.pdf, 2018.

[52] THOMAS, D. R., CLAYTON, R., AND BERESFORD, A. R. 1000 days of UDP amplification DDoS attacks. In *APWG Symposium on Electronic Crime Research (eCrime)* (2017), IEEE, pp. 79–84.

[53] Times, N. Y. Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool. https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html, 2017.

[54] Traynor, I. Russia accused of unleashing cyberwar to disable Estonia. https://www.theguardian.com/world/2007/may/17/topstories3.russia, 2007.

[55] US-CERT. UDP-Based Amplification Attacks. https://www.us-cert.gov/ncas/alerts/TA14-017A, 2018.

[56] US Department of Justice. Criminal Charges Filed in Los Angeles and Alaska in Conjunction with Seizures Of 15 Websites Offering DDoS-For-Hire Services. https://www.justice.gov/opa/pr/criminal-charges-filed-los-angeles-and-alaska-conjunction-seizures-15-websites-offering-ddos, 2018.

[57] Zand, A., Modelo-Howard, G., Tongaonkar, A., Lee, S., Kruegel, C., and Vigna, G. Demystifying DDoS as a Service. *IEEE Communications Magazine 55*, 7 (2017).

[58] ZDNet. GitHub hit with the largest DDoS attack ever seen. https://www.zdnet.com/article/github-was-hit-with-the-largest-ddos-attack-ever-seen/, 2018.

[59] Zhang, W., Bai, X., Chen, C., and Chen, Z. Booter Blacklist Generation Based on Content Characteristics. In *International Conference on Collaborative Computing: Networking, Applications and Worksharing* (2018), Springer.