Booter websites characterization: *Towards a list of threats*

Justyna Joanna Chromik, José Jair Santanna, Anna Sperotto, and Aiko Pras

[1]University of Twente - The Nederlands
Design and Analysis of Communication Systems (DACS)

j.j.chromik@student.utwente.nl,{j.j.santanna,a.sperotto,a.pras}@utwente.nl

Abstract. *Distributed Denial of Service (DDoS) attacks mean millions in revenue losses to many industries, such e-commerce and online financial services. The amount of reported DDoS attacks has increased with 47% compared to 2013. One of the reasons for this increase is the availability and ease of accessibility to websites, which provide DDoS attacks as a paid service, called Booters. Although there are hundreds of Booters available, current researches are focused on a handful sample of them - either to analyse attack traffic or hacked databases. Towards a thorough understanding and mitigation of Booters, a comprehensive list of them is needed. In this paper we characterize Booter websites and demonstrate that the found main characteristics can be used to classify Booters with 85% of accuracy. The Dutch National Research and Education Network (SURFnet) has been using a list generated by our methodology since 2013, what demonstrates high relevance to the network management community and the security specialists.*

1. Introduction

Distributed Denial of Service (DDoS) attacks are considered number one operational threat on the Internet. DDoS attacks aim to make a target machine, service or network unavailable to its intended users. To perform powerful attacks, attackers (mis)use hundreds or even thousands of distributed sources, such as infected computers or misconfigured servers. For many industries, such as e-commerce and online financial services, DDoS attacks are especially devastating. To those industries, DDoS attacks cause millions in revenue losses, reputation damage, and customer attrition [Arbor Networks 2014, Ponemon Institute 2014].

The amount of reported DDoS attacks has increased with 47% compared to 2013 [Akamai Technologies 2014]. One of the reasons for this increase is the effectiveness, simplicity and availability of websites that provide DDoS attacks as a paid service, called *Booters*. These websites offer attacks for a very cheap price, for instance, less than 5 USD [Karami and McCoy 2013], powerful enough to put most of small and medium-sized enterprise companies' websites offline [Santanna et al. 2015b]. Researches on mitigation of Booters phenomenon focus basically in two areas: (i) characterising the attacks [Santanna et al. 2015b] and (ii) analysing the leaked databases [Santanna et al. 2015a]. Although both of them have a clear contribution towards Booter mitigation, in order to address the whole phenomenon (not a particular set of Booters), they fail in a key element: a relevant, updated, and extensive list of Booters.

In order to help security specialists to retrieve such list and get a thorough understanding about the Booter phenomenon, the goal of this paper is to reveal the main characteristics of Booter websites. By using those characteristics we show that a Booter list can be retrieved with high accuracy. The main contributions of this paper are the following:

- To provide a relevant set of search terms to retrieve URLs related to Booters and a crawler to retrieve all needed information of the websites, such as the structure, visual and textual content, and the WHOIS information (Section 3).
- To reveal the 9 main characteristics of Booter websites, achieved by an extensive analysis of features used to classify websites (Section 4).
- To demonstrate that the 9 main characteristics of Booter websites can classify Booter with an accuracy of 85% (Section 4.6).

Since 2013, a Booter list generated based on our methodology have been used by the Dutch National Research and Education Network (SURFnet) to observe the users accessing Booters and their correlation with attacks. This is just one example that demonstrates high relevance of our work to the network management community and the security specialists. Only by knowing the threats we can mitigate them.

2. Related work

In the literature there is no work related to Booter websites classification. Therefore, in this section we focus on approaches that classify generic websites based on features. Although the existing approaches have several different goals we focus on specifically three of them: (i) approaches that classify the subject or type of a website [Lindemann and Littig 2006, Rajalakshmi and Aravindan 2011, Lindemann and Littig 2007, Kovacevic et al. 2004], (ii) approaches that aim to filter websites [Jo et al. 2013, Hammami et al. 2006], and (iii) approaches that aim to generate blacklists [Ma et al. 2009]. The features used in those approaches could possibly be used in Booter area. The list of features that we found is the following:

1. **URL**: this feature discloses the overall composition of a URL. Usually a URL is composed of three elements: (i) network application protocol, (ii) the URL host name, and (iii) the URL path name. For example, in *http://www.domainname.tld/path/to/the/article.html*, 'http://' is the protocol, 'www.domainname.tdl' is the host name, and '/path/to/the/article.html' is the path name.
2. **Website structure**: is a feature that reveals, among others, two aspects: (i) the website depth level and (ii) the number of known pages of a website. The former is a terminology defined by us that analyses the number of slashes ('/') a URL path has. For example, the URL *http://www.domainname.tld/path/to/the/article.html* has depth level '4'. The latter aspect is the number of indexed webpages that have the same host name and are reached by Google Search engine. For example, the number of know pages is 2 if Google Search returns 2 pages that contain a same *www.domainname.tld*, such as *www.domainname.tld/1.html* and *www.domainname.tld/2.php*.
3. **WHOIS**: is a feature that reveals information of domain names, such as (i) the registration date, (ii) the owner, (iii) the nameservers related to that domain name, and (iv) the entity responsible for the domain registration (i.e., registrar).

4. **Page content**: is a feature that reveals the elements of a website such as (i) the textual description, (ii) the meta data, and (iii) the visual content, (e.g., buttons, tables, and figures).

In Table 1 we summarize the features that each work addresses to classify websites. Such table shows that most of the existing works focus on the URL, website structure, and the website content. WHOIS and visual content are less popular, but definitely worth investigating. Therefore, in the next section we investigate those four features to characterize Booters.

Paper	URL	Website structure	WHOIS	Website content		
				Textual	Meta	Visual
[Lindemann and Littig 2006]		x			x	
[Rajalakshmi and Aravindan 2011]	x					
[Lindemann and Littig 2007]	x	x				
[Jo et al. 2013]	x		x	x	x	
[Hammami et al. 2006]		x		x	x	x
[Ma et al. 2009]	x	x	x			
[Kovacevic et al. 2004]						x

Table 1. Website features used to characterize websites.

3. The search terms, legal considerations, and our crawler

To investigate the four features described in the previous section, firstly we describe our methodology to define a list of search terms that we use to retrieve Booter websites. We give a special attention to the first search term that we found: "stresser", because it lead us to some legal considerations. After that we describe a crawler that we develop to investigate Booter websites features.

3.1. The first search term and legal considerations

In order to find a list of search terms, with which we can retrieve Booter websites, we started using the most obvious term: "booter". By using such term we found many URLs related to the word "stresser". By definition, Booters should be different from stressers. Booter is a website that provides DDoS attacks as a paid service [Santanna and Sperotto 2014], while by definition a stresser is a company (usually accessed via a website) that provides stress testing on a given system [Rouse 2007].

Both definitions are almost the same because performing a DDoS attack is a way to "stress test" a target system. However, note that stressers aim to intentionally test their customers' systems beyond regular operational capacity, while Booters are used by their clients to "stress test" a third party service. Another important characteristic is that (in theory) stressers perform their tests deliberately and in a test lab, not affecting other entities.

Putting the theoretical definitions aside, we compare the services offered by both, a Booter and a stresser. To do so, we analyse the top one result for the search terms "booter" and "stresser". We decide to anonymize the URL/names of the Booter and the stresser to avoid legal or ethical implications. Table 2 shows our findings.

Attack types		Booter A	Stresser B
Layer 3&4	TCP	✓	
	SSYN	✓	✓
	ESSYN	✓	
	UDP	✓	✓
	UDP-LAG	✓	✓
	DRDoS		✓
	CHARGEN	✓	
Application layer	GET	✓	
	HEAD	✓	
	POST	✓	
	RUDY	✓	✓
	ARME	✓	✓
	SLOWLORIS	✓	✓

Table 2. Services offered by a Booter and a stresser

The first observation is that technically the Stresser B offers the same resource exhaustion actions (attacks) as Booter A. The second observation is that both offer most of the known types of DDoS attacks, which target the Layers 3&4 and the application layer. Our paper has no intention to describe how each type of attack works, for more information see [Mirkovic and Reiher 2004]. The third observation is that although Booter A does not explicitly offer Distributed Reflection Denial of Service (DRDoS), CHARGEN is a type of DRDoS. Therefore, both Booter A and Stresser B offer the strongest type of DDoS attacks reported nowadays. Finally, we notice that Stresser B has no restriction in relation to the target of "stress test". Given this freedom, the customers can perform attacks against third party services. Therefore, through these four observations we conclude that Stresser B is also a Booter.

The question that arise is: why Booters advertise themselves as stressers? The answer, which we found in hacker forums and many blogs, is that Booters want to avoid legal problems by hiding illegal actions (DDoS attacks using compromised machines) behind legal services (stress testing) [Kassner 2013, Musthaler 2012]. Booters have another strategy to avoid legal problems. Instead of advertising themselves as stressers, they include in their websites Terms of Services (ToS). It is a legal agreement composed by a set of rules that clients need to follow to use their services. Table 3 shows parts of ToS found on Booters.

	Terms of Service statements
Booter C	"We are not responsible for how ever you use this stresser"
Booter D	"Illegal activity which occurs in your account is [...] associated to you"
Booter E	"Anything you do while on Booter E is your own responsibility"

Table 3. Examples of text included in Terms of Service

We observe in Table 3 that Booters clearly do not take any legal responsibilities for user's actions, although their core business is to offer DDoS attacks against anyone and anything connected to the Internet. The legal aspect of Booters is a nudging subject, which requires attention, but will be out of the scope of this research. From technical point

of view we see that stressers are used as Booters. Because of this we use term "stresser" in the set of terms to retrieve Booter websites. In the next subsection we describe how did we find the other search terms.

3.2. The other search terms

To find other terms we search on Google for materials related to Booters and stressers. Through an extensive literature we found other two terms: *"ddos-for-hire"* [Krebs 2013a] and *"ddoser"* [Safe Keys 2013]. Finally, by using the two former terms ("booter" and "stresser") and the later terms ("ddos-for-hire" and "ddoser") we search the literature using Google Scholar. This Google service aggregates most of the the digital libraries, academic publishers, and repositories worldwide, including IEEE Xplore Digital Library and ACM Digital Library. Through Google Scholar, and closing our set of terms, we found "ddos-as-a-service" [Karami and McCoy 2013]. Note that the reference on the side of earlier mentioned terms is not necessarily the first to use/define these terms, but the place that we have found them.

3.3. Our crawler

After defining the five search terms (*"booter", "stresser", "ddos-for-hire", "ddoser", and "ddos-as-a-service"*), in this section we describe our approach to retrieve a list of URLs related to Booters and the additional information needed to classify them according to the four website features (described in Sec. 2). To do so, we develop a crawler to fulfil the following requirements:

1. Retrieve as many URLs related to Booters as possible based of the list of search terms. These retrieved URLs are called in this paper as "potential Booters".
2. Extend the URLs retrieved in the previous requirement to include all known pages related to these URL domain names.
3. Retrieve the WHOIS information of the URL domain names.
4. Download the Booter website content.

In order to retrieve the URLs related to Booters (first requirement), we use a python search script [1]. This approach was chosen over other approaches [2][3][4] because it is not limited on the amount of results able to retrieve (e.g., 24 URLs). To find all web pages related to a website (second requirement) we use the Google Search with operator "site:". This operator returns as result only URLs within the domain requested, for example the output of *"site:name-of-potential-booter.com"* is a list of pages (URL paths) in the domain *"name-of-potential-booter.com"*.

To retrieve the WHOIS information (third requirement) we use pythonwhois package [5]. Although such library is able to return more than 20 different information about a domain name, in our WHOIS analysis (Sec. 4.4) we only use 4 of them: (i) the creation date, (ii) the registrar of the domain name, (iii) the nameservers that the domain is pointing to, and (iv) the contacts of the domain administrator. To fulfil the last requirement and

[1] http://breakingcode.wordpress.com/2010/06/29/google-search-python/
[2] http://googolplex.sourceforge.net/
[3] http://www.catonmat.net/blog/python-library-for-google-search/
[4] http://googlesystem.blogspot.nl/2008/04/google-search-rest-api.html
[5] http://cryto.net/pythonwhois/

download the content of Booter websites, we firstly decide that we should keep our identity anonymous. This precaution was taken because a security specialist was successively attacked after starting investigating Booters [Krebs 2013b]. Therefore, we use The Onion Router (TOR) network that enables online anonymity by encrypting and bouncing the traffic through networks and open relays severs. Secondly, another requirement needed to download the potential-booter-webpages is to support JavaScript. To do so, we use the Selenium browser[6], which is a library that emulates a generic Web browser and therefore is able to support JavaScript.

In summary, our crawler was build to attend the requirements to analyse Booters. Although we use specific libraries and APIs to build our crawler, these were our decisions on how to fulfil the requirements. Therefore other libraries can be used. Note that our crawler can be extended to perform an automated classification of Booter websites, but first the characteristics of the website features should be analysed. More ideas about future works are written in the last section of this paper.

4. Analysis on Booter websites features

In this section we analyse the features of Booter websites. Firstly we describe the list of URLs (Sec. 4.1) used to perform our analyses. Secondly, we describe our analysis based on the URL characteristics (Sec. 4.2), the website structure (Sec. 4.3), the WHOIS information (Sec. 4.4), and the website content (Sec. 4.5). We close this section highlighting the features that are more representative to classify Booters (Sec. 4.6).

4.1. The list of URLs

By using the search terms and our crawler described in the previous section (Sec. 3.3) we retrieved 1238 URLs, on 15th September 2014. From these 1238, 230 URLs were retrieved by using the term "booter", 370 by using "stresser", 265 "ddoser", 199 "ddos-for-hire", and 174 "ddos-as-a-service". In order to verify if these search terms are representative and distinct we analyse the intersection of retrieved URLs, showed in Table 4.

Search Terms	booter	stresser	ddoser	ddos-for-hire	ddos-as-a-service
booter	**230**	13	3	1	1
stresser	13	**370**	3	0	0
ddoser	**3**	3	**230**	1	1
ddos-for-hire	1	0	1	**174**	11
ddos-as-a-service	1	0	1	11	**199**

Table 4. Intersection of retrieved URLs based on different search terms

Based on Table 4 we notice that our search terms are distinct: very small number of same URLs are retrieved using different search terms, for example only 3 URLs were retrieved using the terms "booter" and "ddoser". " We are aware that our crawler did not retrieve all URLs related to those search terms because each search process was interrupted by a HTTP error (i.e., 503: service unavailable). Although our chosen approach retrieves more URLs than other current approaches, Google Search is still able to detect and block our crawler. Even though, the retrieved list of URLs is sufficient enough to analyse Booters features, since it contains both Booter and non-Booter websites.

[6]http://www.seleniumhq.org

4.2. URL analysis

Based on the list with 1238 URLs we analyse the first feature found in our survey: the URL composition. Table 5 shows a summary of the types of URLs found.

URL Type	URL	# URL retrieved
1	potential-booter.com	71
2	potential-booter.com/login.php	1167
3	www.domain.com/potential-booter	
4	potential-booter.domain.com	

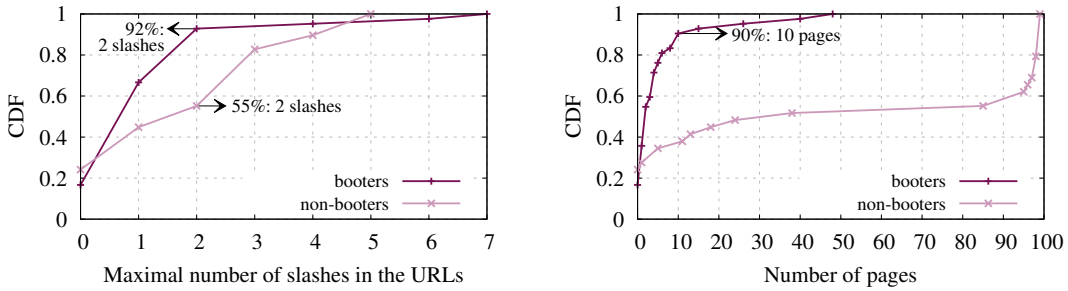
Table 5. Examples of retrieved URLs

In Table 5 we observe four different types of URLs: with only a host name (type 1), with host name and path (type 2), where Booter is a page of a website (type 3), and where a Booter is a subdomain of a domain name (type 4). We want to focus on the URL type that has the highest probability to be a Booter. Note that often URLs type 2 are subpages of URLs type 1. Thus, we decide to analyse only the type 1. Although URLs type 3 and 4 can potentially contain Booters, we noticed that it is more likely that they provided information about Booters, not the websites themselves.

Each one of the 71 URLs type 1 are later called as *potential Booter*, and they will be further classified. After a manual analysis of those potential Booters we found that 42 are Booter websites and 29 are non-Booter websites. All the further sections will be based on the 71 potential Booters.

4.3. Website structure analysis

After the filtering process described in the previous section, we analyse the structure of these 71 potential Booters. Figure 1 summarizes our findings.



(a) Depth of websites.

(b) Known pages.

Figure 1. CDF of website structure aspects.

In Figure 1, graphs of the Cumulative Distribution Function (CDF) of the website structure are shown. While Figure 1(a) shows the CDF of depth level of these 71 website, Figure 1(b) shows the CDF of the known pages. Both graphs show the results for Booters and non-Booters (classified manually in the previous section). We observe in Figure 1(a) that 92% of Booters have their website depth up to 2 levels, whereas only 55% of non-Booters have the same depth. Considering Figure 1(b) we observe that 90% of Booters have 10 or less pages. In addition, Booter websites never exceed 50 known pages, what is

an interesting observation that can be used to eliminate non-Booters from a set of URLs (that in this analysis is almost 50%).

By in depth analysis of the 71 potential Booters we notice that some page names appear more than once, such as “register”, “ToS”, “plans”, “buy”, and “hub”. The number of times we observed those pages is shown in Figure 2. We notice that pages as Terms of Service (ToS) and “registration” are more often appearing when analysing Booters. Almost 60% of Booters have a registration page (24/42) and around 40% of Booters have ToS page (17/42).

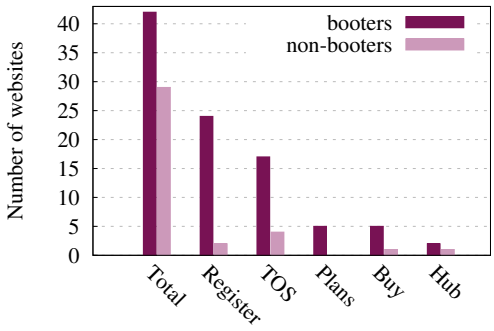


Figure 2. Page names analysis.

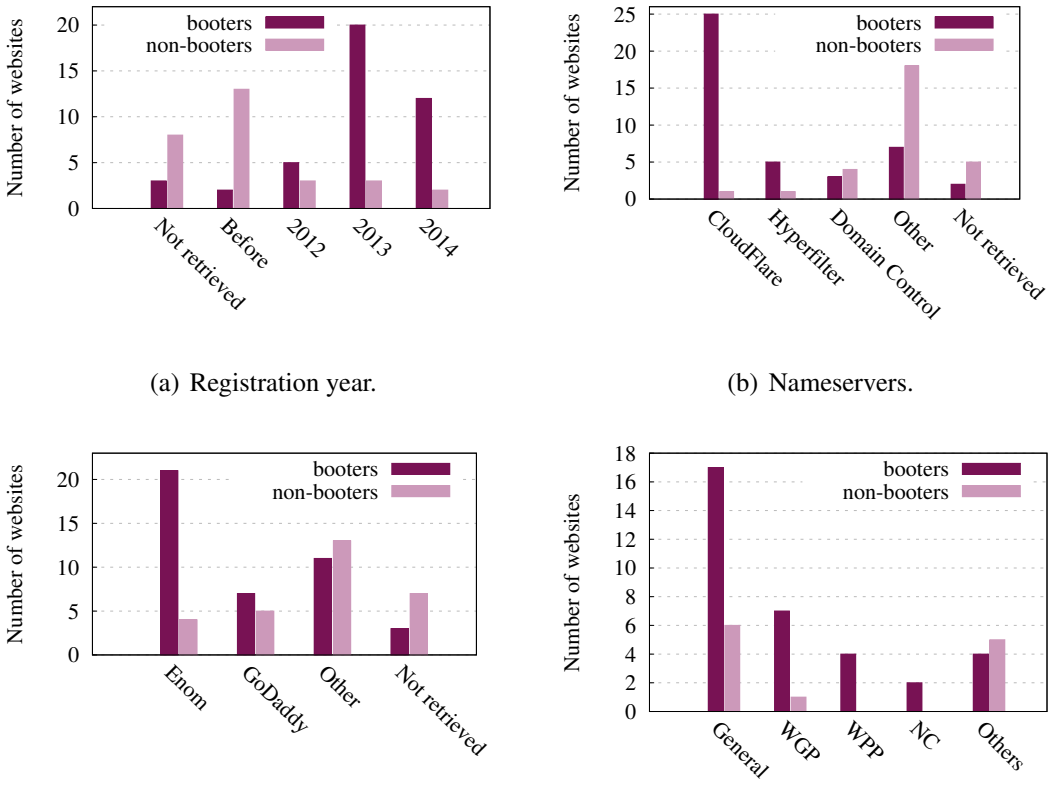
The other page names on the Figure 2, plans, buy, and hub, are not that promising. For example only 5 out of 42 Booters had pages referring to plans or redirecting to purchase page (buy). Although the page “hub” is crucial to Booters, because through that page a user can start an attack, it was found only twice. The reason for that could be that this page is accessible only after logging into the Booter and it is not indexed by Google.

4.4. WHOIS analysis

After analysing the website structure we check the WHOIS information of the 71 potential Booters retrieved by our crawler. We present our findings in Figure 3.

In Figure 3 we observe four different information related to WHOIS. From the first one, in Figure 3(a), we observed that more than 88% of the Booter domain names (37/42) were registered in 2012 (5), 2013 (20), and 2014 (12), whereas a bit less than half of the non-Booter websites were registered before 2012 (13/29). Overall, it shows that most of the Booters by our crawler are relatively new. By analysing the namesevers of the retrieved Booter domain names, showed in Figure 3(b), we are not surprised to observe that almost 60% of Booters (25/42) are associated to CloudFlare. It was already pointed out in [Santanna et al. 2015b] that Booter subscribe services from CloudFlare to be protected against DDoS attacks from the competitors (other Booters). However, we are surprised to observe another company offering DDoS protection, Hyperfilter. It is the first time that this company is observed in this phenomenon. Also in Figure 3(b), we confirm that majority of non-Booters have more variety in nameservers (18/29).

By analysing the companies that provide the domain registration (registrar), showed in Figure 3(c), we notice that half of Booters (21/42) have their domain registered with Enom, which is a known domain registrar. This is probably because of cheap



(a) Registration year.

(b) Nameservers.

(c) Registrar.

(d) Contact of the domain name owner.

Figure 3. WHOIS information.

price, but also because Enom offers the "WhoisGuard" service used for hiding the contact details. This information is more evident when we look into the contact of the responsible for the domain names. In Figure 3(d) we observe that more than 40% of Booters (17/42) have their contact hide from the WHOIS information. Usually the contact is hidden by many services, among them: "WhoisGuard Protected" (WGP - 7/42), "Whois Privacy Protect" (WPP - 4/42), and "NameCheap" (NC - 2/42).

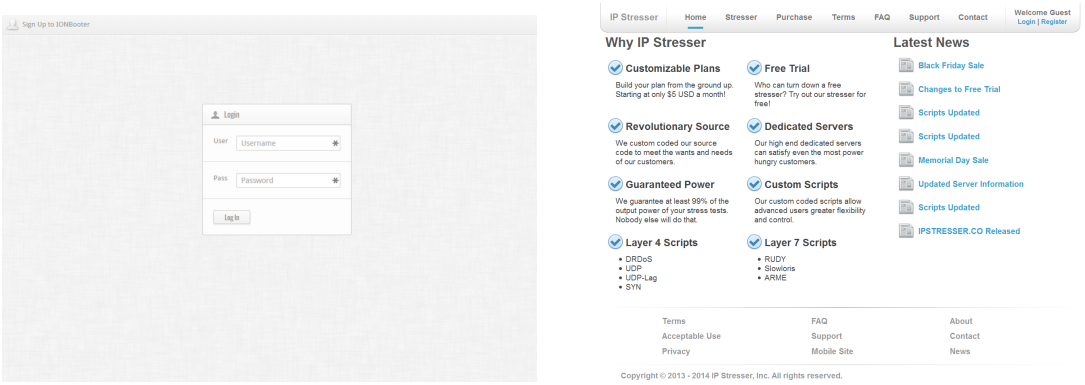
4.5. Website content analisys

The last feature that we use to characterize Booter websites is based on their content analysis. This analysis is divided in two parts: (i) the visual interface and (ii) the meta data, that is: the description and the keywords used to define Booter websites.

4.5.1. Visual interface

By manually accessing the 42 Booters we notice that they have only two completely different types of first page: or (i) a very simple first page containing a simple login interface, for example showed in Figure 4(a), or (ii) a verbose page full of textual content and appealing advertisements, for example shown in Figure 4(b). For both types Booters provide a very simple and user-friendly interface. The most remarkable finding related

to the visual interface was that while more than a half of Booters (22/42) has a “login” button in their main page only 1 non-Booter has such button.



(a) Booter F - login page.

(b) Booter E - login page.

Figure 4. Examples of login pages.

4.5.2. Meta data

When we look into meta data used to define Booters, almost 62% (26/42) has neither description nor keywords, showed in Figure 5. This result is very similar and consistent with the simplicity of Booters visual interface (described in the previous section). We also observe that there is not a clear distinction between non-Booters that use meta data. Therefore, although the meta data can help on the understanding the purpose of a website, because of insufficient information, we can not use this feature to define if a website is a Booter or not.

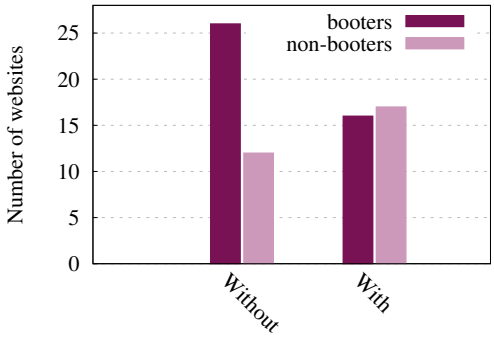


Figure 5. Meta data.

Note that in theory meta data is fundamental to have a better positioning in search engines, such as Google Search. Therefore we decide to correlate the popularity of a Booter with the existence or not of meta data. To do so we use the Alexa’s Rank [7] to get information about the 42 Booter webpages. By doing so, in general we observed that Booters with meta data have a higher ranking, for example in Table 6 two Booters are

[7] http://www.alexa.com

shown. Booter E that has meta data was ranked around the 273k position, while Booter F had a thousand times lower position. Note that the highest Alexa's Rank value is 1 (that usually has Google or Facebook).

Name	Meta data		Alexa's Rank
	Description	**Keywords**	
Booter E	Powerful and Affordable Stress Testing	stresser, denial of service, dos, ddos, dr-dos, syn, ssyn, udp, sudp, udp-lag, rudy, slowloris, arme	272.979
Booter F	-None-	-None-	2.580.782

Table 6. Examples of Booter meta data and their popularity

We are aware that meta data is not the only determining factor to have a higher ranking in the Internet. However, we are positively surprised to observe a clear relation between both factors.

4.6. A summary of the representative Booter features and a brief validation

The goal of this section is to summarize the most relevant features of Booters, which are based on what did we learn from our analysis. In addition we perform a brief validation to show that those features can be used to classify Booters.

In Section 4.2 we conclude that URL type 1, i.e. those that are composed by only the URL hostname, are more suitable to be a Booter. In Section 4.3 we notice that all Booters have less than 50 subpages and in general 2 levels of depth. We also observed that websites, which have pages "register" and "tos" are more often Booters. When it comes to WHOIS information, in Section 4.4, we highlight that Booters tend to use services from DDoS protection companies, such as CloudFlare or HyperFilter. The domain names used by Booters are most likely registered in 2012 or later, and the used registrar is most likely Enom. Moreover, information about the owners of Booters is hidden using services such as "WhoisGuard". Finally, in Section 4.5.1, we showed that Booters often have a simple interface with a login button. Through those observations we define a list with the main features that has a higher change to classify generic URLs as Booter websites:

1. Number of pages less than 50.
2. Depth level of the website of maximum 2.
3. Presence of registration page.
4. Presence of terms of service page.
5. Domain creation time 2012 and later.
6. Obfuscated WHOIS data.
7. Protected by a DPS.
8. Specific registrar: Enom.
9. Login button on page.

We decide to analyse if indeed the list of features can be used to classify Booters. To do so, we collected 3248 URLs related to Booters using the the search terms (Sec. 3.2) and our crawler (Sec. 3.3), on 30th November 2014. After filtering URLs based on URL type 1, we found 156 to perform a manual classification. From the manual classification we found 87 Booters websites and 69 as non-Booters. Then, for each one of the 156 URLs we count how many of the 9 features they have. The results are shown in Figure 6

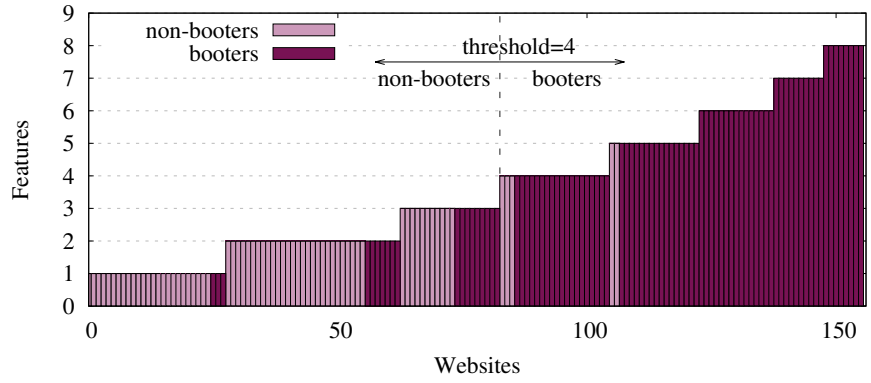


Figure 6. Representative features related to Booters per websites.

Table 7. Accuracy of threshold used to classify Booters

Threshold	True Positive	True Negative	Accuracy	False Positive	False Negative
3	78	52	**83%**	16	10
4	**69**	**63**	**85%**	**5**	**19**
5	50	66	**74%**	2	38
6	33	68	**65%**	0	55

The results in Figure 6 show clearly that the more features related to Booters a website has, the higher is the chance that such website is a Booter. Then, in the future, those features indeed can be used to automate the classification of Booters. However, the only problem that future researchers will have to determine where the threshold of features should be placed. Table 7 show the the accuracy of the threshold of our analysis.

Based on the retrieved URLs and our 9 features we found that URLs that have 4 or more features (threshold 4) show better results in terms of accuracy ((true negative +true positive)/population), 85%. Although this result is very promising, further research should be done to increase the accuracy.

5. Conclusion and Future work

By aiming to help security specialists to retrieve a comprehensive list of Booters, we performed a thorough characterization of Booter websites. First, we discovered the most common features to analyse websites. Then, we developed a crawler to retrieve a representative set of URLs and additional information to perform analysis. After an extensive analysis we highlight the 9 main characteristics of Booter websites. Finally, by using those characteristics we demonstrate that a list of Booters can be retrieved and classified with 85% of accuracy.

We conclude that although the 9 features are representative in the classification of Booter websites, more research needs to be done to achieve a fully automated methodology to retrieve a comprehensive list of Booters. As a future work, we aim to extend the number of retrieved URLs by adding additional sources of information, such as hacker forums, twitter, and youtube. Moreover, the analysis should include URLs type 3 and 4.

More research should be done to improve accuracy, for example by in depth analysis of the meta data or by assigning weights to the features. Since we expect Booters to

evolve, we consider further investigation of the analysis using machine learning. Moreover we urge for investigating the legal aspects of what is allowed as stress testing, including definition of procedures for authentication and verification of identity of people using these services.

Acknowledgments

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.

References

[Akamai Technologies 2014] Akamai Technologies (2014). Prolexic Quarterly Global DDoS Attack Report (Q1 2014). http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q1.html.

[Arbor Networks 2014] Arbor Networks (2014). The Risk vs. Cost of Enterprise DDoS Protection. http://pages.arbornetworks.com/WebsiteRiskvsCost_Ent_DDoS_Protection.html.

[Hammami et al. 2006] Hammami, M., Chahir, Y., and Chen, L. (2006). Webguard: A web filtering engine combining textual, structural, and visual content-based analysis. *Knowledge and Data Engineering, IEEE Transactions on*, 18(2):272–284.

[Jo et al. 2013] Jo, I., Jung, E., and Yeom, H. Y. (2013). Interactive website filter for safe web browsing. *Journal of Information Science and Engineering*, 29(1):115–131.

[Karami and McCoy 2013] Karami, M. and McCoy, D. (2013). Understanding the Emerging Threat of DDoS-as-a-Service. In *6th USENIX Workshop on Large-Scale Exploits and Emergent Threats*. USENIX.

[Kassner 2013] Kassner, M. (2013). What's better than creating your own DDoS? renting one. http://www.techrepublic.com/blog/it-security/whats-better-than-creating-your-own-ddos-renting-one/.

[Kovacevic et al. 2004] Kovacevic, M., Diligenti, M., Gori, M., and Milutinovic, V. (2004). Visual adjacency multigraphs-a novel approach for a web page classification. In *Proceedings of SAWM04 workshop, ECML2004*.

[Krebs 2013a] Krebs, B. (2013a). Ragebooter: 'Legit' DDoS Service, or Fed Backdoor? http://krebsonsecurity.com/2013/05/ragebooter-legit-ddos-service-or-fed-backdoor/.

[Krebs 2013b] Krebs, B. (2013b). The world has no room for cowards. http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/.

[Lindemann and Littig 2006] Lindemann, C. and Littig, L. (2006). Coarse-grained classification of web sites by their structural properties. In *Proceedings of the 8th annual ACM international workshop on Web information and data management*, pages 35–42.

[Lindemann and Littig 2007] Lindemann, C. and Littig, L. (2007). Classifying web sites. In *Proceedings of the 16th international conference on World Wide Web*, pages 1143–1144.

[Ma et al. 2009] Ma, J., Saul, L. K., Savage, S., and Voelker, G. M. (2009). Beyond blacklists: learning to detect malicious web sites from suspicious URLs. In *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1245–1254.

[Mirkovic and Reiher 2004] Mirkovic, J. and Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53.

[Musthaler 2012] Musthaler, L. (2012). DDoS-as-a-Service? You Betcha! It's Cheap, It's Easy, and It's Available to Anyone. `http://www.securitybistro.com/?p=4121`.

[Ponemon Institute 2014] Ponemon Institute (2014). Cyber Security on the Offense: A Study of IT Security Experts. `http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf`.

[Rajalakshmi and Aravindan 2011] Rajalakshmi, R. and Aravindan, C. (2011). Naive bayes approach for website classification. In *Information Technology and Mobile Communication*, pages 323–326. Springer.

[Rouse 2007] Rouse, M. (2007). Stress testing. `http://searchsoftwarequality.techtarget.com/definition/stress-testing`.

[Safe Keys 2013] Safe Keys (2013). Top 10 DDoSer's (Booters, Stressers. `http://www.safeskyhacks.com/Forums/showthread.php?39-Top-10-DDoser-s-(Booters-Stressers)`.

[Santanna et al. 2015a] Santanna, J. J., Durban, R., Sperotto, A., and Pras, A. (2015a). Inside booters: an analysis on operational databases. In *14th IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*. <to appear>.

[Santanna and Sperotto 2014] Santanna, J. J. and Sperotto, A. (2014). Characterizing and mitigating the ddos-as-a-service phenomenon. In *8th IFIP International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2014)*, pages 74–78.

[Santanna et al. 2015b] Santanna, J. J., van Rijswijk-Deij, R., Sperotto, A., Hofstede, R., Wierbosch, M., Granville, L. Z., and Pras, A. (2015b). Booters - an analysis of ddos-as-a-service attacks. In *14th IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*. <to appear>.