HAL
archives-ouvertes.fr

Characterizing and Mitigating the DDoS-as-a-Service Phenomenon

José Santanna, Anna Sperotto

▶ To cite this version:

José Santanna, Anna Sperotto. Characterizing and Mitigating the DDoS-as-a-Service Phenomenon. Anna Sperotto; Guillaume Doyen; Steven Latré; Marinos Charalambides; Burkhard Stiller. 8th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS), Jun 2014, Brno, Czech Republic. Springer, Lecture Notes in Computer Science, LNCS-8508, pp.74-78, 2014, Monitoring and Securing Virtualized Networks and Services. <10.1007/978-3-662-43862-6_10>. <hal-01401293>

HAL Id: hal-01401293
https://hal.inria.fr/hal-01401293

Submitted on 23 Nov 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Characterizing and Mitigating The DDoS-as-a-Service Phenomenon

Jair Santanna and Anna Sperotto

Design and Analysis of Communication Systems (DACS)
University of Twente
Enschede, The Netherlands
{j.j.santanna,a.sperotto}@utwente.nl

Abstract. Distributed Denial of Service (DDoS) attacks are an increasing threat on the Internet. Until a few years ago, these types of attacks were only launched by people with advanced knowledge of computer networks. However, nowadays the ability to launch attacks have been offered as a service to everyone, even to those without any advanced knowledge. *Booters* are online tools that offer *DDoS-as-a-Service*. Some of them advertise, for less than U$ 5, up to 25 Gbps of DDoS traffic, which is more than enough to make most hosts and services on the Internet unavailable. Booters are increasing in popularity and they have shown the success of attacks against third party services, such as government websites; however, there are few mitigation proposals. In addition, existing literature in this area provides only a partial understanding of the threat, for example by analyzing only a few aspects of one specific Booter. In this paper, we propose mitigation solutions against DDoS-as-a-Service that will be achieved after an extensive characterization of Booters. Early results show 59 different Booters, which some of them do not deliver what is offered. This research is still in its initial phase and will contribute to a Ph.D. thesis after four years.

1 Introduction

On March 2013, a Distributed Denial of Service (DDoS) attack almost broke the Internet [1]. The attacker was able to control up to 300 gigabits per second (Gbps) of network traffic and exhaust the communication resources of several hosts and networks, by misusing several services on Internet. Historically, DDoS attacks can be launched only by using advanced technical skills of the attackers, such as computer programming and specific knowledge of computer networks. These skills allow attackers to control several hosts and services with vulnerabilities on the Internet and perform attacks.

However, nowadays, a phenomenon is becoming popular: DDoS attacks are offered as a service (i.e., *DDoS-as-a-Service*), allowing everyone, even those without any kind of advanced knowledge, to launch attacks. Referred to on the Internet as *Booters*, these online tools offer several types of DDoS attacks, with different firepower (network throughput), often by charging low prices, such as

25 Gbps for U$ 5. In addition, *Booters* provide extra services which reduce even more the knowledge needed for customers to perform attacks, such as a *Skype resolver* that discovers the IP address based on the name account of a Skype user.

Booters have gaining in popularity on the Internet and have been used to perform DDoS attacks against several third party services, such as government websites [2], personal websites [3], and game servers [4]. Although increasingly popular [5], the existing literature brings only a partial understanding of the threat [6] [7] [8] [9], for example by analyzing the characteristics of only a single *Booter*, even though a survey of the offered services had allowed us to identify 59 *Booters* (as shown in Section 3).

DDoS-as-a-Service is not a new type of DDoS attack, but several existing types of DDoS attacks. To mitigate just one specific type of DDoS attack is a great challenge. To mitigate several different types, as Booters offer, poses an even greater challenge. In this research we aim to provide an extensive characterization of *Booters* and propose mitigation solutions against DDoS-as-a-Service. In addition, this research will contribute to the understanding of different types of DDoS attacks found nowadays, and characterize the changes in cyber-attack communities.

The remainder of this paper is organized as follows. Section 2 will discuss the research questions, followed by a description of our proposed approach. After that, closing this paper, we provide early results of our research in Section 3.

2 Goal, Research Questions, and Approach

The goal of our research is **to characterize and mitigate the *DDoS-as-a-Service* phenomenon**. To pursue this goal, we have defined the following research questions (RQ) as the basis of our research:

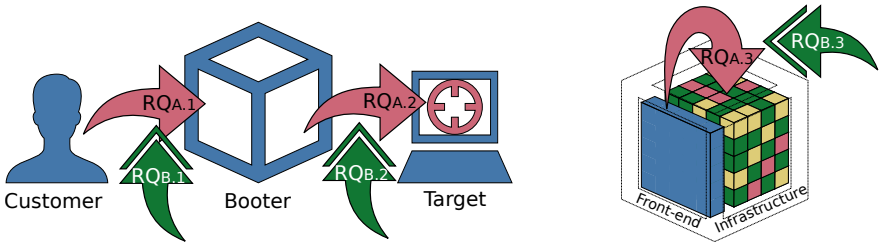
- **RQ$_A$:** How to characterize the DDoS-as-a-Service phenomenon?
- **RQ$_B$:** How to mitigate the DDoS-as-a-Service phenomenon?

By considering Booters as the front-end to access and launch DDoS-as-a-Service, our approach to address both characterization and mitigation research questions is based on investigating each element of the Booters business case (depicted in Fig. 1), and the interaction between them. The Booter business case is composed of the Booter *Customer*, the *Booter* itself, and the *Target* system. Each arrow in the Figs. 1a and 1b represents a step of our approach, which are described in the next sub-sections.

2.1 Characterization Steps

In the context of characterization steps we identify the following research questions.

- RQ$_{A.1}$: How popular Booters are and which services they offer? This research question is the basis to achieve a thorough understanding about the Customer's point of view. In this way, we aim to bring awareness about often



(a) Elements (b) 'Inside the box'

Fig. 1: Booters business case.

Booters have been accessed are and to survey all the key characteristics of Booters. By addressing this research question, we will estimate the size of the threat Booters pose on the Internet.

- RQ$_{A.2}$: What are the characteristics of DDoS attacks launched by Booters? The goal of this research question is to investigate the damage that Booters are able to generate against target systems. Furthermore, we want to compare what is offered to customers (i.e., RQ$_{A.1}$) with what they actually deliver. Finally, and a requisite to achieve the next research question, we want to characterize the infrastructure used to perform attacks.

- RQ$_{A.3}$: How do Booters control infrastructures that perform attacks? In general, Booters are a 'closed box' that advertise themselves by using private infrastructure to perform attacks. However, some works [6] [10] have shown that those infrastructures are composed of several misused hosts and services. Therefore, in this research question we characterize the behavior inside the Booter's box, by investigating the connection between the front-end, in general a Booter's website, and the back-end, composed by the infrastructure that performs attacks, as depicted in the Fig. 1b.

2.2 Mitigation Steps

In the context of mitigation steps we identify the following research questions.

- RQ$_{B.1}$: How to mitigate DDoS-as-a-Service at the customer level? Booters often advertise themselves as stress testers, i.e., tools that stress-test the performance of networks and services, to avoid legal implications. This situation would apply only if the Booter would allow traffic to be sent only to the infrastructure of the customer. However, most Booters recommend to customers not to attack their own infrastructure. Therefore, this research question is the basis to propose solutions to mitigate the '*misbehavior*' of Booters' customer. One way to achieve this is to work in collaboration with exponents of the law to propose countermeasure against Booters and malicious customers.

- RQ$_{B.2}$: How to mitigate DDoS-as-a-Service at the target level? The goal of this research question is to serve as the base to achieve solutions able to cope with different types of DDoS attacks. To do so, we will use the charac-

teristics of DDoS attacks launched by Booters (i.e., $RQ_{A.2}$) to propose specific mitigation solutions against their damaging effects.

- $RQ_{B.3}$: How to mitigate DDoS-as-a-Service at the point where the infrastructure is controlled? Conventional approaches to mitigate DDoS attack aims to find the Command-and-Control (C&C) infrastructure, which is generally hidden behind spoofed IP addresses and several layers of C&C. Nevertheless, once $RQ_{A.3}$ has been addressed, we are able to propose automated solutions to mitigate DDoS attacks at the command and control level.

In summary, the steps presented in this Section, especially in the characterization part, will be achieved based on analysis of large-scale network measurements. To collect this data, we count on global measurements, provided by RIPE Atlas [11], Hurricane Electric [12], and Alexa [13], for example. In addition, we count on collaborations already established, to support our studies and deploy mitigation solutions developed during this research, such as: *SURFnet* [14], CERT.at [15], and the partners of the FLAMINGO Network of Excellence [16]. It should be noted that the steps described in this Section can be addressed out of the presented order.

3 Early Results and Final Considerations

We have developed a crawler that uses Google's Custom Search [17] to find information related to the DDoS-as-a-Service phenomenon, such as blogs, videos, reports, and websites. We have used the following keywords: 'booter', 'ddoser', 'stresser', 'ddos-as-a-service', and 'ddos-for-hire'. Through our crawler and manual classifications, we found 59 Booters since October 2013. Among them, we have identified 34 Booters that are continuously reachable, while the other 25 appeared to be at times offline during the measurement period. The reachable Booters offer the most common DDoS attacks observed nowadays [18], which include: SYN floods, DNS amplification attacks, and attacks based on HTTP GET. In addition, experiments, performed against a dummy target at the University of Twente, seem to indicate that Booters do not always deliver what they advertise. For example, Rebel-security [19] offers 3 Gbps of attack traffic while we measured only 1 Gbps. Even worse, some Booters, such as Olympus Stresser [20] and Vdoss [21], charge money to deliver just a handful of ICMP packets, while was ordered amplification attacks based on UDP.

This research is still in its initial phase and the main goal of this work – as described previously – must be achieved within a period of four years, as the core of a Ph.D. research program.

Acknowledgments

This research is funded by FLAMINGO, a Network of Excellence project (318488) supported by the European Commission under its Seventh Framework Programme.

References

1. Prince, M.: The DDoS That Almost Broke the Internet. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet Accessed on 7 April 2014.
2. Karami, M., McCoy, D.: Understanding the Emerging Threat of DDoS-as-a-Service. In: Proceedings of the 6th UNSENIX Workshop on Large-Scale Exploits and Emergent Threats. LEET'13 (2013)
3. Krebs, B.: The World Has No Room For Cowards. http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards Accessed on 7 April 2014.
4. Prolexic: Multiplayer Video Gaming Attacks. http://www.prolexic.com/knowledge-center-white-paper-series-gaming-reflection-attacks-drdos-ddos Accessed on 7 April 2014.
5. Lackery, J.: A New Twist on Denial of Service: DDoS as a Service. http://blogs.cisco.com/security/a_new_twist_on_denial_of_service_ddos_as_a_service/ Accessed on 7 April 2014.
6. Prolexic: Threat: DDoS Booter Shell Scripts. http://www.prolexic.com/knowledge-center-ddos-threat-advisories-booter-shell-scripts.html Accessed on 7 April 2014.
7. Prolexic: Quarterly Global DDoS Attack Report Q3. http://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q3.html Accessed on 7 April 2014.
8. Goncharov, M.: Russian Underground 101. http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-russian-underground/ Accessed on 7 April 2014.
9. Krebs, B.: Ragebooter: Legit DDoS Service, or Fed Backdoor. http://krebsonsecurity.com/2013/05/ragebooter-legit-ddos-service-or-fed-backdoor/ Accessed on 7 April 2014.
10. Santanna, J.J.: DDoS as a Service. http://www.ietf.org/proceedings/interim/2013/10/14/nmrg/slides/slides-interim-2013-nmrg-1-11.pdf Accessed on 7 April 2014.
11. Atlas, R.: Ripe Atlas website. https://atlas.ripe.net Accessed on 7 April 2014.
12. Hurricane Electric: Hurricane Electric - BGP Toolkit Home. http://bgp.he.net Accessed on 7 April 2014.
13. Alexa: Alexa website. http://www.alexa.com Accessed on 7 April 2014.
14. SURFNet: SURFNet website. http://www.surf.nl Accessed on 7 April 2014.
15. CERT.at: Computer Emergency Response Team Austria website. http://www.cert.at Accessed on 7 April 2014.
16. FLAMINGO: FLAMINGO website. http://www.fp7-flamingo.eu Accessed on 7 April 2014.
17. Google: Google's Custom Search. https://developers.google.com/custom-search/ Accessed on 7 April 2014.
18. Arbor Networks: Worldwide Infrastructure Security Report - Volume IX. http://www.arbornetworks.com/resources/infrastructure-security-report Accessed on 7 April 2014.
19. Rebel-security: Rebel Security's Website. http://rebel-security.com Accessed on 7 April 2014.
20. Olympus Stresser: Olympus Stresser's Website. http://olympusstresser.org Accessed on 7 April 2014.
21. VDoSs: VDoSs' Website. http://vdoss.net Accessed on 7 April 2014.