Inside Booters: An Analysis on Operational Databases

José Jair Santanna
University of Twente
j.j.santanna@utwente.nl

Romain Durban
INSA of Toulouse
romain.durban@gmail.com

Anna Sperotto
University of Twente
a.sperotto@utwente.nl

Aiko Pras
University of Twente
a.pras@utwente.nl

***Abstract*—Distributed Denial of Service (DDoS) attacks are an increasing threat on the Internet. One of the reasons is that websites selling attacks for prices starting from $1.00 are becoming popular. These websites, called *Booters*, facilitate attacks by making transparent the needed infrastructure to perform attacks and by lowering the knowledge to control it. As a consequence, any user on the Internet is able to launch attacks at any time. Although security experts and operators acknowledge the potential of Booters for DDoS attacks, little is known about Booters operational aspects in terms of users, attacks and infrastructure. The existing works that investigate this phenomenon are all restricted to the analysis of a single Booter and therefore provide a narrow overview of the phenomenon. In this paper we extend the existing work by providing an extensive analysis on 15 distinct Booters. We analyze their operational databases containing logs of users, attacks, and the infrastructure used to perform attacks. Among our findings we reveal that (i) some Booters have several database records completely equal, (ii) users that access Booters via proxies and VPNs performed much more attacks than those that accessed using a single IP address, and (iii) the infrastructure used to perform attacks is slightly different from what is known through existing work. The contribution of our work is to bring awareness of Booter characteristics facilitating future works to mitigate this phenomenon.**

I. Introduction

Distributed Denial of Service (DDoS) attacks aim to make a target host, service or network unavailable to its intended users. Those attacks are nowadays the number one threat on the Internet [1]. In addition, the amount of reported DDoS attacks increased by 47% compared to year 2013 [2]. One of the possible reasons for this increase is websites that provide DDoS attacks as a paid service, referred as Booters.

With a price starting from $1, everyone on the Internet is able to launch different types of DDoS attacks by using a Booter [3]. Those websites make their infrastructure transparent to their users, abolishing the need for technical skills to perform attacks. The simplicity, effectiveness, and availability of Booters are making them popular. Booters are becoming more often involved in attacks [4]. However, little is known about the operational aspects of Booters, such as who is accessing Booters, what attacks are requested and what the Booter backend infrastructure is.

Security experts have identified Booters operational databases as an effective source of information for getting a thorough understanding on the operational side of Booters. Those databases contain Booter operational information, such as logs of users, attacks, and the infrastructure used to perform attacks. Existing studies [5], [6], [7], [4], [8], however, are limited to a same database (i.e., booter.tw). Therefore, aspects that vary between Booters cannot be observed and a general overview is missing. For example, Booters can use different infrastructures types to trigger attacks [9].

Our goal is to provide a comprehensive overview on the operational side of Booters. To do so, we analyze 15 MySQL databases of Booters, found on the Internet, in terms of users, attacks, and infrastructure used to trigger attacks. Our main contributions are (*i*) to reveal characteristics of Booter users responsible for ordering attacks, (*ii*) give awareness about the characteristics of attacks ordered by users, and (*iii*) to shed light on the infrastructure used by Booters to trigger DDoS attacks. We believe that an in-depth understanding of how Booters are engineered can help to carry on mitigation tasks. We therefore conclude this paper with advices, based on our analysis, on how Booters attacks can be mitigated.

The remainder of this paper is organized as follows. In Section II, we survey the characteristics of existent analyses on Booter operational databases. In Section III, we discuss about correctness and ethical issues of the databases followed by a detailed description of the investigated databases. Then, we analyze the users, attacks, and the infrastructure used by Booters in Section IV. Finally, in Section V we provide our final considerations and advices for mitigation.

II. Survey of Booter database analyses

The goal of this section is to survey works that analyzed Booter operational databases. All works in this section analyzed the same leaked database of booter.tw (now booter.eu). This database became public after a series of DDoS attacks targeting a computer security blog (krebsonsecurity.com) [10] and the Ars Technica website (arstechnica.com) [11].

First, [5] analyzed booter.tw to investigate the identity of the user that attacked krebsonsecurity.com. Therefore, the paper describes the geolocation of this user, the different IP addresses used to access booter.tw, and the relation between those IP addresses and the TOR network. In addition, [5] reveals the amount, duration, and types of consecutive attacks against krebsonsecurity.com. [6] also describes some characteristics of the Booter user that attacked krebsonsecurity.com. Beside that, [6] geolocates the servers used by booter.tw to trigger attacks. Both works [5] and [6] allow to highlight the importance of analyzing operational databases to find who commissioned an attack.

To provide a general overview of booter.tw database, [7] analyzed the duration and type of all attacks found on the

978-3-901882-76-0 @2015 IFIP

TABLE I. SURVEY OF BOOTER DATABASE INVESTIGATIONS.

Investigated aspect	Thakorlal **[5]**	R.S. **[6]**	Schwarz **[7]**	Karami **[4],[8]**
krebsonsecurity.com attack	✓	✓		
User geolocation	✓	✓	✓	
User under several IPs	✓	✓		
User under anonymized IPs	✓			
User type (attack duration)				✓
User activity status				✓
User identity	✓			
Attack quantity	✓		✓	✓
Attack type	✓	✓	✓	✓
Attack duration			✓	✓
Attack concurrency				✓
Infrastructure status				✓
Infrastructure geolocation		✓		✓
Target geolocation			✓	
Target type			✓	✓
Booter profits				✓
Booter new users				✓

database, the geolocation and types of targets, along with geolocation of booter.tw users. However, the users geolocation methodology was inaccurate because it did not consider users using IP anonymization services, such as proxies, Virtual Private Networks (VPN) services, and TOR's network.

Finally, two similar works [4], [8] give a comprehensive understanding of the booter.tw database. However, the authors did not analyze aspects about the users that could help to identify the perpetrator. Beside that, and similar to [12], they analyzed attacks launched against their own infrastructure. Through this analysis they draw remarkable conclusions about the characteristics of Booter attacks, such as the amount of traffic generated by the attacks.

All aspects described above are summarized in Table I. Although the approaches used in the state of the art are often similar, and in some cases the analysis methodology is not completely clarified, we believe that each work presents valuable novelty on their analysis. However, there is room for improvement. For example, the way to count Booter users considering that some of them use a same email should be taken into consideration; also, the analysis on targets attacked several times by a same user should be performed to get a meaningful conclusions about attacks. In addition, more analysis should be done on the infrastructure used to trigger attacks. booter.tw based his infrastructure on servers and not on compromised machines, called as web-shell (more discussion in Section IV-C). However, some network security specialists [9] point list of web-shells as the main composition of the Booter infrastructure.

In general, the main weakness of the existing works is that they are restricted to booter.tw information. Therefore aspects such as the possible relation among different Booter attacks and victims of attacks, that can help to understand Booters and further mitigate them, cannot be observed. Our work extends most aspects addressed by previous works to several databases and correlates those sources of information.

III. BOOTER OPERATIONAL DATABASES

In this section we discuss the ethical aspects on using Booter operational databases and the authenticity of the data. After that, we describe characteristics of Booter databases as outcome of a preliminary analysis.

A. Ethical and consistency considerations

All 15 databases analyzed in this paper were retrieved from websites that publicly share hacked information on the Internet, such as pastebin.com and bitleak.net [1]. Following the discussion described in [8] that analyzed booter.tw database, one of the key points on using hacked information is to use it in an ethical fashion. Therefore, by using the same methodology as [8] to overcome ethical issues, we omitted all kind of personal information, such as email addresses and usernames, even when these details were known.

Another key issue, also addressed in [8], is the fact that the data are of unknown provenance. It implies an uncertainty on the completeness, and on the accuracy of the data. For example, [13] by interviewing a Booter owner (asylumstresser.com) describes that attacks were regularly deleted from the database. Therefore, each part of our analysis contains discussions about the consistency of the databases.

B. Overall database characteristics

Each of Booter databases analyzed in this paper contains at least 100 logs of attacks, which we believe is a representative number to analyze and compare operational characteristics.

Table II shows an overview of the investigated databases with a focus on verifying the time period of the available data records. The table is divided in three parts. The first one introduces general statistics about the databases, such as the domain name, the number of attacks, and the date of the first attack. The second part shows when Booter domain names have first been observed in DNSDB[2] and in DomainTools (whois.domaintools.com)[3] by using their history of domain names. Both tools have been used to verify the consistency of the available databases because they keep history of domain names. The last part of the table compares the differences between the first attacks in the databases and the oldest dates according to the two tools used.

According to the first part of the Table II, the dataset span is not proportional to the number of attacks. For example booter.tw has smaller dataset span than vaporizebooter.com, however the number of attacks is the opposite. It means that popularity is potentially also a factor that influences the usage of a Booter. However, Booters popularity will not be addressed in this paper. Another observation in the first part is that the operation time of those databases starts at least in 2011, such as for pandabooter.com and vaporizebooter.info. Concerning these two Booters, we observed that both first attacks were performed exactly at the same moment. However, by comparing

[1]Although it is straightforward to find those databases, the authors can provide the URLs to retrieve them.

[2]DNSDB is an online tool working with Passive DNS data since 2010 allowing requests to analyze the history of a domain name

[3]DomainTools is a website giving whois information about websites and keeping an history of it

TABLE II. OVERALL DATABASE CHARACTERISTICS AND VALIDATION

Booter domain name	Total Attacks	Dataset span* [days]	First attack	DomainTools	DNSDB	DNSDB - Domain-Tools	First attack - DomainTools	First attack - DNSDB
booter.tw	48844	403	24/01/13	13/07/12	14/12/12	154	195	41
legionbooter.info	38248	134	04/04/13	30/08/11	29/08/11	-1	583	584
pokeboot.com	6915	83	10/12/12	17/10/12	16/10/12	-1	54	55
superstresser.com	5565	36	12/02/14	04/04/13	02/04/13	-2	314	316
national-stresser.com	2756	93	05/09/13	03/05/13	01/05/13	-2	125	127
212-booter.net	1993	57	04/07/13	24/04/13	24/04/13	0	72	72
notoriousbooter.com	879	99	20/01/14	25/04/13	09/04/13	-16	271	287
vaporizebooter.info	725	971	05/09/11	22/05/12	29/09/12	130	-260	-390
xrshellbooter.com	629	41	19/03/12	27/10/11	26/10/11	-1	145	146
flashstresser.net	580	32	24/05/13	25/04/13	16/04/13	-9	30	39
Nullboot.net	343	65	20/01/14	18/11/13	20/11/13	2	64	62
panicstresser.com	209	0	30/07/12	12/07/12	11/07/12	-1	18	19
hazardstresser.com	173	88	15/03/13	27/04/13	11/04/13	-16	-43	-27
vstresser.com	157	423	01/02/13	06/05/13	07/05/13	1	-93	-94
pandabooter.com	104	258	05/09/11	09/05/12	08/05/12	-1	-247	-246

all databases we attested that both Booters share 90 records, consisting in 28 attacks and 62 records that are related to the infrastructure used to perform attacks. It means that at least one of the two Booters reused a database from another Booter. The only other case of shared records is xrshellbooter.com having identical records with pandabooter.com (34 records) and vaporizedbooter.info (4 records), which are related to the infrastructure.

Considering that we are aware that some Booters have records removed from their databases [13], we decided to investigate it by correlating domain names and dates with DomainTools and DNSDB. Firstly, we compare the information from both tools and confirm that in most cases they report a similar date, meaning that they observed the same behavior and then can be trusted. However, two Booters (booter.tw and vaporizebooter.info) have more than four months of difference. It could be a consequence of the measurement observation points of DNSDB and DomainTools. Secondly, in the third part of the Table II, by comparing the first attack date with both tools we discovered that for most of them the first attack was performed several months after the first observation by the tools. It means that i) either some data was deleted or ii) the attacks started to be performed after many days that a Booter was online. However, when the difference is bigger than months (e.g., legionbooter.info) the first option is the most suitable. A surprising observation is, once again, about vaporizebooter.info and pandabooter.com. Both Booters have attacks occurring long before the Booters have been seen online by the tools (among a few other Booters). It sustains our assumption that those Booters potentially copied their datasets from another Booter that was active a year before and shared its database or got hacked.

As expected, in a preliminary analysis we found that all MySQL databases have a similar schema, depicted in the Fig. 1. This observation helps us to perform a consistent comparison between Booters.

As depicted in Fig. 1, the generic database schema is mainly composed of six tables:

- **Users**: stores personal accounts on Booters, which contains a username and an email address;
- **Logins**: contains a set of IP addresses used by a user to login in a Booter;

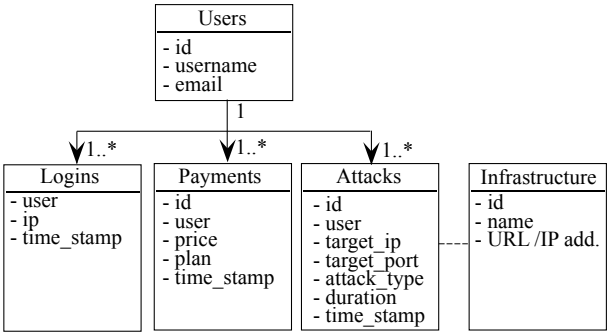


Fig. 1. Booter database generic schema

- **Payments**: consists of the amount of money paid by users. The amount paid is defined depending on an arrangement of (i) the maximum duration of attacks and (ii) a fixed period in which a user can perform attacks (plan_expiration);
- **Attacks**: stores records of attacks ordered by users. These logs contain at least three main aspects: (i) the target's identifier (e.g., IP address, URL or Skype username), (ii) the target's port number, and (iii) the date of the attack. In addition, some databases contain further details, such as the attack type, the attack duration, and the infrastructure used to perform attacks.
- **Infrastructure**: stores the list of URLs or IP addresses of intermediary systems used to launch the attacks (servers or web-shells).

Although our schema is composed of six tables, in general Booter databases have more tables. Furthermore, the names used in databases can be different from what we described on our schema. However, the structure of all investigated Booter databases still follows the described schema.

IV. DATABASES ANALYSIS

In this section we analyze and compare the content of the Booter databases. The analysis is divided in three parts: users, attacks, and the infrastructure used by Booter to perform attacks. Each part has a distinct methodology based on investigating information of the Booter database tables. Tables

'users', 'logins' and 'payments' will be used to analyze the behavior of Booter users (Section IV-A). Table 'attacks' is used to analyze characteristics of attacks (Section IV-B) and to compare with the 'infrastructure' table. This last comparison reveals the relation between the attacks offered and the infrastructure used (Section IV-C).

A. Booter users

First of all, it is important to differentiate users and customers of Booters. A user is a person that created an account on a Booter. A customer is a user that purchased services on Booters. These two terms are used to differentiate these two categories in the following sections. Our methodology to differentiate unique users is based on the email address or the user unique identifier. Table III summarizes quantitatively differences between both categories based on the analysis of the database tables 'users','payments' and 'attacks'.

Table III shows for each database the number of users and customers, the subgroup of users/customers that performed one or more attacks (called attackers), and the amount of money paid by customers to Booters. By comparing different Booters, the number of attacks neither is proportional to the number of users nor to the amount of money profited. For example, booter.tw has far less users (312) and customers (80) than superstresser.com (2,236 users and 684 customers) but performed almost 9 times more attacks and earned 1.6 more than the latter. Another observation is that the number of customers is significantly smaller than the number of users. It means that many users are just attracted to take a look at what Booters can offer. Meanwhile a few users are interested in becoming customers and performing attacks.

The most notable observation on Table III is that the number of users that performed attacks (users that paid and launched attacks) is higher than the total number of customers (except for superstresser.com and panicstresser.com). Although it is possible that some users had privileges allowing them to order attacks without paying, it is more likely that some payments records are missing. The best example that proves the second hypothesis is showed by superstresser.com, for which the payment table contains only records from middle 2013, but the attacks records start at the beginning of 2012.

Another observation that emphasizes the removal of records is the number of customers that launched attacks that is smaller than the overall number of customers. Although it is entirely possible that some customers never launch any attack, we believe this to be unlikely in such a large proportion. Therefore, we suspect that some users that launched attacks have seen their payments records removed, preventing them to be classified as customers.

TABLE III. BOOTER USERS OVERALL INFORMATION

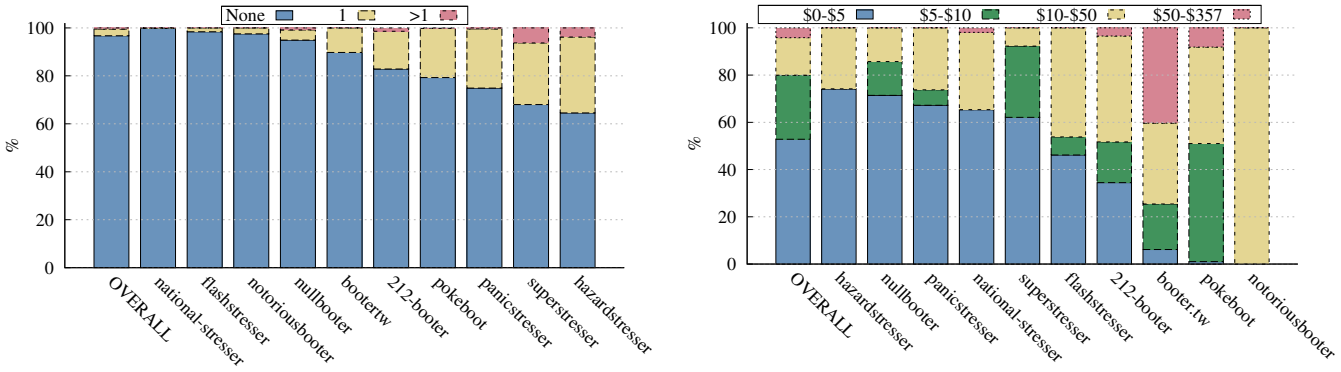
Booter	Total users	User attacker	Customers	Customer attacker	Profits [USD]
booter.tw	312	277	80	26	8127.00
superstresser.com	2236	163	684	135	4885.00
pokeboot.com	464	194	96	94	2181.00
panicstresser.com	235	25	57	11	615.00
212-booter.net	140	57	28	24	509.00
national-stresser.com	1892	81	46	-	497.00
hazardstresser.com	79	24	28	-	307.00
flashstresser.net	749	66	13	7	165.00
notoriousbooter.com	81	22	2	-	37.00
nullboot.net	118	26	6	-	31.00

In the next subsection, we analyze in details the payments made by customers, the usage of strategies to hide the real identity of users.

1) Payments: By analyzing the payments characteristics we give awareness about the customer choices in terms of Booter offers. Our methodology for this analysis is based on the payments database table in which is shown at least the amount paid, the date of the payment, and the email of the customer. Therefore, 5 Booters that did not provide this information were excluded from our analysis (i.e., vaporizebooter.info, legionbooter.info, xrshellbooter.com, vstresser.com, and pandabooter.com).

Fig. 2(a) shows, for each Booter separately and on the overall of all surveyed databases, how many times users purchase attacks from Booters. As expected the number of users that did not pay is far larger than the number of customers. However, the most surprising information is that a user rarely paid twice to perform attacks. Note that when a user pays to a Booter, he is paying to perform as many attacks as he want during a specific time interval, called as expiration date. Therefore we can conclude that i) Booter users are satisfied to perform a set of attacks, or ii) payments records have been removed too often to observe users buying again later.

By analyzing only Booter customers (not users in general)



(a) Payments per user.

(b) Amount paid.

Fig. 2. Payment.

TABLE IV. USER IP ADDRESS(ES) AND ATTACKS

Booter domain name	1 IP	2 IPs	≥3 IPs	Sum users IPs	Total Users	Attack related 1 IP	Attack related 2 IPs	Attack related ≥3 IPs	Sum attacks related IPs	Total Attacks
booter.tw	64	34	191	289	312	3,392	1,055	44,382	48,829	48,844
legionbooter.info	230	31	29	290	23113	11,053	4,020	2,879	17,952	38,248
pokeboot.com	52	19	40	111	464	503	493	1,091	2,087	6,915
superstresser.com	379	79	141	599	2236	494	832	4,005	5,331	5,565
national-stresser.com	9	5	3	17	1892	64	29	8	101	2,756
212-booter.net	99	21	33	153	140	364	802	815	1,981	1,993
notoriousbooter.com	2	0	2	4	81	29	0	0	29	879
flashstresser.net	522	66	114	702	749	136	89	346	571	580
nullboot.net	5	0	2	7	118	146	0	56	202	343
hazardstresser.com	14	7	8	29	79	21	0	13	34	173

we show in Fig. 2(b) how much they were willing to pay for attacks. In overall, more than 50% of all customers paid $5.00 or less to perform attacks. This is an important finding because the existing works, all based only on booter.tw, have a slightly different observation about the price charged by Booters. Through this analysis we highlight that although Booters offer several prices to perform attacks, the cheapest ones are the most chosen by users. notoriousbooter.com and nullbooter.net results are less representative because their number of customers is very small, 2 and 6 respectively.

Another observation in Fig. 2(b) is that only 4 Booters offer attacks that were purchased for more than $50. For those Booters we also found interesting customers outliers. For example booter.tw earned $3,000 in almost 1 day with only 2 customers. Our hypothesis to explain this is that it is most probably due to failure in the payments that lead to a record but that it is not a real benefit for the Booter (two email addresses tried repeatedly to pay the exact same amount during a short period of time). In another extreme we found 6 users in booter.tw database that appeared in the payment table but in fact paid nothing ($0.00) to perform attacks. It is explained because this Booter, in special, has promotional campaigns allowing a user to perform attacks for free.

2) IP adresses, TOR, VPN and proxy usage: The goal of this section is to analyze how Booter websites were accessed to figure out if users are trying to hide their activities. This analysis was motivated by related works (see Section II) that mentioned Booter users using VPN and proxies. Our methodology is divided in three steps. Firstly, we observe the number of unique IP addresses used by each user, assuming that users logging in using several IP addresses are most likely using VPN or proxies. Secondly, we focus on analyzing users that used TOR[4] by correlating the IP addresses of logins with the list of exit-nodes of TOR. Exit-nodes are the exit of the TOR network to the Internet. TOR exports the list of exit-nodes every hour since February 2010 and this list can change through time. At last, we analyze the countries resolved from the IP addresses. This analysis should emphasize the users that are using an intermediary service to hide themselves. Our assumption is that a user can not (in theory) be in multiple countries around the world in a short period of time. All analyzes in this subsection are based on investigating the 'logins' table from Booter databases.

Table IV summarizes the number of users that access Booters using one, two, and three or more IP addresses. Then, we show the sum of users that have IP address records stored in the database to compare with the total number of users. In the same table, we also show the number of attacks performed by users that accessed Booters via a single IP address, 2, and 3 or more. At last, we show the sum of attack related to IP addresses and the total number of attacks.

The first observation is that, in general, the number of users that access Booters with a single IP address represents the largest fraction. For example, superstresser.com have almost 2.6 times more users that access Booters with one IP address than the ones that access with three. A possible reason could be that most of the users (53%) accessed Booters only once in the analyzed datasets. However, it is very interesting to observe that users that access Booters with 3 or more IP addresses generated far more attacks than the first group. For instance users that access superstresser.com with three IP addresses launched almost ten times more attacks than the users that access them with a single IP address. It means that users that perform more attacks are more likely to take precautions in hiding their real IP address.

The exception of having users related to several IP addresses performing more attacks is legionbooter.info users. Note that for this Booter the number of attacks related to one IP is far bigger than related to three IPs. However, the number of users missing is representative, calculated via the difference between the total number of users (23,133) and the users related to IP addresses (290). In addition the difference between the total number of attacks and the attacks related to IP addresses is also representative. It gives us indications that possibly a large number of records were removed. Slightly different from legionbooter.info, the Booters booter.tw, 212-booter.net, and flashstresser.net are very consistent, meaning that (even if some records were removed) the number of users and attacks matches with the relation of user IP addresses and the number of attacks related to those IP addresses.

After analyzing the relation between attacks and ways that users access Booters, we analyze how many of them accessed using TOR. Table V summarizes our findings.

Table V shows Booter users that used TOR one or more times to login in a Booter. In addition, the table shows the number of logins made by those users and how many among those logins were realized by using TOR. Finally, we describe the number of attacks launched by those users and the ratio between attacks and number of users.

We are very surprised to observe that only 4 Booters were

[4]TOR is free software that helps users to defend against traffic analysis and censorship, that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

TABLE V. DETAILS PER BOOTER ABOUT USERS USING TOR

Booter domain	Total Users	TOR users	Login TOR users*	Login with TOR	Attack TOR users	Attack /TOR users
superstresser.com	2236	8	256	82	205	25,6
booter.tw	312	7	9128	146	3595	513,6
flashstresser.net	749	4	255	13	24	6
xrshellbooter.com	374	1*	1*	1*	26	26

found having users that used TOR. Even more surprised to notice that the number of users that used TOR to access Booters (20) is insignificant in comparison to the total number of users. However, as explained earlier, those users performed far more attacks than the average of users. For example, the users that access booter.tw via TOR performed 513 attacks each, on average (opposed to 31 attacks for all users with logins information). Note that for xrshellbooter.com we had only the last login IP address for all users. Even though, this Booter user performed 26 attacks, that we consider a reasonable number of attacks.

Note that the number of users that access Booters with more than 1 IP address (according to Table IV) is far bigger than the number of users that used TOR. This means that some users are taking precautions, but also that there are still users using several IP addresses without using TOR. This does not exclude that they could also use others services, others VPN or proxies. We refined the analysis of the count of IP addresses per user by resolving the addresses to retrieve the Authoritative Server (AS) and the corresponding country, which has a low probability to have changed in the last year. Reasoning in term of countries allows to solve the issue of a user accessing a Booter from legitimate different locations (home, school, work, WiFi etc.) and also the dynamic IP addresses allocation from their ISP.

Table VI shows our findings in terms of geolocation of IP addresses per countries and attacks. As expected, the number of user IP addresses related to one country is bigger than the other two options. It happened because the number of logins related to one IP address (in Table IV) is also the biggest one. However, surprisingly most of attacks are related to a single country, not to $\geq$3 countries (except for booter.tw). It means that our assumption that users that access Booters with different IP addresses are using VPN and proxies is not completely true. This happens because, as written before in this section, a user can access from different places where there is an Internet connection (e.g., home and school). Even though, it is still clear that some users access Booters via VPN and proxies because they originated from several countries. Furthermore, the most important finding showed in Table VI is that the proportion of attacks by these users, logging in from several countries, is significantly higher than those logging in from a single one.

Note that the analysis on countries is much less significant than on the IP addresses analysis. If we consider that users logging in from a single country are not using any VPN or proxy, then it could mean that many customers are ordering attacks without trying to hide themselves. This confirms our previous hypothesis that minorities of customers are performing more attacks and are taking precautions. But above all, this also shows that a large number of customers are performing less attacks but apparently without taking any precautions. This means that their activity could be more easily detected and mitigated.

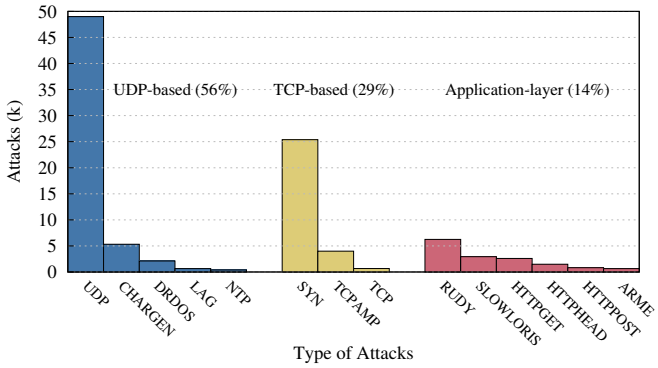


Fig. 3. Attack types

B. Attacks

In this section we characterize attacks ordered by Booter users to provide an overview of what kind of attacks have been the most chosen. Firstly, we observe the types of attacks that were recorded in the databases. Secondly, we analyze how attacks were performed over time (i.e., in consecutive or parallel way). At last, we study the duration of attacks.

1) Attack types: To investigate the types of attacks the most chosen by users, we analyze records from the database attacks table. Since the names of attacks vary from a Booter to another, we clustered the types of attacks into three categories. Firstly, UDP-based attacks is a category that includes Distributed Reflection DoS attacks (DRDoS), such as attacks based on CharGen, DNS, and NTP, but also what they advertise as "UDP" which can be a pure UDP flood or any type of attacks relying on the UDP protocol. TCP-based attacks are the second category of attacks. It includes SYN flood, "TCP" and "TCPAMP" attacks. Both categories (UDP and TCP-based) relying on protocols from the transport and network layer to perform attacks. The last category is the Application-layer attacks, which includes RUDY, SLOWLORIS, ARME, and HTTP-based attacks (HEAD/POST/GET). There are others types of attacks found in databases but ignored in our analysis because they were too vague terms to be classified in a category, such as "SMALL1", "test", and "FULL-POWERED-ATTACK".

The rationale behind clustering attacks in categories is that we are aware that Booters advertise some types of attacks but perform a more specific attack. For example, [4] shows that although booter.tw advertises attacks as "UDP", however this Booter performs DRDoS attacks based on DNS and CharGen. Note that users are not aware about which specific attack types are performed by Booters. This information about the attack performed is restricted to Booter owners.

Fig. 3 shows the sum of all attack types clustered per category. Note that the number of UDP-based attacks is almost double than others. It was not surprising that UDP and SYN flood attacks were the most popular among users. This is because we expect that Booters follow the same trend of DDoS attacks on the Internet [1].

TABLE VI. USER COUNTRIES RELATED TO ATTACKS

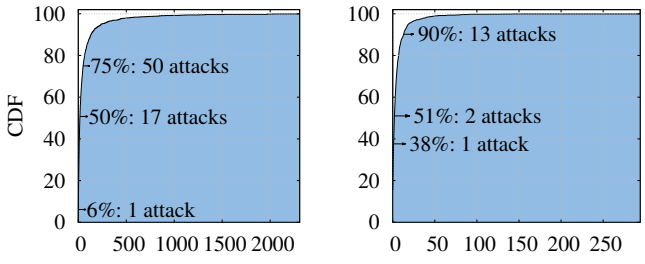
Booter domain name	1 Country	2 Countries	≥3 Countries	Attacks related 1 country	Attacks related 2 countries	Attacks related ≥3 countries	Attacks / 1 country	Attacks / 3 country
booter.tw	172	57	60	14,131	6,336	28,362	82,2	473
legionbooter.info	272	14	4	15,923	1,171	858	58.5	215
pokeboot.com	81	18	12	1,280	510	297	15.8	25
superstresser.com	499	56	30	2,396	1,735	1,196	4,8	40
national-stresser.com	13	2	2	93	-	8	7.2	4
212-booter.net	146	7	0	1,475	506	-	10.1	-
notoriousbooter.com	3	0	1	29	-	-	9.7	-
flashstresser.net	631	49	22	338	150	83	0.5	4
nullboot.net	6	0	1	153	-	49	25.5	49
hazardstresser.com	20	6	3	22	12	-	1.1	-

2) Attacks usage: To understand how users chose attacks and how often do they perform them, we analyze the history of attacks for customers. Fig. 4(a) and 4(b) show cumulative distribution of the overall and over time results, respectively. According to the overall analysis (Fig. 4(a)), only 6% of customers performed a single attack. It means that users do not buy a package of attacks to perform a single attack but to keep attacking targets, into the period of their package expiration. Another finding is that 25% of users perform more than 50 attacks, which is a representative number of attacks.

By analyzing attacks over time (Fig. 4(b)) we notice that 38% of users do not perform consecutive attacks. On average, users performed only one attack per day. It is remarkable that 10% of users that perform more than 13 attacks also performed consecutive attacks against on a same target (investigated in the next subsection). We also found some outliers, such as a single user that ran 2,308 attacks in ∼8 days, which on average represents 294 attacks per day.

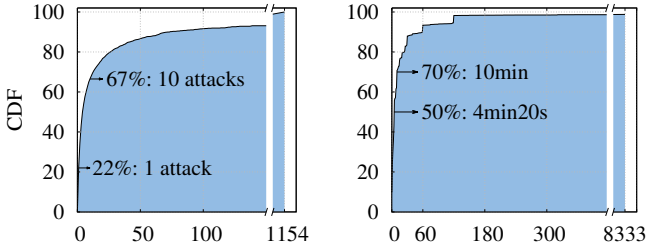
By analyzing attacks on a the same target by a same user (Fig. 5(a)), we notice that only 22% of the attacks targeted only once a same target by a same user. Consequently, it means that most of users performed two or more attacks against a same target. Note that 67% of the attacks have been launched at least 10 times on a same target by the same user.

If we analyze the probability for an attack to be re-launched on the same target less than 5 minutes after the end of the previous one, we can see that 58% of attacks have been at least repeated once more, as showed in Fig. 5. The attacks seem to be chained to produce a longer one, 19% of all attacks are part of a DDoS campaign of at least 5 consecutive attacks. This behaviour makes more sense when we analyse the duration of the attacks. As we can see on Fig. 5(b), attacks are usually short. 70% of them last less than 10 minutes. An explanation



(a) Overall. (b) Per day.

Fig. 4. Attacks per user



(a) Attacks on the same target (b) Attacks duration CDF

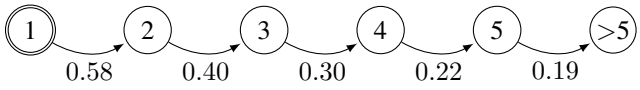


Fig. 5. Probability for attacks to be relaunched less than 5 minutes later

for it is that the prices for short term attacks (less than 10 min) are lower than for longer attacks.

By analysing attacks we also notice that 32% of consecutive attacks have been launched in parallel. It indicates that new attacks against a same target started before the end of a current one. This means that most of the time, customers are willing to deal as much damage as possible to their target and for a longer period of time.

C. Booter infrastructures

Our final analysis on operational Booter databases regards the infrastructures used to perform attacks. Although previous works describe the Booter infrastructure as based on servers (see Section II), by analyzing records from the infrastructure database table we had a completely different observation on that. Table VII shows for each Booter the number of web-shells and servers listed in the infrastructure database table, together with the types of attacks performed. Note that "UDP(+)" means that a Booter perform UDP-based attacks including DRDoS.

Surprisingly, all Booters, except booter.tw, had their infrastructure based on *Web-shells*, which is completely different from what the related work conclude. Web-shells are scripts hosted on machines (compromised or not) that are accessed via HTTP/GET or HTTP/POST and expect parameters to launch attacks, such as the target's IP address or URL, the duration of the attack, the destination port, and (sometimes) the type of attack. For example, in *http://example.com/web-shell.php?host=yourwebsite.com&time=30&port=80* a web-

TABLE VII. BOOTER INFRASTRUCTURE

Booter domain name	Web-shell		Servers	Attacks types
	GET	POST		
booter.tw	-		15	UDP, TCP, App-layer
superstresser.com	2		-	UDP(+), TCP, App-layer
notoriousbooter.com	1		-	UDP(+), TCP, App-layer
212-booter.net	1		-	UDP(+), App-layer
flashstresser.net	7		-	UDP, TCP
panicstresser.com	4		-	-
hazardstresser.com	2		-	-
legionbooter.info	16	-	-	UDP(+), TCP, App-layer
vaporizebooter.info	209	-	-	-
pandabooter.com	466	139	-	-
xrshellbooter.com	134	64	-	-

shell hosted in example.com will perform an attack against yourwebsite.com, during 30 seconds, on port 80.

By analyzing the name of scripts we notice that most of them are PHP scripts[5]. An interesting observation, showed in Table VII, is that web-shells (in theory) can cover all types of attacks (UDP, TCP, and Application-layer attacks), such as superstresser.com. However, according to [9], DRDoS attacks can not be covered by web-shells (or at least no web-shell has been found with these characteristics). It is not possible (yet) because to perform this type of attacks machines running web-shells need to have a list of other services that will be mislead to perform attacks, such as DNS and NTP services. It means that only Booters that have their infrastructure based on servers can be used to perform DRDoS attack. Consequently, it implies that notoriousbooter.com, superstresser.com, 212-booter.net, and legionbooter.info that perform DRDoS attacks should also have their infrastructure based on servers but the URL to access it might be hard coded (written in the source code), not in the database.

A last observation is that, although booter.tw did not offer DRDoS attacks, we already wrote in the previous subsection that this Booter performed DRDoS attacks based on DNS and CharGen instead of pure UDP attacks. So, it makes even more sense booter.tw infrastructure is based on servers.

V. FINAL CONSIDERATIONS AND RECOMMENDATIONS

In this paper we conducted a structured analysis of 15 Booter operational databases, which allowed us to gain insights on how Booters are used. Our analysis indicates that Booter operational databases are often incomplete and sometimes inconsistent and their content should therefore be used *cum grano salis*. For this reason, in several parts of our analysis we were not able to provide a definitive explanation of our observations, instead of it, we draw many hypothesis to encompass the uncertainty of those databases. However, we have also shown that the such operational databases are a valuable source of information about how Booter are used in practice and offer valuable insights that can help to mitigate this phenomenon.

The picture that emerges from the analysis conducted in this paper is that Booters are a phenomenon with very distinct characteristics. From the one side, we found the majority of users accessing Booters with a unique IP address, willing to pay less than $ 10, performing attacks with less then 5 minutes duration, and targeting a few URL or IP addresses. This is in line with our initial hypothesis that Booters are in use among users with limited skills. On the other side, we also found harmful users that hide themselves via VPN and proxies, accessing Booters using hundreds IP addresses from dozens of countries, willing to pay several hundreds of dollars to perform hundreds of attacks per day, often against the same target.

Our recommendations are as follows: *i)* considering that most of the users seem to take little precaution when accessing Booters, we advice to implement URL filtering based on Booter domain names. This practice has been adopted by our partners at CERT SURFnet and the University of Twente, and has successfully stopped several users that access Booters. As a consequence of this practice, however, the number of users that access Booters via VPN or proxies (therefore from an unfiltered connection) might increases.

ii) by using a more effective but more complex mitigation strategy, we recommend to directly mitigate the Booter infrastructure. In particular, we suggest to perform a campaign against web-shells, since our study shows that web-shells are currently the preferred infrastructure. Removing web-shells or blacklisting them is likely to mitigate a large fraction of the attacks. However, this is not a straightforward task, and further research is needed for creating and maintaining a comprehensive list of web-shells.

iii) we advise to mitigate DRDoS. To the best of our knowledge, web-shells are not able (yet) to perform DRDoS attacks as they do not contain the list of reflector and amplifier services (such as DNS, NTP, and CharGen). For this type of attacks, Booters rely on servers and the possibility of forging IP addresses (IP spoofing) that do not belong to the originating network. To overcame this type of attacks we advise the implementation of Best Current Practice (BCP38) proposed by Internet Engineering Task Force (IETF) [14]. This practice proposes an implementation of ingress-filtering rules to block all traffic from IP addresses that do not belong to the address space of the originating network.

[5]The list of web-shells were removed from this paper for legal/ethical reasons but can be retrieved by requesting the authors

ACKNOWLEDGMENT

This work was funded by the Network of Excellence project FLAMINGO (ICT-318488), which is supported by the European Commission under its Seventh Framework Programme. Special thanks go to Farsight Security for assisting us in providing valuable information.

REFERENCES

[1] Arbor Networks, "DDos Attacks: the Scale of the Problem," https://www.brighttalk.com/webcast/9053/83657.

[2] Akamai, "The State of the Internet (Q3 2013)," http://www.akamai.com/dl/akamai/akamai-soti-q313.pdf.

[3] J. J. Santanna and A. Sperotto, "Characterizing and Mitigating The DDoS-as-a-Service Phenomenon," in *8th International Conference on Autonomous Infrastructure, Management and Security*, ser. AIMS'14, 2014.

[4] M. Karami and D. McCoy, "Understanding the Emerging Threat of DDoS-as-a-Service," in *6th UNSENIX Workshop on Large-Scale Exploits and Emergent Threats*, ser. LEET'13, 2013.

[5] V. Thakorlal, "Analysis of DDoS Service Database used to attack Brian Kreb's Website," http://vijayjt.blogspot.nl/2013/04/analysis-of-ddos-service-database-used.html.

[6] Rever Security, "Analysis of the Booter.tw Database," http://www.reversecurity.com/2013/03/analysis-of-bootertw.html.

[7] D. Schwarz, "Digging Through an Administrative Network Stressor Providers Database," http://www.arbornetworks.com/asert/2013/03/digging-through-an-administrative-network-stressor-providers-database/.

[8] M. Karami and D. McCoy, "Rent to Pwn: Analyzing Commodity Booter DDoS Services," *USENIX ;login:*, 2013.

[9] Prolexic, "Prolexic Threat Adviory - DDoS Booter Shell Scripts," http://www.prolexic.com/kcresources/prolexic-threat-advisories/prolexic-threat-advisory-ddos_Booter-scripts_041912/Prolexic_Threat_Advisory_DDoS_Booter_Scripts_052612.pdf.

[10] B. Krebs, "The World Has No Room For Cowards," http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/w.

[11] S. Gallagher, "Details on the denial of service attack that targeted Ars Technica," http://arstechnica.com/security/2013/03/details-on-the-denial-of-service-attack-that-targeted-ars-technica/.

[12] J. J. Santanna, R. Rijswijk-Deij, A. Sperotto, M. Wierbosch, L. Granville, and A. Pras, "Booters - An Analysis of DDoS-as-a-Service Attacks," in *14th IFIP/IEEE Symposium on Integrated Network and Service Management (accepted)*, ser. IM'15, 2015.

[13] B. Krebs, "The Obscurest Epoch is Today," http://krebsonsecurity.com/2013/03/the-obscurest-epoch-is-today/.

[14] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," BCP 38, 2000.