Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services

Mohammad Karami
George Mason University
mkarami@gmu.edu

Youngsam Park
University of Maryland, College Park
yspark@cs.umd.edu

Damon McCoy
New York University
mccoy@nyu.edu

ABSTRACT

DDoS-for-hire services, also known as *booters*, have commoditized DDoS attacks and enabled abusive subscribers of these services to cheaply extort, harass and intimidate businesses and people by taking them offline. However, due to the underground nature of these booters, little is known about their underlying technical and business structure. In this paper, we empirically measure many facets of their technical and payment infrastructure. We also perform an analysis of leaked and scraped data from three major booters—Asylum Stresser, Lizard Stresser and VDO—which provides us with an in-depth view of their customers and victims. Finally, we conduct a large-scale payment intervention in collaboration with PayPal and evaluate its effectiveness as a deterrent to their operations. Based on our analysis, we show that these booters are responsible for hundreds of thousands of DDoS attacks and identify potentially promising methods to undermine these services by increasing their costs of operation.

1. INTRODUCTION

Distributed Denial-of-Service (DDoS) attacks are becoming a growing threat with high profile DDoS attacks at the end of 2014 disrupting many large scale gaming services, such as Microsoft's XBox Live and Sony's PlayStation networks [4]. These attacks were later claimed to be launched by the Lizard Squad as advertisements for their new DDoS-for-hire service called *Lizard Stresser* [3].

There is a long line of technical work exploring how to detect and mitigate these types of attacks [11, 12, 16, 22, 23, 25, 26, 36].

However, a large amount of DDoS attacks are being launched by relatively unsophisticated attackers that have purchased subscriptions to low-cost DDoS-for-hire (commonly called booter) services. These services are operated by profit-motivated adversaries that can scale up their DDoS infrastructure to meet the increasing demand for DDoS attacks. Despite the threat they pose, little is known about the structures of these booters.

Prior works have pointed out that understanding attackers dependencies on other support services [31] and potential chokepoints [7] in their operations could be useful for understanding how to more effectively undermine them. In this paper, we undertake a large scale measurement study of booter services to understand how they are structured both technologically and economically with the focus of isolating potential weaknesses. We explore booters from three different angles including analysis of leaked and scraped data, measurements of their attack infrastructure and a payment intervention.

Our analysis of leaked and scraped data from three booters—Asylum Stresser, Lizard Stresser and VDO [1]—demonstrates that these services have attracted over 6,000 paid subscribers that have launched over 600,000 attacks. We also find that the majority of booter customers prefer paying via PayPal and that Lizard Stresser, which only accepted Bitcoin, had a minuscule 2% sign-up to paid subscriber conversion rate compared to 15% for Asylum Stresser and 23% for VDO, which both accepted PayPal. By analyzing attack traffic directed at our own servers we are able to characterize the set of amplifiers they use to direct large amounts of traffic at their victims. In order to measure the resilience of their payment infrastructure, we conduct a payment intervention in collaboration with PayPal and the FBI. Our evaluation of the effectiveness of this approach suggests that it is a promising method for reducing the subscriber base of booters.

The rest of the paper is structured as follows. In Section 2, we provide a background on booter services and explain the ethical framework for our study. Section 3 presents related work and Section 4 presents our analysis of leaked and scraped data from three booter services. Next, we present measurements of their attack infrastructure in Section 5. In Section 6, we present our analysis of a payment intervention that resulted in disrupting revenue to several booters. Finally, we present a higher level discussion of our analysis in Section 7 and concluding remarks in Section 8.

WWW 2016, April 11–15, 2016, Montréal, Québec, Canada.
ACM 978-1-4503-4143-1/16/04.
http://dx.doi.org/10.1145/2872427.2883004.

[1]We assign each booter service a unique three letter code based on their domain name to avoid unintentionally advertising their services. The two exceptions are Asylum Stresser, which ceased operation before our study and Lizard Stresser, which has already been highly publicized.

2. BACKGROUND

In this section we explain the high level business and technical structure of booter services as well as the underlining ethical framework for our measurements.

2.1 Booter Services

Booter services have existed since at least 2005 and primarily operate using a subscription-based business model. As part of this subscription model, customers or subscribers [2] can launch an unlimited number of attacks that have a duration typically ranging from 30 seconds to 1-3 hours and are limited to 1-4 concurrent attacks depending on the tier of subscription purchased. The price for a subscription normally ranges from $10-$300 USD per month depending on the duration and number of concurrent attacks provided. These services claim that they are only to be used by network operators to stress test their infrastructure. However, they have become synonymous with DDoS-for-hire.

These services can be found by visiting underground forums where they advertise and by web searches for terms, such as "stresser" and "booter." The services are all in English; we did not find any evidence of similar services focused on other markets, such as Asia or Russia. They maintain frontend sites that allow their customers to purchase subscriptions and launch attacks using simple web forms. Their backend infrastructure commonly consists of databases that maintain subscriber information, and lists of misconfigured hosts that can be used for DDoS amplification. Rather than using botnets, most booter services rent high-bandwidth Virtual Private Servers (VPS) as part of their attack infrastructure. Ironically, booter services depend on DDoS-protection services, such as CloudFlare, to protect their frontend and attack infrastructure from attacks launched by rival competing booter services.

Figure 1 provides a detailed illustration of the infrastructure and process of using a booter service. (①) The customer first locates a booter site and visits their frontend webserver, which is normally protected by CloudFlare. (②) The customer must next purchase a subscription using a payment method, such as Bitcoin or PayPal. (③) The customer then uses the frontend interface to request a DDoS attack against a victim. (④) This request is forwarded from the frontend server to one of the backend attack servers. (⑤) The backend server then sends spoofed request packets to a set of previously identified misconfigured amplification servers. (⑥) Finally, DDoS traffic in the form of replies is sent to the victim from the amplification servers.

2.2 Ethical Framework

As part of the ethical framework for our study, we consulted with our institution's general counsel and placed restrictions on the types of booter services we actively interacted with along with what we included in this paper. First, we did not engage with any DDoS service that advertised using botnets and ceased active engagement with any booter that we realized was using botnets. For example, in the case of Lizard Stresser, when we became aware that a botnet was being used, we immediately abandoned plans to collect active attack measurements from this service and restricted ourselves to passive measurements. Our victim server was connected by a dedicated 1 Gbs network connection that was not shared with any other servers. We also obtained consent from our ISP and their upstream peering points before conducting any DDoS attack experiments. We also minimized the attack durations, notified our ISP before launching any attack and had a protocol in place to end an attack early if it caused a disruption at our ISP.

[2]We use these two terms interchangeably in this paper.

Type	Avg # of requests	Avg bandwidth
CHARGEN	22.76 (s)	564.56 (kbps)
NTP	1.07 (s)	231.43 (kbps)
DNS	0.71 (s)	12.71 (kbps)
SSDP	0.18 (s)	3.89 (kpbs)

Table 1: *Average number of requests per second and average bandwidth consumed in kbps for each amplifier.*

There were no other methods for us to obtain measurements of their attack infrastructure, such as the set of amplifiers used and rate of usage, except for launching attacks. Our method did create some harm to amplifiers and their upstream peering points by consuming bandwidth resources which we quantify in Table 1. The largest amount of bandwidth consumed was 564.56 kbps for CHARGEN amplifiers and the least was 3.89 kbps for SSDP amplifiers. Over the course of our experiments we did not receive any complaints from the operators of these amplifiers. Based on our analysis, longer 1 hour attacks only discovered about 20% additional amplifiers over a one minute attack. Given this, we would recommend shorter one minute attacks for future self-attack based experiments to further minimize bandwidth consumed when measuring booters' attack infrastructure.

In order to profile the attack infrastructure used by booters and gain insights into how they operate we had to purchase subscriptions. When purchasing a subscription for a booter service, we selected the cheapest option to minimize the amount of money given to these services. In total, we spent less than $140 and no individual booter service received more than $19 in payments as part of the measurements in this study. Payments were made primarily using PayPal and we assumed that proper controls were put in place at PayPal to mitigate the risk of money flowing to criminal groups. Also, the 9 booters that overlapped with our payment intervention study likely lost larger sums of money due to our reporting of their PayPal accounts than we paid to them. As part of our design methodology, we minimized the amount of money paid and targeted a small set of booters to obtain valuable measures of their attack infrastructure.

We received an exemption from our Institutional Review Board (IRB), since our study did not include any personally identifiable information and was based on publicly leaked data and scraped data that was publicly accessible. The leaked data contained usernames that did not identify the true names of subscribers, email addresses that again did not directly reveal the real identify of subscribers, and the IP addresses of subscribers used to login into the service. We did not include any raw data from these leaks or scrapes and we made no attempts to link this information to the real identities of subscribers. The leaks and scrapes also contained victim's IP addresses. Again, we did not include any raw victim's IP addresses and we did not mention any victims directly in the paper. When dealing with publicly leaked and scraped data, our protocol was to create no ad-

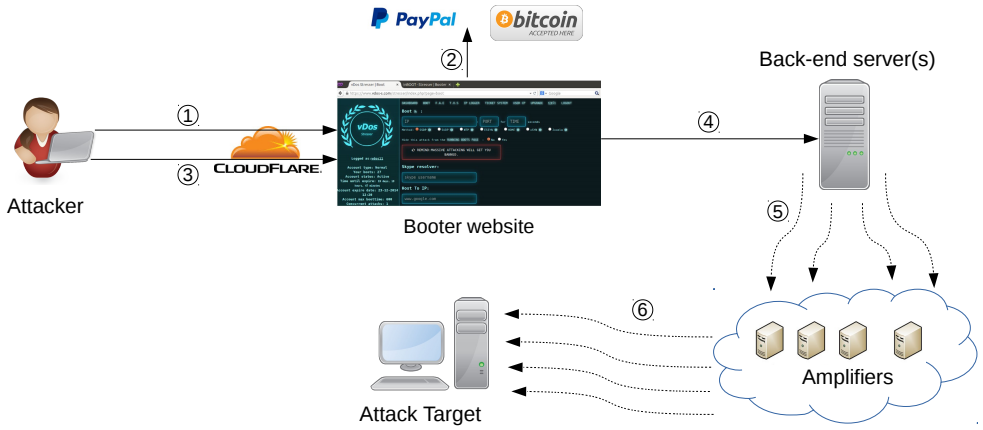

Figure 1: *Structure of booter services.*

ditional harm from our analysis or what we included in the paper.

3. RELATED WORK

DDoS attack and defense techniques have been studied for close to two decades [11, 12, 16, 22, 23, 25, 26, 36]. There have also been several empirical studies of DDoS attacks in the wild using backscatter analysis [20] which were revisited by Wustrow *et al.* [35]. More recent studies have measured Network Time Protocol (NTP) based DDoS attacks [9] and conducted broader measurements of UDP amplifiers along with introducing methods to identify spoofing-enabled networks [15].

Other studies have explored the structure of botnet based DDoS attacks [5] and malware [8, 30]. However, the closest related work to ours in this vein is by Welzel *et al.* which monitored the impact of DDoS attacks on victims [34] and an analysis of a leaked database from a single booter service done by Karami and McCoy [14]. Our work differs from this previous work in that we are focused on holistically understanding the stakeholders and infrastructure these booter services rely on to operate across a larger set of booter services.

Our study is in the same vein as prior work that views security problems through an economic lens [21]. We set out to understand the stakeholders and infrastructure of criminal DDoS-for-hire enterprises as has been done in other domains. Since booters are a criminal support service rather than the previously studied domain of abusive advertising [17, 19, 33] , they operate under a different set of constraints. In this respect our work is more along the lines of studies focused on criminal support services, such as email spam delivery [13, 28], fake social links [29] and fake account creation [32].

In Section 4, we show that even though booter services are criminal-to-criminal enterprises their payment methods more closely resemble those of consumer-to-criminal. Using a methodology similar to that presented by Clayton *et al.* [7], we show that there is a concentration of booters that accept payments using PayPal. This indicates that the *follow-the-money* and payment intervention approach which has been demonstrated to be effective in previous studies [18] might be at least partially effective at undermining booter services.

The largest contribution of our study is in characterizing the ecosystem of subscription-based booter services, which has not been studied in much depth. We show that these booters are structured differently than traditional botnet based DDoS services that are rented for a fixed time period in terms of the underlying attack infrastructure, customer base, business model and payment methods. We believe that our findings enable a better understanding of the effectiveness of ongoing efforts to disrupt their attack infrastructure at the amplifier and hosting level. We also offer a detailed analysis of the nature of these services, how they are structured and a preliminary evaluation of the potential effectiveness of a payment intervention.

4. INSIDE VIEW OF BOOTERS

In this section, we analyze publicly leaked backend booter databases and scraped data. From this analysis we present some numbers to better understand the dynamics and scale of booter services. This includes, the amount of revenue generated, the number of users, the number of victims and the number of attacks initiated by the subscribers of these services.

4.1 Data Sets

Our datasets for this section are comprised of two leaked backend databases for Asylum and Lizard Stresser and scraped data from VDO. A summary of these data sets is included in Table 2. Before presenting our analysis, we will first describe each of these data sets in more detail.

VDO Scraped Data. At the time we started monitoring *VDO* to measure the scale of its operation in early December 2014, it was one of the top booter services on underground forums with a high rate of positive reviews. During an 8 weeks period ending in early February 2015, we crawled this booter on 10-minutes intervals to collect data on users of the service and details of attacks launched by them. We found *VDO* to be unique in reporting a wealth of public data on its users and their attack details. This data includes a list of users logged into the service in the last 15 minutes where paid subscribers were distinguished from unpaid users. Also, the booter displayed a list of all currently running attacks and their details including the attack type, target, and duration. Users were able to optionally choose to remain anony-

Booter	Period	All Users	Subscribers	Revenue	Attacks	Targets
Asylum Stresser	10/2011-3/2013	26,075	3,963	$35,381.54	483,373	142,473
Lizard Stresser	12/2014-01/2015	12,935	176	$3,368 †	15,998	3,907
VDO‡	12/2014-2/2015	11,975	2,779	$52,773*	138,010	38,539
Total	-	50,985	6,918	$91,522.54	637,381	184,919

Table 2: *Summary of Asylum Stresser and Lizard Stesser leaked databases and scraped VDO reported data. † Revenue was converted from bitcoin to USD. *Revenue is estimated based on subscription cost and number of paying subscribers. ‡ Domain name is abbreviated to the first three characters.*

mous when logging into the service and hide the IP address or URL of the target when initiating an attack. However, the default option was for all the information to be public and we found only less than 30% of scraped login records to be anonymous and the target was hidden for 39% of all the attack instances we observed during the 8 weeks monitoring period.

While we cannot fully vet this self-reported data, we did verify that the data representing our actions were reported accurately. We also validated that all NTP attacks reported for a day were accurate by sending monlist requests in 10-minute intervals to a set of 12 NTP amplifiers known to be abused by *VDO* and recorded the received responses. A total of 44 distinct victims were the target of NTP attacks as reported by *VDO* during that 24 hour time period and we were able to find matching records for all 44 targets in the monlist responses collected from the set of monitored NTP servers. This gives us some increased level of confidence that the details of reported attacks and users are accurate.

Asylum Stresser Backend Database. Asylum Stresser was an established booter that was in operation for over two years before their backend database — containing 18 months of operational data that included user registrations, payments and attack logs — was publicly leaked. It ceased operation shortly after the leak and has not resumed operation. This leaked database has been vetted by many members of the anti-DDoS community that located their own test accounts in the user registration data and is believed to be authentic.

Lizard Stresser Backend Database. Lizard Stresser was launched in late December of 2014 by individuals calling themselves the *Lizard Squad*. This same group was responsible for DDoS attacks on Sony PlayStation and Microsoft Xbox networks on December 25, 2014. Their backend database covering their first two weeks of operation that included user registrations, payments and attack logs was publicly leaked. For this database, since all payments were in bitcoin and the wallet addresses are included, we have validated that this part of the database is accurate. We have also checked for internal consistency within these leaked databases. While we cannot rule out that some of the data has been fabricated, it would take a fair amount of resources to create this high fidelity of a forgery.

4.2 Subscribers

We find that 15% of Asylum users and 23% of all VDO users purchased a subscription, compared to less than 2% of all Lizard Stresser users [3]. This might be attributed to the fact that Asylum and VDO both accepted PayPal payments at least sporadically while Lizard Stresser only accepted Bitcoin as a payment method. It is difficult to attribute why the conversion rate of registered users to subscribers is much less for Lizard Stresser, since other factors, such as the media coverage, might have also driven many users to sign up out of curiosity. The Lizard Stresser's leaked database contains a total of 225 user support tickets. Out of these, 42 are related to user requests for purchasing subscriptions using PayPal. As one potential attacker wrote, "I want to pay via paypal real bad I'm a huge fan of and want to buy this ASAP but I don't have bitcoins."

[3]Note that Lizard Stresser did not offer free trial accounts.

4.3 Revenue

Asylum collected 99.4% ($35,180.14) of their revenue through PayPal payments and only 0.6% ($201.40) of their revenue was collected using their secondary payment method of MoneyBookers. Lizard Stresser collected all their revenue through their only supported payment method of Bitcoin and VDO accepted both PayPal and Bitcoin. They are presumably profitable, but these individual booters do not generate the profits required to pay the upfront capital, fees and potential fines for dedicated credit card merchant processing accounts. This amounted to around $25-$50K per an account, as was the case with illicit pharmaceutical and fake antivirus groups that had revenues on the order of millions of USD dollars a month [19, 27].

4.4 Attacks

From the leaked data we find that these three booters were responsible for over half a million separate attacks against over 100,000 distinct IP addresses. While the average attack from VDO only lasted 27 minutes, this data demonstrates the large-scale abuse problems and unwanted traffic generated by these services. Our analysis of victims finds that they are predominantly residential links and gaming-related servers, with a small number of higher profile victims, such as government, media and law enforcement sites. This matches previous analysis of victims from leaked databases [14]. For VDO our scraped data included the type of DDoS attack launched and our analysis of this data shows that amplified attacks, where the adversary attempts to exhaust the bandwidth capacity of the victim's connection, accounted for 72% of all attacks launch from VDO. The next most popular class of attacks were SYN flooding attacks, which made up only 16% of all attacks.

5. ATTACK INFRASTRUCTURE

Our measurements of booters' attack infrastructure are based on engaging with these services to understand what techniques and hosts are being actively used for attacks. Using this information might better inform defenders as to which ISPs and hosts to focus on for blacklisting, remediation and notification efforts. Our analysis of frontend servers finds a reliance on CloudFlare to protect booter's infrastructure from takedown and DDoS. In addition, we find that booters gravitate to using more stable amplifier infrastruc-

ture when possible. This differs from previous studies that scan the Internet for the vulnerable populations of misconfigured amplification servers many of which might be transient and not be used for DDoS attacks. We also identify two hosting providers connected to the same ISP that are actively courting booter operators and providing stable high bandwidth attack servers that allow spoofing.

5.1 Data Set

Our first task was to identify booter services for this part of our study. Absent a centralized location for finding booters, we found services via search engines and advertisements on hacker forums. We selected 15 booter services that received the most positive feedback on underground forums for our attack infrastructure characterization. The number of booters was kept relatively small in order to minimize the amount of money we paid to these services. We make no claim about the coverage these booters provide of the entire ecosystem. Rather, we were looking to provide a sample of stable services ranked highly for search terms associated with booter services. In addition, these booters garnered the most positive replies to their advertisements on underground forums.

We purchased a one month subscription from each of the services which ranged from $2.50-18.99 and focused on measuring amplification attacks based on our measurements of VDO that showed it was the most common type of attack. In addition, amplification attacks were the default attack type for all 15 booters. More precisely, we chose to measure the most common amplification reflection attack types offered by the booters, which were SSDP, NTP, DNS and Chargen. Table 3 shows the set of booters, the four attack types that booter offered and the cost of a basic month subscription.

We conducted attacks directed at our target server from December 2014 - January 2015. The goal of these attacks was to map out the set of misconfigured hosts that were being used by each booter to amplify their reflection attacks. The configuration of our target system used for measuring the attacks was an Intel Xeon 3.3GHz server running Ubuntu with 32 GB of RAM and an isolated 1 Gbps dedicated network connection.

We used gulp [24], which is a lossless Gigabit packet capture tool to capture attack traffic. Each attack lasted for one hour total and was comprised of many shorter attack instances of 10 minutes each, which is the standard time limit for basic subscriptions. The reasoning behind the longer attack times was to increase our probability of identifying all the misconfigured reflection hosts used by a booter for each attack type.

5.2 Frontend Servers

Booter services maintain a frontend website that allows customers to purchase subscriptions and launch DDoS attacks using convenient drop-down menus to specify the attack type and victim's IP or domain name. These frontend websites commonly come under DDoS attack by rival booters and are subject to abuse complaints from anti-DDoS working groups. All 15 booters in our study use CloudFlare's DDoS protection services to cloak the ISP hosting their frontend servers and to protect them from abuse complaints and DDoS attacks.

As part of this study, we contacted CloudFlare's abuse email on June 21st 2014 to notify them of the abusive nature of these booters. As of the time of writing this paper, we have not received any response to our complaints and the still active subset of booters continue to use CloudFlare. This supports the notion that at least for our set of booters CloudFlare is a robust solution to protect their frontend servers. In addition, *crime are.com* has a list of over 100 booters that are using CloudFlare's services to protect their frontend servers.

Booter	Attack Types	Cost
ANO	DNS	$6.60
BOO	NTP,Chargen	$2.50
CRA	DNS,SSDP	£10.99
GRI	NTP,SSDP	$5.00
HOR	NTP,SSDP	$6.99
INB	DNS,NTP,SSDP	$11.99
IPS	NTP,SSDP,Chargen	$5.00
K-S	SSDP,Chargen	$3.00
POW	SSDP	$14.99
QUA	DNS,SSDP	$10.00
RES	DNS,NTP	$10.00
SPE	DNS,NTP,SSDP,Chargen	$12.00
STR	DNS,SSDP	$3.00
VDO	DNS,NTP,SSDP	$18.99
XR8	DNS	$10.00

Table 3: *List of booter services we measured, the attack types offered, and the cost of the least expensive one-month subscription.*

5.3 Attack Servers

Renting back-end servers to generate attack traffic is the primary expense for operators of booter services. We did some research to get a broad sense of the market availability and cost of back-end servers that allow the source IP address to be spoofed. Being spoof friendly, fast uplink speed and high caps or unmetered bandwidth usage are the key requirements of a server appropriate for supporting the operation of a booter service. Providers of spoof friendly Virtual Private Servers (VPS) can be located on the same underground forums as where booters advertise their services. These VPS providers often explicitly advertise the ability to spoof source IP addresses as one of their key features.

In order to understand if these services delivered on their claims of allowing spoofing and providing the bandwidth they advertised we rented VPS from two hosting providers that advertised on underground forums. We rented one of the spoof-friendly virtual servers directly from a booter service included in our study.

Provider	VPS IP	Uplink speed	Bandwidth	Monthly cost
CaVPS Host	192.210.234.203	3.5 Gbps	Unmetered	$35
Spark Servers	96.8.114.146	949 Mbps	10 TB	$60

Table 4: *Spoofing enabled VPS services.*

Table 4 summarizes the services that we purchased. Both of the VPSs we purchased were connected to the same ISP (ColoCrossing) in the US. We also verified that both VPSs allowed spoofing and measured their actual link speeds. One VPS provided around 1Gbps uplink bandwidth and the other one provided up to 3.5Gbps. Due to budget limitations we could only rent these two VPSs and did not rent any higher end dedicated servers. However, our initial results show that this is a potentially effective method of mapping out abusive

	Chargen		DNS		NTP		SSDP	
Booter	(#)	(%)	(#)	(%)	(#)	(%)	(#)	(%)
ANO	-	-	1,827	73%	-	-	-	-
BOO	370	65%	-	-	1,764	86%	-	-
CRA	-	-	43,864	56%	-	-	64,874	46%
GRI	-	-	-	-	1,701	72%	10,121	60%
HOR	-	-	-	-	8,551	58%	242,397	30%
INB	-	-	38,872	55%	4,538	92%	170,764	54%
IPS	1,636	44%	-	-	1,669	85%	90,100	29%
K-S	1,422	30%	-	-	-	-	5,982	76%
POW	-	-	-	-	-	-	1,424,099	11%
QUA	-	-	10,105	85%	-	-	39,804	67%
RES	-	-	2,260	82%	27	100%	-	-
SPE	2,358	38%	26,851	61%	6,309	35%	258,648	24%
STR	-	-	93,362	53%	-	-	7,126	74%
VDO	-	-	16,133	82%	6,325	82%	150,756	62%
XR8	-	-	44,976	52%	-	-	-	-
Total	4,565	23.46%	181,298	35.30%	17,599	42.31%	2,145,015	11.84%

Table 5: *Number of total amplification servers and percentage of overlap with amplification servers used by other booters.*

hosting and we plan to scale this part of our measurements as future work.

5.4 Attack Techniques

Due to their effectiveness, amplified volume-based attacks are the default attack technique offered by most booter services. We focused our analysis on SSDP (more commonly known as Universal Plug and Play (UPnP)), DNS, NTP and Chargen. These attacks depend on servers running misconfigured UPnP, DNS resolvers, NTP and Chargen services that enable attackers to amplify attack traffic by sending spoofed packets with the victim's source address in the IP header and having these services respond with a larger amount of traffic directed to the victim.

5.5 Amplifiers

As part of our measurements we can map out the set of amplifiers that are being abused to magnify the traffic volume of attacks. This sheds light on the population of hosts that are not only potential amplifiers, but are actively being used as amplifiers for DDoS attacks. Table 5 shows that the set of abused Chargen and NTP servers are smaller and more highly shared between two or more services, whereas there is an ample supply of DNS and SSDP servers that are used as amplifiers. However, the overlap of DNS servers used by two or more booter services is still relatively high suggesting that these DNS resolvers might be more stable, have higher bandwidth connections and be in more limited supply.

5.6 Amplifier Location

As demonstrated by Table 6, both the geolocation and AS of amplifiers used by booters are fairly diffuse. There are a few notable exceptions, such as the concentration of Chargen amplifiers in China with three Chinese ASs connecting 34% of these amplifiers. In addition, there is a slight concentration of abused NTP servers connected to one Taiwanese AS and two United States network operators. This might indicate a potential to focus notification and patching efforts on these networks, given the limited pool of hosts used for Chargen and NTP attacks from Table 5. Feeds of these actively abused servers could also be distributed to these network operators and to DDoS mitigation services.

CC	%	AS	%
Chargen			
CN	48.78%	4134 (Chinanet)	14.46%
US	12.51%	37963 (Hangzhou Alibaba Advertising)	10.47%
KR	5.50%	4837 (CNCGROUP China169 Backbone)	6.88%
RU	4.58%	17964 (Beijing Dian-Xin-Tong Network)	2.61%
IN	2.56%	7922 (Comcast Cable Communications)	2.61%
DNS			
US	12.38%	4134 (Chinanet)	2.68%
RU	11.58%	3462 (Data Communication Business Group)	2.15%
BR	9.19%	18881 (Global Village Telecom)	1.46%
CN	6.84%	4837 (CNCGROUP China169 Backbone)	1.45%
JP	3.61%	7922 (Comcast Cable Communications)	1.27%
NTP			
US	31.47%	3462 (Data Communication Business Group)	14.01%
TW	15.29%	46690 (Southern New England Telephone)	12.35%
CN	10.68%	7018 (AT&T Services)	4.84%
KR	5.50%	4134 (Chinanet)	3.58%
RU	4.74%	4837 (CNCGROUP China169 Backbone)	2.18%
SSDP			
CN	36.26%	4837 (CNCGROUP China169 Backbone)	18.98%
US	19.37%	4134 (Chinanet)	11.16%
EG	6.83%	8452 (TE Data)	6.61%
AR	5.37%	22927 (Telefonica de Argentina)	5.13%
CA	5.36%	7922 (Comcast Cable Communications)	4.60%

Table 6: *Top country locations and autonomous systems for amplifiers.*

5.7 Amplifiers Churn

In order to measure the stability of these amplifiers we probed them periodically for 13 weeks to understand how many were still located at the same IP and misconfiged. As shown in Figure 2, the set of DNS resolvers were the most stable with nearly 80% still misconfiged and located at the same IP after one month, and over 60% were still misconfigured after 13 weeks. This result is counter to the previous results of churn based on Internet wide scanning that found a 50-60% churn rate for DNS servers after one week [15]. It potentially indicates that booters have gravitated to using a more stable set of DNS resolvers and that focusing mitigation efforts on these might cause these DNS attacks to be less efficient and require additional bandwidth and cost. However, our measurements were collected after those in the previous study making direct comparisons challenging.

5.8 Amplification Factor

One of the few direct costs incurred for every attack a booter service launches is the bandwidth sent from their rented attack servers. In order to reduce this cost amplifi-

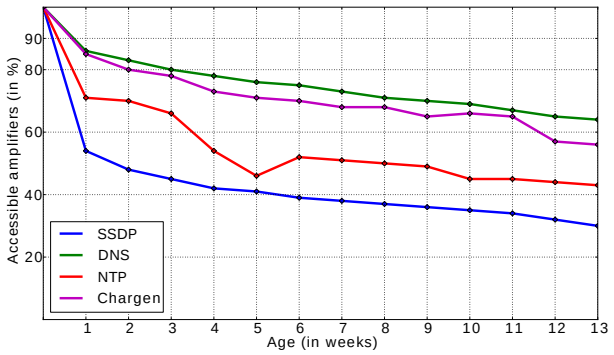

Figure 2: *IP churn of amplifiers.*

cation attacks are used for volume-based flooding attacks. Our amplification factor measurements largely agree with the lower-end bandwidth amplification factor numbers reported in a previous study [15], with NTP attacks resulting in an average amplification factor of 603 times. Chargen was the next largest at 63 times, DNS resulting in an average of 30 times amplification and SSDP generating the smallest average amplification factor of 26 times. This and the limited number of NTP amplifiers confirms that the communities focus on prioritizing notification and patching of misconfigured NTP servers is the correct approach. We also suggest that some effort be placed into notifying operators of servers with misconfigured and abused Chargen services, since these are the next largest threat and there is also a potentially constrained supply.

6. PAYMENT INTERVENTION

As part of our study we sought out opportunities to understand and also measure the effectiveness of undermining DDoS Services. In this section, we present our measurements of a payment intervention that was conducted in collaboration with PayPal and the FBI.

We find that reporting accounts to responsive payment service providers, such as PayPal, can have the desired effect of limiting their ability and increasing the risk of accepting payments. This technique requires constant monitoring of the booters and drives them to move to more robust payment methods, such as Bitcoin.

6.1 Payment Ecosystem

At the onset of our study, the majority of booter services accepted credit card payments via PayPal as their primary mechanism for receiving funds from their customers. In addition, some booters accepted bitcoin payments and a limited number accepted credit card payments using Google Wallet[4] and virtual currencies, such as WebMoney and Perfect Money. These last two prohibit customers from the United States from opening an account and using their platform.

We identified a larger set of 60 booter services [5] that accepted PayPal and created custom crawlers to monitor their payment methods and merchant accounts for about 6 weeks from April 22, 2014 through June 07, 2014. To receive their payments using PayPal, booter services redirect customers to the PayPal website where existing PayPal users can login and complete a transaction. After logging into PayPal, our crawlers were able to collect the merchant account identifier of the corresponding booter service from the HTML source of the page without completing a transaction.

The set of booters selected for monitoring were located from underground forum advertisements and web searches for terms commonly associated with booter services. Again we make no claim about the coverage these booters provide of the entire ecosystem. To minimize the effect of unstable booters on our study, the final set of booters included in our analysis was limited to the 23 stable booter services that were able to successfully use PayPal to receive funds for at least half of the time before the PayPal intervention and used at least one PayPal account after the intervention. Nine of these 23 booter services overlapped with the set of 15 booters measured in section 5. Among the reasons that six booters were not included in this measurement is that some did not accept PayPal and others did not accept PayPal over half the time in the first 6 week period.

After collecting our initial data on the stability of their PayPal merchant accounts, we reported these booter's domains and accounts to PayPal. The organization then began to monitor merchant accounts linked to these domains and suspended them after an investigation. Note that PayPal will initially limit merchant accounts that are found to violate their terms of service by accepting payments for abusive services until they perform an investigation of the account. Once an account is limited the merchant cannot withdraw or spend any of the funds in their account. This will result in the loss of funds in these accounts at the time of freezing and potentially additional losses due to opportunity cost while establishing a new account. In addition, PayPal performed their own investigation to identify additional booter domains and limited accounts linked to these domains as well. This had the affect of a large-scale PayPal payment disruption for the majority of booter services.

In order to further understand the effectiveness of our payment intervention, we monitored underground forums where these booters advertise their services and news feeds from booters we joined to discover qualitative data on the effectiveness of PayPal's payment intervention.

6.2 Usage Pattern of PayPal Accounts

Based on our observations, booter services will generally use only one PayPal account at a time to receive payments. Once a limit is put on an account, they will change it. At times, they will also proactively change accounts to reduce the risk of having limits imposed. We used the dataset collected during the initial monitoring period to understand how frequently booter services were changing their PayPal accounts. Note that our age measures are both right and left-censored. For the booter's initial account our data is left-censored and for the last account our data is right-censored. However, we believe our age measurements accu-

[4]Google phased out their digital goods payment processing at the start of March 2015 — `https://support.google.com/wallet/business/answer/6107573`.

[5]This set is larger than the previous set, since we did not have to pay for a subscription in order to monitor their payment accounts.

Booter	accounts before	accounts after	Status
ANO ⋆	6 (8.2)	7 (2.9)	✓
AUR	6 (7.2)	6 (2.7)	✗
BOO •	6 (8.3)	11 (2.7)	✓
CRI †	4 (9.0)	1 (2.0)	✗
DAR ◇	4 (6.0)	5 (4.8)	✓
DIA †	3 (15.7)	0 (-)	✗

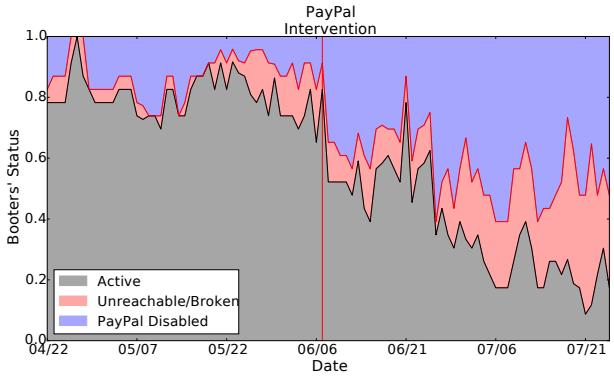

Figure 5: *Status of booters over time.*

booter's ability to accept PayPal payments and operate the booter. Each booter was categorized by one of the following statuses each day, based on the results of our crawl.

Active: The booter is able to successfully use a PayPal account to receive payments from its customers.

Unreachable/Broken: Either the booter's frontend website was not responding to HTTP requests, the booter service had closed or the frontend site was not functional.

PayPal Disabled: The booter's frontend website is active, but the service has either removed PayPal as a payment option, or the PayPal account linked to the booter website is limited and therefore unable to receive payments.

Figure 5 shows the status of booter services over time. The vertical line represents the date on which we started sharing our data with PayPal and PayPal started to independently investigate the reported accounts and take action against them. As observed in Figure 5, the percentage of active booters quickly drops from 70-80% to around 50% within a day or two following the intervention date and continues to decrease to a low of around 10%, before fluctuating between 10-30%. This resulted in an increase in PayPal unavailability from 20% before the intervention to 63% during the intervention. In addition, we observed 7 booter services in our study shut down their businesses and most of the remaining services switched to alternative payment methods, such as Bitcoin.

6.4 Qualitative Assessments

In addition to our quantitative measurements, we also have qualitative evidence of the efficacy of PayPal's payment intervention. By monitoring the underground forums where these services advertise we can witness the impact of these account limitations. Wrote one booter operator during the intervention, "So until now 5 time my 5 PayPal Accounts got Limited on My stresser is other stresser have same Problem with the f***ing Paypal ? is there any solution what we should do about f***ing Paypal ?" Similarly, customers vented their frustration at being unable to purchase a booter service using PayPal. Wrote one booter customer, "when i go to buy a booter it normally says i can't buy because their PayPal has a problem."

In a number of cases, booters directly link their closures to loss of funds due to PayPal merchant account limitations. This message was posted on the front page of a defunct booter service, "It's a shame PayPal had to shut us down several times causing us to take money out of our own pocket to purchase servers, hosting, and more."

6.5 Booter Response

As with any intervention, the target, in our study booters, will respond by adapting to the pressure. In this case, we do not have enough quantitative measurements to assess the effectiveness or the full range of responses to our attempt to undermine booter's payment infrastructure. However, we have identified several common classes of adaptations in response to the intervention.

Alternate payment methods. Most booters have added Bitcoin as an alternate payment method and have posted links to services that allow customers to purchase bitcoins using credit cards or PayPal. In addition to bitcoins some switched to Google Wallet and others added the option to pay using virtual currencies, such as Webmoney and Perfect Money. By all accounts, these have resulted in reduced customer bases unless the booter can directly accept credit card payments. Evidenced by the fact that many booters continued to replace their PayPal accounts even when previous ones were limited and their funds were lost. Assuming that alternative payment methods did not result in reduced revenue or higher costs there would be little incentive to continue using risky payment methods, such as PayPal.

Referrer anonymizing services. We have noticed that some booters have stopped directly linking to PayPal and are now linking to an intermediary site and then redirecting the customer from this intermediary domain to PayPal's site. This intermediary redirection site is used to hide the booter's real domain name in the referrer field from PayPal. A subset of booters have also started to replace this intermediary domain every time they replace a PayPal account. The effect of this is that it requires active crawling and measurements of booter sites to identify a new PayPal account. This bypasses passive methods PayPal could use to linking accounts, such as by using referrers, which results in increasing the difficulty of monitoring booter's PayPal accounts and effort required to investigate these accounts.

Offline payment. Finally, in some cases booters have required customers to open a ticket to pay using PayPal. This method increases the effort to monitor the booter for new accounts, since instead of an automated crawler someone must now interact with the booter service manually. However, this method also requires the booter service to manually activate each account and drives away customers that are seeking automated subscription purchasing systems.

7. DISCUSSION AND FUTURE WORK

We have gathered a few key points from ours and the community's efforts to understand and undermine these DDoS services. Most of these potential strategies involve driving up costs of operating booter services and reducing the convenience of subscribing.

Reducing scale. Limiting access to convenient payment methods, such as PayPal, had an impact on the scale of booter services based on our quantitative and qualitative analysis. However, based on the short duration of the intervention it is unclear if this approach would continue to be effective in the longer-term. As future work, we plan to understand how to improve the effectiveness of these interventions and make them sustainable. This in part requires developing more robust monitoring tools that better miti-

gate countermeasures being deployed to make their payment methods more robust to interventions.

Reducing effectiveness of attacks. We plan to continue our monitoring efforts of the amplification servers used by booters and begin sharing this information with existing patching efforts, such as the OpenResolverProject [2] and OpenNTPProject [1]. Along with this, we plan to experiment with active notifications sent to the ISP and abuse contact for the server. There is some indications that active notification improves patching rates in context of patching vulnerable services [6, 10].

Increasing costs. This might be achieved with an increased effort to locate and blacklist or de-peer low-cost hosting services that cater to DDoS attacks by providing the ability to spoof and unlimited bandwidth. This might force these services to pay a premium for bullet-proof hosting attack servers, which would result in reduced profitability or be passed along to subscribers in the form of increased subscription costs.

In addition, convincing CloudFlare and other free anti-DDoS services to prohibit these booter services would increase their costs by forcing them to build and pay for anti-DDoS services that cater to these abusive booters. Admittedly these suggestions will likely not result in large cost increases unless tremendous amounts of pressure were placed on these parts of their infrastructure.

Increasing risk to operators. Our analysis of data provided by PayPal suggests that much of this activity is occurring in the United States. If this is the case there is the potential that increased law enforcement efforts could have a direct impact in arresting key operators of these services and increasing the perceived risk of operating and using these services. In the case of operators it is likely they could be replaced by overseas operators. However, in the case of customers it might be difficult to find a new subscriber based for these services that is located outside the United States and Western Europe if the perceived risk of using these services increased. To this end we plan to work with law enforcement to understand how effective this type of intervention is on mitigating the threat of booter services.

8. CONCLUSION

Unfortunately, there is no silver bullet that will mitigate the threat posed by booter services overnight. These booters have grown in scale due to the perceived low-risk nature, their profitability and increasing demand for DDoS attacks.

In this paper we have mapped out a range of support infrastructure that booters depend on in terms of advertising, attack, hosting and payment. We demonstrated that payment interventions, which undermine the accessibility of convenient payment methods, such as PayPal, can potentially have an impact on reducing the scale of these services. Our hope is that by continuing to explore new methods for understanding and undermining booters, we can identify increasingly effective methods of adding friction, cost and risk to these ventures that further erodes their scale and profitability over time.

9. ACKNOWLEDGMENTS

We thank PayPal's Information Security team for their assistance. This work was supported by National Science Foundation grant NSF-1237076 and gifts from Google.

10. REFERENCES

[1] Open NTP Scanning Project. http://OpenNTPProject.org/.

[2] Open Resolver Project. http://OpenResolverProject.org/.

[3] Lizard Squad's Xbox Live, PSN attacks were a 'marketing scheme' for new DDoS service. http://www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/, 2014.

[4] Lizard Squad Strikes Again: Why Can't Sony And Microsoft Protect Themselves? http://www.ibtimes.com/lizard-squad-strikes-again-why-cant-sony-microsoft-protect-themselves-1823282, 2015.

[5] A. Büscher and T. Holz. Tracking DDoS Attacks: Insights into the Business of Disrupting the Web. In *Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats*, LEET'12, pages 8–8, Berkeley, CA, USA, 2012. USENIX Association.

[6] O. Cetin, M. H. Jhaveri, C. Ganan, M. van Eeten, and T. Moore. Understanding the role of sender reputation in abuse reporting and cleanup. In *Workshop on the Economics of Information Security*, 2015.

[7] R. Clayton, T. Moore, and N. Christin. Concentrating correctly on cybercrime concentration. In *Proceedings (online) of the Fourteenth Workshop on the Economics of Information Security (WEIS)*, Delft, Netherlands, June 2015.

[8] E. Cooke, F. Jahanian, and D. McPherson. The zombie roundup: Understanding, detecting, and disrupting botnets. In *Proceedings of the Steps to Reducing Unwanted Tra c on the Internet*, SRUTI'05. USENIX Association, 2005.

[9] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir. Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, IMC '14, pages 435–448. ACM, 2014.

[10] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, and V. Paxson. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, IMC '14, pages 475–488, 2014.

[11] J. Ioannidis and S. M. Bellovin. Implementing Pushback: Router-Based Defense Against DDoS Attacks. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2002, San Diego, California, USA*, 2002.

[12] S. Kandula, D. Katabi, M. Jacob, and A. Berger. Botz-4-sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds. In *Proceedings of the 2ND Conference on Symposium on Networked Systems Design & Implementation*, NSDI'05, pages 287–300. USENIX Association, 2005.

[13] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamalytics: An Empirical Analysis of Spam Marketing Conversion.

In *Proceedings of the 15th ACM conference on Computer and communications security*, 2008.

[14] M. Karami and D. McCoy. Understanding the Emerging Threat of DDoS-as-a-Service. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats*, Berkeley, CA, 2013. USENIX.

[15] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, pages 111–125. USENIX Association, 2014.

[16] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks. In *Proceedings of the 8th USENIX Workshop on O ensive Technologies*, August 2014.

[17] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and S. Savage. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In *Proceedings of the IEEE Symposium and Security and Privacy*, pages 431–446, May 2011.

[18] D. McCoy, H. Dharmdasani, C. Kreibich, G. M. Voelker, and S. Savage. Priceless: The Role of Payments in Abuse-advertised Goods. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, 2012.

[19] D. McCoy, A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, G. M. Voelker, S. Savage, and K. Levchenko. Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs. In *Proceedings of the 21st USENIX Conference on Security Symposium*, 2012.

[20] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage. Inferring Internet Denial-of-service Activity. *ACM Trans. Comput. Syst.*, 24(2):115–139, May 2006.

[21] T. Moore, R. Clayton, and R. Anderson. The Economics of Online Crime. *Journal of Economic Perspectives*, 23(3):3–20, 2009.

[22] V. Paxson. An Analysis of Using Reflectors for Distributed Denial-of-service Attacks. *SIGCOMM Comput. Commun. Rev.*, 31(3):38–47, July 2001.

[23] C. Rossow. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium*, February 2014.

[24] C. Satten. Lossless Gigabit Remote Packet Capture With Linux. `http://staff.washington.edu/corey/gulp/`, 2008.

[25] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Practical Network Support for IP Traceback. In *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '00, pages 295–306, 2000.

[26] S. M. Specht and R. B. Lee. Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. In *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems*, pages 543–550, 2004.

[27] B. Stone-Gross, R. Abman, R. Kemmerer, C. Kruegel, D. Steigerwald, and G. Vigna. The Underground Economy of Fake Antivirus Software. In *Economics of Information Security and Privacy III*, pages 55–78. Springer, 2013.

[28] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-scale Spam Campaigns. In *Proceedings of the 4th USENIX Conference on Large-scale Exploits and Emergent Threats*, LEET'11, 2011.

[29] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao. Follow the Green: Growth and Dynamics in Twitter Follower Markets. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 163–176, 2013.

[30] V. L. Thing, M. Sloman, and N. Dulay. A Survey of Bots Used for Distributed Denial of Service Attacks. In *New Approaches for Security, Privacy and Trust in Complex Environments*, pages 229–240. Springer, 2007.

[31] K. Thomas, D. Huang, D. Wang, E. Bursztein, C. Grier, T. Holt, C. Kruegel, D. McCoy, S. Savage, and G. Vigna. Framing dependencies introduced by underground commoditization. In *Proceedings of the Fourteenth Workshop on the Economics of Information Security (WEIS)*, Delft, Netherlands, June 2015.

[32] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxson. Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In *Proceedings of the 22nd Usenix Security Symposium*, 2013.

[33] D. Y. Wang, M. Der, M. Karami, L. Saul, D. McCoy, S. Savage, and G. M. Voelker. Search + Seizure: The Effectiveness of Interventions on SEO Campaigns. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, IMC '14, pages 359–372, 2014.

[34] A. Welzel, C. Rossow, and H. Bos. On Measuring the Impact of DDoS Botnets. In *Proceedings of the 7th European Workshop on Systems Security (EuroSec 2014)*, April 2014.

[35] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston. Internet Background Radiation Revisited. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, IMC '10, pages 62–74. ACM, 2010.

[36] Y. Xiang, K. Li, and W. Zhou. Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics. *IEEE Transactions on Information Forensics and Security*, 6(2):426–437, June 2011.