Service in denial – clouds going with the winds

Vit Bukac, Vlasta Stavova, Lukas Nemec, Zdenek Riha, Vashek Matyas

Faculty of Informatics, Masaryk University, Brno, Czech Republic
{bukac, vlasta.stavova, lukas.nemec, zriha, matyas}@mail.muni.cz

Abstract. We analyze the threat of DDoS-for-hire services to low and medium power cloud-based servers or home users. We aim to investigate popularity and availability of such services, their payment models, subscription pricing, complexity of the generated attack traffic and performance.

1 Introduction and DDoS-as-a-service description

Our research aims to provide a comprehensive analysis of the Distributed Denial of Service as a Service (DDoSaaS) phenomenon. We evaluate the threat that DDoSaaS poses to low to medium power cloud-based servers or home users. Our goal is to measure the performance of generated attacks and properties of attack traffic, investigate financial aspect of the services, evaluate service popularity and compare their source codes. The information we collected allows us to conduct a grounded assessment of DDoSaaS risks for cloud providers and common users.

DDoSaaSs often present themselves as stress testing services (often called booters or stressers), willing to test the resistance of a chosen target to Distributed Denial of Service (DDoS) attacks. The services are accessed via websites that require prior registration. Common features of a DDoSaaS website are: it is in English, lists prices in US dollars and is easily retrievable through mainstream search engines. According to [1], the websites are frequently accessed through aggregated booter lists (e.g., top10stressers.com, thebestbooters.com), hacker sites (e.g., hackforums.net, hackbulletin.com) or Skype resolvers that translate Skype nicknames to latest IP addresses (e.g., iskyperesolve.com, skypegrab.net).

The websites frequently contain a Terms Of Service page, where service operators disclaim any responsibility for damages caused by users of the service. However, service operators do not check whether a customer is ordering attacks on targets under her supervision. Most common DDoSaaS customers are online gamers who seek to gain a competitive advantage over their opponents [2].

When ordering an attack, the customer has to specify a target URL or an IP address, length of the attack (limited by paid subscription, see Section 6.2) and an attack type. These values are inserted into a web form on the stresser webpage and submitted to a back-end server. The server evaluates the request and orders attack servers to initiate an attack.

Most services are very customer friendly. The main webpage contains dashboards with news for customers, such as newly available attack types or bandwidth increases and basic service statistics. A ticketing system is usually prepared for customers to report bugs and any issues. Many services even claim

24/7 support via instant messaging channels and offer occasional promo actions, such as subscription discounts or free trials.

The bandwidth available for attacks is usually advertised in the order of several gigabits per second or more (e.g., Anonymous Stresser 5 Gbit/s, Quantum Booter 15 Gbit/s). DDoSaaS employs a limited number of powerful servers that send attack traffic. The traffic is usually subsequently amplified by unsuspecting poorly configured intermediaries. DDoSaaSs also quickly adopt newly discovered attack methods. We have encountered sites offering attacks that were amplified through recently discovered vulnerabilities in Joomla content management system, Microsoft SQL Server or SSDP protocol.

The current modus operandi of DDoSaaS provides a good level of anonymity for both providers and technically knowledgeable users. Payments can be sent by anonymous cryptocurrencies (see Section 6.1), attack traffic has spoofed source IP addresses and webpages can be accessed through anonymization proxies.

Section 2 outlines the details of our dataset. Section 3 analyzes the properties of recorded attack traffic. Section 4 provides analyses of aggregated leaked databases of DDoSaaSs. Section 5 investigates DDoSaaS source code. Section 6 discusses the economic aspects of DDoSaaS. Summary of relevant previous work is provided in Section 7. Section 8 concludes our paper.

2 Dataset description

The list of domains that we investigated with respect to DDoSaaS contains 542 records. This list was constructed from searches for keywords such as booter, stresser, ddos-for-hire or ddosaas. These searches were run at Google search engine, YouTube and Hackforums.net site. In order to confirm that a particular domain is hosting a DDoSaaS website, at least one of the following conditions must have been fulfilled:

- The website behind the domain name is still accessible and belongs to a DDoSaaS service.
- A snapshot of the index webpage exists at a third party store (e.g., Google cache, CloudFlare cache, web.archive.org, etc.). The snapshot shows that the index webpage belonged to a DDoSaaS service.
- The domain name was mentioned on a hacker forum in a discussion about DDoSaaS services to be running and serving customers.

We confirmed 423 websites to be associated with DDoSaaS, 84 of which were accessible at some point during our investigation. We were able to create user accounts on 71 of them, to list supported payment methods from 82 and to list available subscription offers from 62 of them.

Most detailed information about the popularity of DDoSaaS can be extracted from leaked databases. Similarly, the internal working of DDoSaaS websites is best evaluated from the website source code. We have collected 53 archives of DDoSaaS website source code and separate 31 database files that have been released to sites such as pastebin.com or leakforums.org.

Database files contain records about user accounts, attacks and payments. We aggregated attack records and user records from multiple databases in order to build a comprehensive view which is not specific to any given DDoSaaS service. Unfortunately, only one payment database file was available for quantitative analysis. An aggregated summary of the databases is provided in Table 1.

The source code archives contain a total of 23,443 files with 13,983 unique MD5 hashes. Aggregated statistics of source code is listed in Table 2. Each archive has an associated name of a stresser whose files it supposedly contains. However, in most cases we were unable to verify that the archive is indeed related to the announced stresser, except for trivial checks such as verifying the logo image.

Table 1. Database files summary.

Database	Booters	Records
Attack logs	17	153,578
User logs	31	90,962
Payment logs	Quantum	16,990

Table 2. Source code files summary.

File extension	Files	MD5s
png/gif/jpg	14,676	8,770
php	4,094	2,285
js	1,832	1,227
html/htm	431	316
other/no ext	2,410	1,385
Total	23,443	13,983

In order to analyze the properties of attack traffic, we created a high performance virtual server on Amazon Elastic Compute Cloud (EC2). The virtual machine was configured with 4 virtual CPUs running on Intel Xeon core, 15 GB RAM and SSD storage. The server was connected with at least 1 Gbit/s line. Operating system was Ubuntu Trusty 14.04. The server was hosting a dummy webpage that imitated a webpage of a gaming clan. Attack traces were recorded with tcpdump command-line packet analyzer. Traffic records were collected for 300 seconds starting just prior to an attack launch, while the attack itself was executed for 30 s.

A total of 272 attacks were recorded from 16 DDoSaaSs. Attacks were launched against the server between December 2014 and April 2015. Attacks were directed either to the server IP address or to the hosted dummy webpage. Every attack method was tested twice in order to increase the chance of succesful attack traffic recording (see Section 3.1). All attack traces along with supporting documents are available at DDoS-Vault repository [3].

Detailed listing of tested services, global rank of their web pages [1], estimated monthly visits, numbers of created accounts and number of performed attacks can be found in Table 3. We focused on highly popular, extensively used DDoSaaSs with many users. Statistics show that DDoSaaSs are used by tens of thousands of users and are responsible for a staggering number of DDoS attacks. Our 272 recorded attacks are listed by attack classes and source DDoSaaSs in Table 4.

3 Traffic analysis

3.1 Attack success rate

An attack was considered succesful if its power exceeded predefined bitrate and packet rate limits (see below) and if the real attack type corresponded to the attack type requested by the customer. Power is a key metric of a flooding denial-of-service attack. It is expressed by a bitrate or a packet rate. Bitrate determines the capability to flood network links towards the victim network with an undesired traffic. A high packet rate can cause failures at network devices between attack sources and the victim (e.g., firewall, proxy, office router).

Since DDoSaaSs are primarily used against home connections and small servers, the limits were set in accordance with average Internet connection speeds as listed in Q4 2014 report from Akamai [4]. An attack power was deemed sufficient if the average bandwidth exceeded 25 Mbit/s or if the average packet rate exceeded 20,000 packets per second during the 30 s attack period.

Columns Bit and Packet in Table 4 show the percentage of recorded attacks of a chosen booter that surpass respective attack power limits. Approximately 51% of all attacks, regardless of source booter, *failed to exceed either power limit.* Approximately 43% did not even reach 1 Mbit/s. Such attacks can be considered ineffective against any target.

We also observe significant differences in attack power success rate of different booters. There are numerous potential reasons why a DDoSaaS attack strength is low: underprovision of resources, scams, malfunction of backend stressing infrastructure, DDoS-prevention measures at ISP network and/or cloud infrastructure.

We could not identify any time relations between attacks that fail to reach the desired power. We compared attack bitrates and packet rates between each two attacks with the same attack method on the same booter. Out of 135 pairs of such attacks, both attacks failed to exceed the bitrate/packet rate limits at 60 pairs and one attack failed to exceed the limits at 18 pairs. For example, two DNS amplification attacks were executed at hornystress.me in the span of three hours. The first attack failed to generate any harmful traffic while the second attack reached up to 380 Mbit/s of incoming traffic.

Differences between attack launch times in these 18 pairs oscillate between one hour and three days. Other attacks were also succesfully executed in the meantime at the same booter. Therefore, we believe that a combination of factors is behind power drops. Issues at the side of DDoSaaS are not solely responsible. As a consequence, the success rate of attacks against home connections or cloud providers without a DDoS protection may be significantly higher. Further research will be needed to evaluate the conditions that affect the attack power.

A customer specifies the requested attack type. However, *collected traffic records did not always correspond to the requested type.* Potential reasons include: maintaining public image (booters claim to have capabilities that they actually lack), malfunction of backend stressing infrastructure or unwillingness to use non-spoofed attacks. The column Type in Table 4 shows the percentage of attacks whose dominant portion of traffic corresponds to the customer request.

Table 3. Booter statistics for February 2015. Global ranks and monthly visit estimates were collected from [1]. Total user account and executed attack statistics were collected directly from dashboards at stresser web pages where available.

Booter	Global rank	Est. visits	Accounts	Attacks
anonymous-stresser.com	571,894	25,000		
booter.in	258,375	55,000	6,324	22,635
booter.io	464,756	35,000	9,336	45,073
connectionstresser.com	319,831	40,000	17,444	180,751
destressbooter.com	659,154	25,000		
hornystress.me	297,124	70,000		16,310
ipstresser.com	45,082	420,000		
legion.cm	1,254,496	10,000	10,393	
networkstresser.com	215,904	100,000		28,523
networkstresser.net				20,417
powerstresser.com	169,402	130,000	10,197	44,273
quantumbooter.net	323,716	55,000		
ragebooter.com	314,984	50,000	14,022	12,148
restricted-stresser.info	1,821,164	5,000		
titaniumstresser.net	79,299	310,000		305,494
vdos-s.com	689,739	20,000	17,452	

Table 4. Recorded attacks.

		Attack class			Booter success (%)		
DDoSaaS		UDP	TCP	HTTP	Bit	Packet	Type
anonymous-stresser.com		8	2	16	15	19	100
booter.in		10	6	0	50	56	63
booter.io		8	4	0	50	67	83
connectionstresser.com		10	2	0	67	50	100
destressbooter.com		20	0	2	5	0	73
hornystress.me		18	14	2	32	44	76
ipstresser.com		14	2	6	59	82	100
legion.cm		2	0	8	0	0	80
networkstresser.com		12	2	0	86	86	21
networkstresser.net		10	5	0	0	0	100
powerstresser.com		4	4	0	0	0	100
quantumbooter.net		5	4	0	56	78	100
ragebooter.com		10	6	0	31	6	75
restricted-stresser.info		8	4	18	21	29	100
titaniumstresser.net		4	2	4	100	50	100
vdos-s.com		4	12	0	63	88	88
Total attacks		147	69	56			
Class success (%)	Bit	57	17	7			
	Packet	42	55	18			
	Type	72	100	100			

An aspect of DDoSaaS quality is the speed with which an attack is launched after it is requested by the customer. We measured the time between an attack order and the timestamp of first incoming attack traffic packet. Average time to start an attack was 7 seconds and 80% of the attacks started in 10 seconds or less. Such a rapid response is especially important for gamers, who represent a large portion of DDoSaaS customers.

3.2 Attack power

A histogram of measured bitrates of attacks in our dataset is shown in Table 5. Bitrate only rarely exceeds 1 Gbit/s. The attack types most likely to reach a high bitrate are CHARGEN and DNS. TCP-based and HTTP-based attacks showed a poor bitrate performance. Succesful NTP and SSDP attacks have the clearest power boundaries around 400 Mbit/s and 300 Mbit/s respectively.

Table 5. Recorded attack bitrate histogram.

Class	Type	Bitrate (Mbit/s)							Total
		25	200	400	600	800	1000	>1000	
HTTP	HTTP	52	0	0	4	0	0	0	56
TCP	SYN	42	3	1	1	0	0	0	47
TCP	TCP	15	7	0	0	0	0	0	22
UDP	CHARGEN	9	2	7	6	3	0	2	29
UDP	DNS	8	6	6	3	2	2	2	29
UDP	NTP	16	1	6	7	0	0	0	30
UDP	Other	16	1	3	0	0	0	0	20
UDP	SSDP	14	5	15	5	0	0	0	39

An attack packet rate histogram is given in Table 6. Attack types associated with the high packet rate are SYN, TCP, SSDP and NTP. TCP SYN attacks exhibit below-average values both for bitrate and packet rate, because this attack is based on the exhaustion of victim connection state table buffer.

Table 6. Recorded attack packet rate histogram.

Class	Type	Packet rate (packets per second)							Total
		20k	40k	60k	80k	100k	120k	>120k	
HTTP	HTTP	46	7	3	0	0	0	0	56
TCP	SYN	21	7	10	5	3	0	1	47
TCP	TCP	10	3	2	0	2	1	4	22
UDP	CHARGEN	19	8	2	0	0	0	0	29
UDP	DNS	18	6	2	0	1	0	2	29
UDP	NTP	17	0	0	2	2	3	6	30
UDP	Other	16	2	2	0	0	0	0	20
UDP	SSDP	15	2	2	2	4	8	6	39

Overall, even succesful DDoSaaS attacks were *not powerful enough* to cause a denial-of-service effect against a cloud-based server with high resources. However, the attack power of succesful attacks may be sufficient to saturate uplinks of low- to mid-range servers or at least cause a degradation of service if the traffic reaches the server itself. Conversely, more than 40% of all attacks would fail to overwhelm even home connections with 1 Mbit/s or less download speed.

3.3 Attack traffic properties

Tables 7 and 8 show values of most common attack traffic source ports and packet lengths. The booters column specifies how many booters contained the listed feature values in their attack traffic. The traffic column indicates the percentage of all traffic in an appropriate attack class that has the respective property. Source ports clearly show that UDP-based attack employ amplifiers, hence the traffic is incoming from well-known ports. Conversely, TCP-based attacks rely on simple IP spoofing and their traffic source ports are evenly distributed. Due to a low number of useable HTTP attack traffic samples, this attack type has been excluded from further research.

Table 7. Most frequent packet lengths.

Attack type	Length (B)	Booters	% traffic
CHARGEN	57	7/9	5%
DNS	4044	4/10	9%
NTP	468	9/11	99%
SSDP	296	10/11	6%
SYN	40	14/14	93%
TCP	40	3/4	99%

Table 8. Most frequent source ports.

Attack type	Port	Booters	% traffic
CHARGEN	19	7/9	92%
DNS	53	10/10	54%
NTP	123	9/11	99%
SSDP	1900	10/11	90%
SYN	80	11/14	22%
TCP	80	3/4	<1%

Table 9 lists some of the manually chosen key unique identifiers that distinguish the attack traffic from the benign traffic. Interesting are similar domain names in DNS amplification attacks. Since a domain name is not inherent to an attack type, we assume that DDoSaaS operators either rent their back-end infrastructure from other providers or buy attack scripts on an open market. Both of these approaches have been known to be used for other service types [5].

Table 9. Application-layer artifacts.

Class	Type	Artifact type	Values	Booters
UDP	DNS	Query domain name	fkfkfkfz.guru	2/10
UDP	DNS	Query domain name	doleta.gov	2/10
UDP	SSDP	HTTP Location	IGD.xml	8/11
UDP	SSDP	HTTP Location	rootDesc.xml	8/11
UDP	NTP	Request code	MON_GETLIST	9/11

NTP traffic in our dataset shows to be extremely homogenous. All attack packets come from port 123/UDP, carry NTP payload with request code 42 (MON_GETLIST) and IP length 468 bytes. These signs are consistent with a well-documented NTP vulnerability CVE-2013-5211. NTP amplification attacks based on MON_GETLIST command were analysed by Czyz et al. in [6].

Predominant SSDP attack variant is fairly new, first observed in July 2014 [7]. The attack is amplified by unpatched home routers and smart appliances.

SYN attacks have a standard well-understood form. Incoming attack traffic has spoofed source IP addresses, packet length 40 B and SYN flag set. Anomalous were TCP window sizes where in 86% of cases values were set to 0.

We can see that *attack traffic even from different DDoSaaS shows remarkable similarities*, such as packet lengths or application-layer artifacts. The traffic is simple, constructed for maximum attack effectiveness rather than for stealthiness. By using attack reflectors, the DDoSaaS operators sacrifice the capability to randomize attack traffic properties (e.g., packet lengths, source ports, header field values) and circumvent advanced victim DDoS protection solutions. DDoSaaS operators have no control over reflectors, therefore the final attack traffic exhibits a high degree of uniformity, because reflectors are configured to respond with standard, non-randomized responses. It is fairly easy to configure rules for packet filters to drop or throttle most of the attack traffic. Since the primary DDoSaaS targets are home connections or low-end servers without trained security teams who would react to evolving attacks, we do not expect any sudden increase in the use of detection avoidance techniques in the future.

4 Database analysis

We have collected records from leaked databases of 31 services. The statistics presented are based on aggregated records of databases as specified in Table 1.

Table 10 shows more than 75% of attacks performed by stressers are at most 10 minutes long. Our aggregated records therefore support the results of Karami and McCoy [2]. Unsurprisingly, most common lengths of actual boots are equivalent to subscription maximum booter lengths (Table 11). Therefore, we can assume that DDoSaaS customers execute attacks for the maximum boot length available to them.

Table 12 shows that *UDP-based flooding attacks have a significantly higher popularity* than TCP-based or HTTP-based attacks. This is likely to be caused, at least partially, by DDoSaaS operators who set UDP attacks as the default option. UDP is also preferable due to its amplification factor. Protocols such as CHARGEN, NTP, SSDP or DNS are frequently exploited by DDoSaaS operators to increase the impact on victims without having to increase the attacker's available bandwidth. TCP-based attacks are almost exclusively variations of SYN flooding. Somewhat surprising is popularity of RUDY and Slowloris attacks compared to generic HTTP GET/POST/HEAD flooding.

In 84% of attacks, the target port of the attack was 80 (HTTP), followed by ports 3074 (Xbox LIVE), 6005 (BMC Software), 25565 (Minecraft/MySQL),

Table 10. Boot lengths histogram.

Interval (s)	Attacks
0 – 100	40,836
101 – 200	27,971
201 – 400	31,940
401 – 600	2,649
601 – 800	2,753
801 – 1000	6,650
1001 – 1200	4,076
>1201	19,671
Total	136,546

Table 11. Boot lengths popularity.

Length (s)	Attacks	Booters
300	20,866	16
120	18,414	16
60	12,570	17
600	12,557	16
250	6,843	11
100	5,749	16
1800	5,280	10
90	5,205	11
500	5,093	14

53 (DNS) and 27015 (GoldSrc game engine). Port 80 is often used by DDoSaaS as a default value, probably because it is rarely filtered by firewalls. Conversely, several representatives of gaming services in the list of most popular target ports confirm *the prominent role of gamers* among DDoSaaS customers [2].

Table 12. Attack types popularity.

Type	Category	Attacks	Booters
UDP	UDP	69,635	11
ESSYN	TCP	19,744	3
NTP	UDP	19,416	2
SSYN	TCP	13,714	10
RUDY	HTTP	6,310	8
TCP	TCP	4,648	5
Slowloris	HTTP	2,958	8
UDPLAG	UDP	2,929	7
DRDOS	unknown	2,816	4

Table 13. Victim IP geolocation.

Country	Attacks
US	53,509
FR	15,811
UK	9,239
CA	6,901
DE	6,317
NL	4,962
AU	4,465
SE	2,622
Other	34,861

Geographic location of victim IP addresses suggests that DDoSaaSs are used primarily against North American and European targets (Table 13). Almost 39% of attacks are aimed at the US IP space, FR accounts for 11% and UK for 7%.

We analyzed the payment database records of the Quantum booter from September 2012 to March 2014. The database contains records related to 10,269 paying customers out of 20,695 registered. Mean payment was approximately 21 USD, with median and mode both 8 USD. Total income during the period exceeds 220,000 USD, while monthly income averages at 12,000 USD. That is a significantly higher income than the income reported from the twBooter analysis [2] (see 7). We expect that the prospect of such future income, coupled with few barriers to entry (see Section 5) will lead to an increasing number of DDoSaaS sites in the future.

5 Website source code analysis

DDoSaaS webpages are built with PHP and common frameworks, such as Bootstrap, jQuery, jQuery UI, jQuery Sparklines, Modernizr, prettyPhoto or Raphael according to our screening of 65 unique live websites.

We collected code from 53 DDoSaaS websites and analyzed them for similarities. All sites used PHP scripts, usually supported by the MySQL database. Each site consisted of 105 PHP source code files on average. We calculated the MD5 hashes of all PHP files and found 94 PHP files that were shared/reused (each) by at least 3 sites. We manually analyzed all the 94 shared files to understand their role and divided them into 7 categories. Table 14 summarizes our findings. Most shared source codes are files handling *user management and CAPTCHA*.

Table 14. Shared source codes categories.

Category	Files	Category description
user management	39	Managing user accounts and passwords, user logins
CAPTCHA	11	CAPTCHA
index pages	10	Index/home page + news/messages
lib	10	CCS, JavaScript, ...
attack management	7	Attack management + statistics...
PayPal	6	PayPal payments
misc	11	IP geolocation, IP logging, database access etc.

Finding similarities in source code files is not always trivial. The cryptographic hash algorithm MD5 can only find perfectly identical files. Even a slight change, such as rewriting an email address in a support ticket submission form, makes MD5 matching impossible. Therefore, we decided to also use the spamsum algorithm implemented in the ssdeep program [8]. The spamsum algorithm calculates context triggered piecewise hashes based on the FNV (Fowler/Noll/Vo) hash algorithm. The algorithm was used to find similarities in the source code of the 53 previously mentioned websites. We calculated how many source files across various sites have their ssdeep hash similarity score higher than 95. On average, each site shares at least one ssdeep hash with 7.45 other sites and has 46.5 ssdeep (>95) similarity relationships (i.e., shared similar files).

We have identified 9 similarity clusters. All websites in a cluster share 10 or more files with ssdeep similarity higher than 95. These 9 clusters were formed by 25 websites. Another 20 sites shared some of their files with others, but without distinctive partners. The remaining 9 sites did not share any similarities.

Such similarity might indicate that the same, or similar, teams are behind multiple services. Another reason might be simple code reuse. As the functionality required by most of the websites for a DDoS services is very similar, and as the source code of many web sites has leaked to the public, the coders of the web sites will be tempted to reuse the existing code. Availability of source code will lead to *an easier establishment of new DDoSaaSs.*

6 Economics

6.1 Payment methods

Desired properties of payment methods supported by DDoSaaS are user friendliness for technically unskilled users, anonymity for both seller and buyer and low fees, because exchanged payments are usually fairly small. Service providers also prefer payment methods that do not support payment revocation.

In December 2014, we analyzed payment methods supported by 82 DDoSaaS providers and found 19 different payment systems. The most popular system was PayPal, which was supported by 63 DDoS services, followed by Bitcoin (42) and Google Wallet (21). Contrary to findings in [5], WebMoney was not among supported payment systems of any DDoSaaS.

We have noticed *a distinct move towards the support of cryptocurrencies* during our research. Cryptocurrencies are anonymous, decentralized, gaining popularity among the general population, subjected to only limited regulation and payments cannot be revoked as soon as they are included in the blockchain. Bitcoin is now a widely accepted payment method among DDoSaaSs, but we also encountered support for Omnicoin, Litecoin and Dogecoin, mostly thanks to aggregating payment gateways such as GoCoin or CoinPayments.

Direct use of credit cards is very rare, supported by only 3 services. However, online payment services that allow the user to transfer money from his credit card or bank account to the service account are still common. Paypal, Skrill, Starpass, 4Virtuals, Okpay and Dwolla all fit into this category. With the exception of PayPal, at least one of these services was supported by 11 DDoSaaSs.

6.2 Subscriptions

DDoSaaS services provide a variety of subscriptions for different prices. Subscriptions are characterized by price, currency, subscription length, maximal boot time, attack concurrency and available attack bandwidth. Surprisingly, available attack bandwidth is rarely advertised. Some DDoSaaS services employ client-based botnets as their attack infrastructure. Limited knowledge about bandwidth and availability of particular hosts makes it difficult for service providers to estimate real available bandwidth at any given moment. Attack concurrency is similarly obscured by most services, although generally only one attack is permitted at a time if not otherwise stated.

Subscriptions are time-bound. During the subscription, a customer may initiate an arbitrary number of attacks. Monthly subscriptions are most popular, with more than 95% services offering these, followed by lifetime subscriptions offered by 66%. Price for monthly subscription varies between 1.99 and 35 USD for the cheapest and from 7.5 to 289 USD for the most expensive subscription.

Figure 1 shows samples of monthly subscriptions in USD. We can see that *the boot length/price ratio does not converge to a common value.* Monthly subscription with the same boot length can be ordered for considerably different

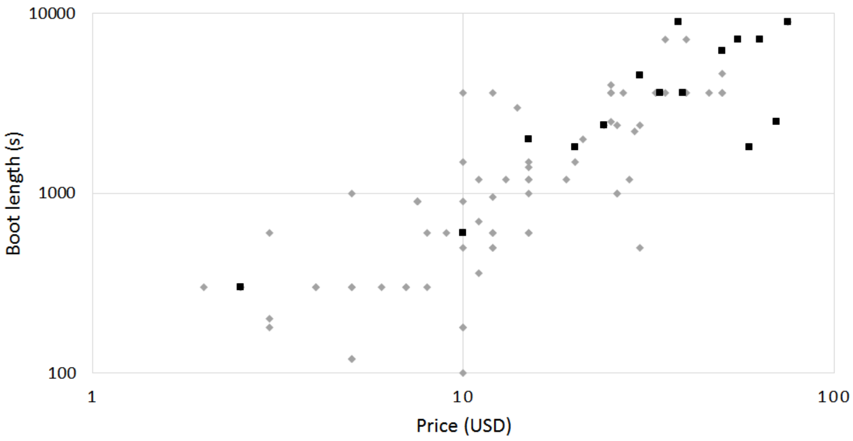

Fig. 1. Monthly subscriptions. Light rhombuses mark subscriptions with one concurrent attack. Dark squares mark subscriptions with two or more concurrent attacks. Graph scale is logarithmic.

prices at different services. Oppositely, increasing attack concurrency clearly increases the price of subscription. A combination of low subscription prices with unlimited attacks during the duration of subscription makes the per-attack price potentially extremely low.

In the case of payments via cryptocurrencies, subscriptions are activated automatically. When purchasing a subscription, the customer is offered several payment methods. Once the payment is successfully finished, the customer's requested subscription is activated without any further intervention from an operator. In the case of cryptocurrencies, automated subscriptions decrease the initial time for the customer to be able to launch attacks to a couple of hours at most. Elimination of a direct contact channel between the customer and the DDoSaaS operator also results in increased privacy for both parties.

7 Related work

The first academic paper that focused solely on DDoSaaS services was published by Karami and McCoy in 2013 [2]. The authors analyze the leaked database of the twBooter service and execute several simple attacks against their server. Key revelations are that the attack traffic is generated by servers, attack strength is sufficient to disrupt low to medium-sized web sites, primary service customers are gamers who prefer short attack lengths and most frequent targets are either game servers or game forums.

Yu et al. discuss the threat of DDoS attacks against cloud-based servers as a resource competition problem [9]. They observe that even though the cloud has enough resources to overcome DDoS attacks, the resources are not distributed as needed by customers. Specifically, virtual machine instances are usually reserved with fixed computational, memory and bandwidth limits. A DDoS attack may cause that these limits are exceeded, overwhelming the target instance.

The crimeware-as-a-service (CaaS) business model was investigated by Sood and Enbody [5]. In the CaaS model, roles for service creators and service operators are divided. The authors emphasize the importance of crime forums for advertising and e-currencies for exchange. Web Money is cited as an online payment system that is used extensively in the underground market. DoS attack order is described as a process when key communication between the seller and buyer takes place on an IRC channel.

Investigation into DDoS-for-hire services was highly publicized by articles that have been published by a well known computer security expert Brian Krebs (e.g., [10, 11]), who was also fairly successful in tracking several service owners. Krebs argues that most stresser services are operated by US citizens who possess a limited knowledge, rely on PayPal payment system and hide their webpages behind the CloudFlare content delivery network. The author also points out that the source code of DDoSaaS web pages may be frequently reused.

Shortly before submission of our paper, Santanna et al. published two studies about DDoSaaS [12, 13]. Our and their studies are complementary. In [12], authors analyze properties of 7 DNS-based and 2 CHARGEN-based DDoSaaS-generated attacks directed against a university network. Compared to their study: (1) We analyze the attacks from the perspective of a cloud-based server. (2) Our scope includes many more independent attacks with a greater variety of attack types. (3) We estimate the attack success rate and evaluate also the application layer traffic properties. Oppositely, [12] complements our paper with the investigation into the geolocation of reflectors and the discussion of a competition between various DDoSaaSs.

Second paper by Santanna et al. focuses on the analysis of booter databases [13]. The paper provides an extensive overview of DDoSaaS user/customer behavior, which fits in with our analysis of economical aspect of DDoSaaS, as well as information about the user location. Our aggregated database with more sources and more records also confirms observations of Santanna et al. that most attacks are shorter than 10 minutes and UDP-based attacks are the most popular.

8 Conclusions

Over the years, DDoS-for-hire services have matured into user friendly services with a wide customer base that extends beyond technically savvy users. Main advancements are automated subscription activation, automated attack execution and support for anonymous payment methods such as Bitcoin. The three key findings of our research are as follows:

- Attacks generated by DDoSaaSs are not overly powerful with bitrates only sporadically exceeding 1 Gbit/s.
- Attack traffic has a low complexity, does not employ randomization and shares similarities even between various DDoSaaSs.
- More than a third of attacks were not fully blocked by a cloud provider.

We believe that the threat of DDoSaaS will increase in time, mainly due to a low price, open advertisement, achievable anonymity and a service model that makes these services quickly and widely accessible to many potential customers. In the same time, the number of DDoSaaS services will grow, due to freely available source code and low initial entry costs when compared to potential earnings.

All collected attack traces are available at DDoS-Vault project webpage [3].

Acknowledgements

Authors would like to thank to Geraint Price for his comments and valuable suggestions. Vashek Matyas was supported by the Czech Science Foundation project GBP202/12/G061.

References

1. "SimilarWeb." Webpage. http://www.similarweb.com. Accessed: 2015-06-26.
2. M. Karami and D. McCoy, "Understanding the Emerging Threat of DDoS-as-a-Service," in *6th USENIX Workshop on Large-Scale Exploits and Emergent Threats*, 2013.
3. V. Bukac, "DDoS-Vault project," 2015. https://github.com/crocs-muni/ddos-vault/wiki. Accessed 2015-08-16.
4. Akamai, "The State of the Internet Report Q4 2014." Technical report, 2015.
5. A. K. Sood and R. J. Enbody, "Crimeware-as-a-service – A survey of commoditized crimeware in the underground market," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 28–38, 2013.
6. 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*, ACM, 2014.
7. PLXsert, "SSDP Reflection DDoS Attacks." PLXsert Threat Advisory, Sep 2014.
8. J. Kornblum, "Identifying almost identical files using context triggered piecewise hashing," *Digital investigation*, vol. 3, 2006.
9. S. Yu, Y. Tian, S. Guo, and D. Wu, "Can We Beat DDoS Attacks in Clouds?," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, 2014.
10. B. Krebs, "DDoS Services Advertise Openly, Take PayPal." http://krebsonsecurity.com/2013/05/ddos-services-advertise-openly-take-paypal/, May 2013. Accessed: 2015-08-16.
11. B. Krebs, "Lizard Kids: A Long Trail of Fail." http://krebsonsecurity.com/2014/12/lizard-kids-a-long-trail-of-fail, Dec 2014. Accessed: 2015-08-16.
12. J. J. Santanna, R. van Rijswijk-Deij, A. Sperotto, R. Hofstede, M. Wierbosch, L. Zambenedetti Granville, and A. Pras, "Booters – An analysis of DDoS-as-a-Service Attacks," in *Proceedings of the 14th IFIP/IEEE Symposium on Integrated Network and Service Management*, 2015.
13. J. J. Santanna, R. Durban, A. Sperotto, and A. Pras, "Inside booters: an analysis on operational databases," in *Proceedings of the 14th IFIP/IEEE Symposium on Integrated Network and Service Management*, 2015.