Quiet Dogs Can Bite: Which Booters Should We Go After, and What Are Our Mitigation Options?

José Jair Santanna, Ricardo de O. Schmidt, Daphne Tuncer, Anna Sperotto, Lisandro Z. Granville, and Aiko Pras

Large network security companies often report websites, called Booters, that offer DDoS attacks as a paid service as the primary reason for the increase in occurrence and power of attacks. Although hundreds of active Booters exist today, only a handful of those that promoted massive attacks faced mitigation and prosecution actions. The authors focus on Booters that are "under the radar" of security initiatives.

ABSTRACT

Large network security companies often report websites, called Booters, that offer DDoS attacks as a paid service as the primary reason for the increase in occurrence and power of attacks. Although hundreds of active Booters exist today, only a handful of those that promoted massive attacks faced mitigation and prosecution actions. In this tutorial article we focus our attention on Booters that are "under the radar" of security initiatives, by advertising high attack power and being very popular on the Internet. We discuss and provide grounds for critical thinking on what should be further done toward Booter mitigation.

INTRODUCTION

Booters can easily be found on the public web through search engines (e.g., Google). Distributed denial of service (DDoS) attacks performed by Booters can be hired for a couple of U.S. dollars. Booters also present multiple ways of paying for their "service" (e.g., Paypal, Bitcoin, and credit card), while offering various types of attacks (e.g., SYN flood, DNS-based reflection, and application layer attacks). Karami *et al*. [1] showed that the large number of active Booters and the ease with which these can be found and their service hired contribute to the increasing occurrence of DDoS attacks. This observation proved to be correct given that the majority of attacks, including the most powerful DDoSs, have been launched by Booters (at a data rate higher than 100 Gb/s), as reported by Akamai (https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf, accessed 21 March 2017).

Although hundreds of active Booters exist, few of those involved in massive attacks underwent mitigation actions. Booters that to date have been the target of investigations, mitigations, or prosecutions are the ones that successfully disrupted the operation of popular services, such as Xbox Network, PlayStation Network, Instagram, and Tinder (http://krebsonsecurity.com/?s=booter, accessed 21 March 2017). In 2016, the vDos Booter [2] was reported to have launched more than 170,000 DDoS attacks in less than four months; as a consequence, vDos owners were arrested. In 2016, a sustained 540 Gb/s attack, launched by the LizardStresser Booter (https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks, accessed 21 March 2017), was also witnessed during the Olympic Games in Brazil, as well as a staggering terabit-per-second attack using the Mirai botnet (also related to Booters — https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar, accessed 21 March 2017) targeting OVH (https://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/, accessed 21 March 2017) and Dyn (http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack, accessed 21 March 2017). These are only a few examples of Booter attacks, which were eventually reported in the news and caught the public's attention. However, in only some cases did the people responsible for the Booters behind these attacks face legal consequences. The goal of this tutorial article is to raise awareness about Booters that stay "under the radar" of security initiatives by advertising high attack power and being extremely popular.

The research on Booter mitigation is still at an early stage. Most of the existing work has been focused on looking at the technical characteristics of the attacks performed by Booters [3–5] and profiling their targets [6]. Other initiatives [3, 7] have used leaked Booter databases to, for example, enumerate the characteristics of hired attacks. Other research efforts have been exploring issues associated with identifying Booter websites [8], discovering and mitigating the infrastructures used by Booters to perform attacks [9, 10], and describing Booters' financial operations [1]. In this tutorial article, we extend the contribution from those previous efforts by providing extra ground for discussions and critical thinking on what one can further do and how to mitigate Booters.

In the first part of this article, we focus on answering the question *which Booters should we go after?* Using a combination of measurement datasets that we collected ourselves and also

Digital Object Identifier: 10.1109/MCOM.2017.1600992

José Jair Santanna, Ricardo de O. Schmidt, Anna Sperotto, and Aiko Pras are with the University of Twente; Daphne Tuncer is with University College London; Lisandro Z. Granville is with Federal University of Rio Grande do Sul.

0163-6804/17/$25.00 © 2017 IEEE

retrieved from public sources, we highlight which of those "under the radar" Booters are very popular and advertise high attack power for low prices, but have not yet undergone any meaningful mitigation action. Our ground-truth is a list of 435 Booter domain names from the Booter Blacklist initiative (http://booterblacklist.com, accessed 21 March 2017) [8]. Our dataset and associated scripts for data analysis are publicly available at http://jairsantanna.com/booter_ecosystem_analysis (accessed 21 March 2017). In the second part of this article, we provide a thorough discussion of mitigation options to address the problem of Booters. Our methodology is based on identifying organizations (in)directly involved with Booters that could take part in mitigation actions to inhibit or even dismantle Booter operations. We finally conclude the article by discussing the lessons learned.

Which Booters Should We Go After?

Mitigation and prosecution actions performed against the Booter ecosystem (i.e., websites, owners, clients, and infrastructure) have mostly targeted those Booters that launched powerful attacks toward large organizations. However, there are still hundreds of Booters, such as those revealed by the Booter Blacklist initiative, that are somehow "under the radar" of security initiatives and therefore rarely the target of mitigation actions. Obviously, not all Booters could be mitigated at once, but a priority order would be welcome. The first Booters to be mitigated should preferably be the ones that perform the most powerful attacks. Identifying these Booters is a task mostly restricted to large network security companies that have the ability to classify the most dangerous attacks of those targeting their clients. In this section, we describe a heuristic to prioritize the mitigation of a (second) set of Booters. Our heuristic relies on the following three premises.

Booters' Services Are Not Likely to Be Ethical or Legal: It is debatable whether an illegal Booter can be a legitimate stress tester. However, as presented by Douglas *et al.* in [11], the attack infrastructure used by Booters mostly consists of compromised/misused machines (e.g., botnets and amplifier services). Others have attested to this argument by hiring attacks from Booters and testing them against controlled environments [3–5].

The Ratio between the Number of Accesses to Their Websites and the Number of Launched Attacks Is Similar between All Booters: This premise leads us to conclude that the most accessed Booters are those likely to launch more attacks.

The Attack Power Advertised by Booters Can Be Factual: It has been observed that Booters, in general, deliver far less attack power than they promise to their clients [5]. However, Booters that caught the attention of the media performed attacks stronger than they actually advertised on their respective websites. For example, `lizardstresser.su` attacked the PlayStation and Xbox networks during Christmas 2013 with 300 Gb/s attack power, while on their website (as of 2013) attacks up to 125 Gb/s were advertised. To further support our premise, we argue that it is quite easy to find amplifiers for reflection attacks and/or to compromise a large number of systems (e.g., Internet of Things devices). Therefore, skilled hackers and owners of Booters can easily scale up their attack power [12].

Based on our premises, our heuristic to highlight Booters consists of four steps. First, we identify the most accessed Booters using the website ranking provided by Alexa (http://alexa.com, accessed 21 March 2017). For each of the 435 Booter domain names in http://booterblacklist.com, we scrape the Alexa rankings from 1 November 2016 to 1 February 2017. Our analysis only considers those Booter domain names that ranked up to 3 millionth in Alexa, which represents around 1 percent of the total number of registered domain names in the entire Internet (http://verisign.com/innovation/dnib, accessed 21 March 2017). We then scrape these top-ranked Booter domain names to reveal their highest advertised attack rate (i.e., the most powerful attack) and their price range. Finally, we investigate the dates of creation and expiration of their domain names based on Whois information. This last step shows how long the top-ranked Booters are offering (and likely delivering) attacks without facing any type of mitigation action.

Figure 1 summarizes our findings. From the ground-truth list of 435 Booter domain names, 33 ranked among the top-1 percent of all most accessed domain names on the Internet (Fig. 1a). In addition to their position in Alexa's ranking, we observed that 8 Booters offer attacks with a rate of 100 Gb/s or higher (Fig. 1c); these are Booters ranked in the following positions: 4, 7, 8, 13, 14, 18, 25, and 32. Attacks of 100 Gb/s or more are powerful enough to bring most systems offline on the Internet, especially those that are not protected by large security companies. Figure 1b shows that some of these 8 Booters (i.e., Booters ranked at 4, 14, 18, and 32) charge at maximum US$100, while their cheapest service plan is US$10 or less. Such a range of prices is surprising when considering that the cost of recovering from a DDoS attack is on average US$53,000 for small and medium companies, and US$417,000 for large companies (https://press.kaspersky.com/files/2015/09/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf, accessed 21 March 2017). Based on our premises and findings, it can therefore be deduced that these last four Booters (ranked at 4, 14, 18, and 32) are the ones that, at the lowest cost to their clients, can do the most damage to the target of an attack. Furthermore, we observed that four other Booters offer attacks for free (Booters ranked 1, 5, 9, and 10). However, upon closer examination of these Booters, we discovered that, except for the Booter ranked 9th, they all promote services from other (paid) Booters. We believe that these "free-service" Booters are used to increase the popularity of actual paid Booters.

From those Booters listed in Fig. 1, three domain names are currently for sale, ranked 19, 29, and 31. These domains pointed to actual Booter websites that were active in the past, as confirmed by the Internet Archive initiative (https://archive.org, accessed 21 March 2017; The Internet Archive has dozens of historical snap-

Mitigation and prosecution actions performed against the Booter ecosystem have mostly targeted those Booters that launched powerful attacks towards large organizations. However, there still exist hundreds of Booters, such as those revealed by the Booter Blacklist initiative, that are somehow "under the radar."

Infected machines can be part of a botnet able to perform various types of attacks. Misused public services are in turn only used for reflection and amplification attacks. The last element in the Booter ecosystem is the Booter operational database, where all information about clients and hired attacks is stored.

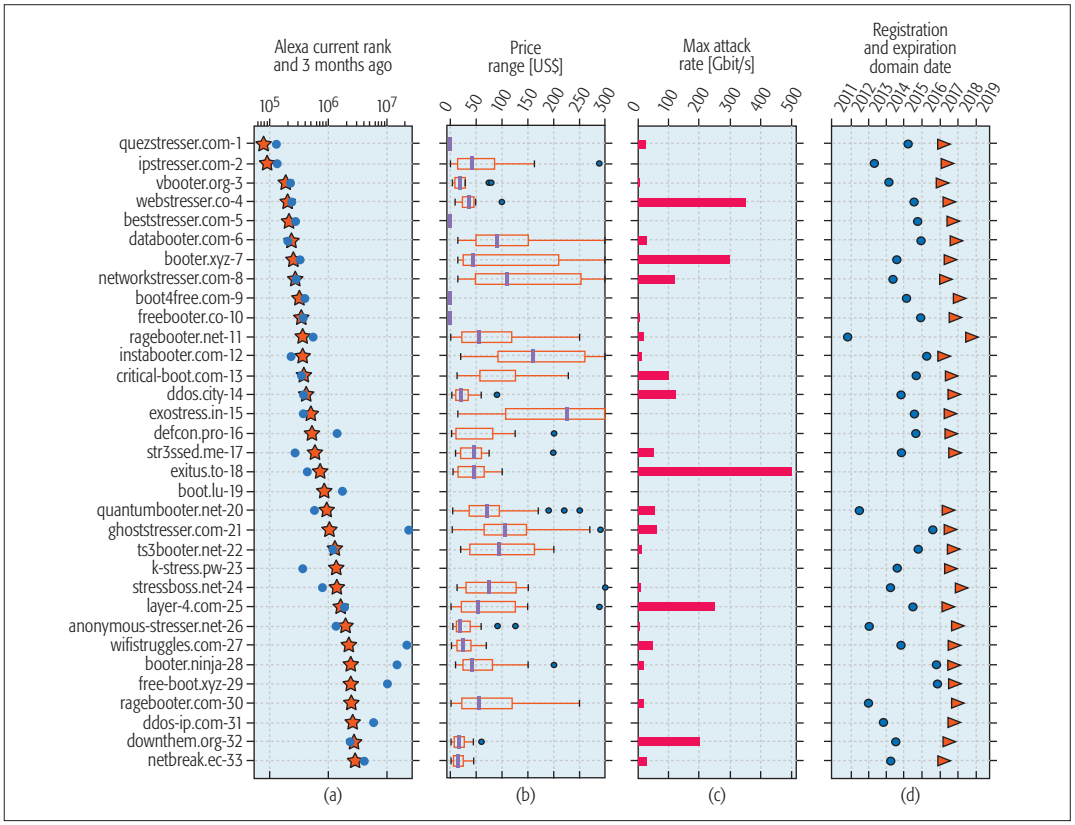

Figure 1. a) Top ranked Booter domain names, up to the 3 millionth position in Alexa ("star" is the current rank, while "dot" is the rank 3 months ago); b) price range (minimum, gigabits per second); d) registration and expiration dates of domain names.

shots of these specific domain names.). These are still highly ranked domains in Alexa because users still try to reach them. This assumption is supported by the DNSDB initiative (https://www.dnsdb.info, accessed 21 March 2017), one of the largest collections of DNS records worldwide. We found in DNSDB records that each of these three domains have received thousands of DNS requests (likely interpreted as web access) in the last two years.

Finally, we observed that two Booter domain names (ranked 11 and 30) point to the same Booter website. This Booter has, among all the top ranked ones, the oldest domain creation date: it was registered in 2011. Although it was reported in 2013 by a security specialist (https://krebsonsecurity.com/2013/05/ragebooter-legit-ddos-service-or-fed-backdoor, accessed 21 March 2017), we are unaware of any mitigation or prosecution action against it. A possible explanation is that this Booter is actually an "FBI backdoor," as described by its owner. A speech by the CEO of CloudFlare mentioned that "sometimes we have court orders to not take (web)sites down" (https://www.youtube.com/watch?v=Wr-PrSqI16A&t=2929s, accessed 21 March 2017). Whether true or not, the concrete fact is that this Booter is still online. We further discuss CloudFlare and other DDoS protection services in the following section.

Our heuristic clearly provides means to highlight Booters "under the radar" of security companies that should be the first to undergo mitigation actions. In the next section, we discuss how third-party organizations can enroll on mitigation actions against Booters.

Who Can Help Perform Mitigation Actions?

Figure 2 shows the ecosystem of Booters, that is, all elements involved in Booter activities. To identify organizations that can engage in mitigation actions against Booters, we first look at those that are (in)directly involved in the Booter ecosystem. To hire an attack, a client must first access the Booter website and create an account. The access to a Booter website usually happens via a third-party cloud-based security provider (CBSP) transparent to the client. The payment for a hired attack (or an attack plan — sets of attacks that can be performed within a given period of time) is done via a third-party payment system. After selecting a "service" and paying for the plan, clients can launch attacks at any time and against any target on the Internet.

To perform DDoS attacks, Booters use a back-end infrastructure that consists of three types of machines: command and control (C&C) machines, infected machines (computers with bugs in Fig. 2), and misused public services (computers with exclamation marks in Fig. 2). Booters are unlikely to send attack traffic directly from their C&C machines. Instead, infected machines can be part of a botnet able to perform various types of attacks. Misused public services are in turn only used for reflection and amplification attacks (e.g., DNS-based and NTP-based attacks). The last element in the Booter ecosystem is the Booter operational database, where all information about clients and hired attacks is stored.

In addition to CBSPs and a payment system, five other organizations are also (in)directly involved in the Booter ecosystem:

- Web hosting companies that host the content of Booter websites
- Top-level domain (TLD) operators
- Domain registrars that provide means for the registration of Booter domain names
- Web indexing and search companies that facilitate finding Booter websites
- Local DNS resolvers that resolve Booter domain names to IP addresses

We next show to what extent these third-parties are involved with Booters and discuss potential actions they could perform to support the mitigation of the Booter phenomenon. The starting point of the analysis presented in this section is the same list of 435 Booter domain names described and analyzed in the previous section.

TLDs Operators, Domain Registrars, Web Hosting Companies, and CBSPs

These four types of organizations are analyzed together for the following two reasons. First, they are linked to Booters mainly via domain names. Second, the same company may provide different types of services. Examples of such organizations include SIDN (https://sidn.nl, accessed 21 March 2017), which is both a TLD operator (of .nl) and a domain registrar; GoDaddy (http://godaddy.com, accessed 21 March 2017), which is both a domain registrar and a web hosting company; and CloudFlare (https://cloudflare.com, accessed 21 March 2017), which is both a web hosting company and a CBSP.

We use distinct methodologies to analyze each of these four types of organization: for TLDs, we look into the composition of Booter domain names; for domain registrar, we rely on Whois information; and for web hosting and CBSPs, we use their IP address and autonomous system (AS) information (http://www.team-cymru.org/IP-ASN-mapping.html, accessed 21 March 2017).

As shown in Fig. 3, by looking at the composition of domain names, we observe that more than 68 percent of all 435 Booters are registered within the .com and .net TLDs. Other TLDs account for less than 5 percent of registrations each. For example, .nl accounts for around 1 percent of registrations. We also see that 74 percent of Booter domain names contain the terms "stresser," "booter," or "ddos." Information on the composition of domain names could be used by TLD operators and registrars to, for example, take down existing domains or prevent the registration of new (suspect) ones. An enabler to check Booter domain names was proposed in [8]. Preventing the registration of new domains could, however, impact the registration of valid domain names that could eventually be classified as suspect.

We analyzed the impact of domain names that have the terms "stresser," "booter," or "ddos" in their composition, and are registered within .com, using a large-scale active DNS measurement dataset [13]. We found out that from all 2721 domains names in .com containing one of the three terms, only 61 domain names (less than 3 percent) are *not* related to Booters.

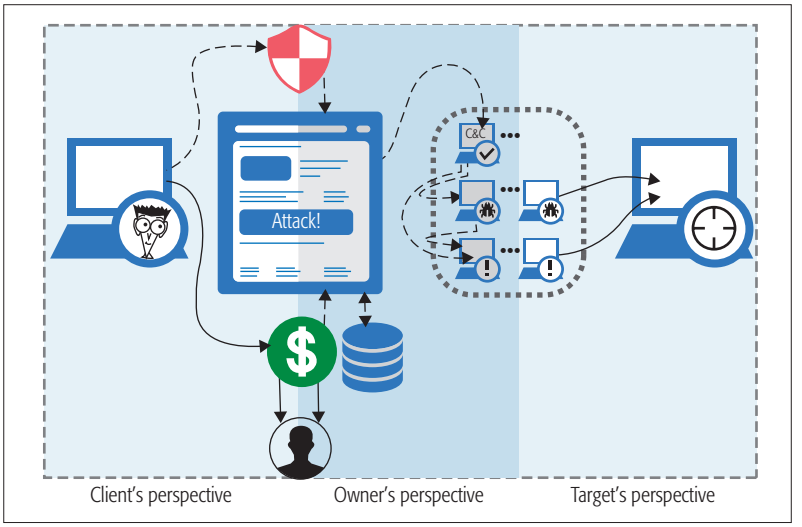

Figure 2. Booter ecosystem.

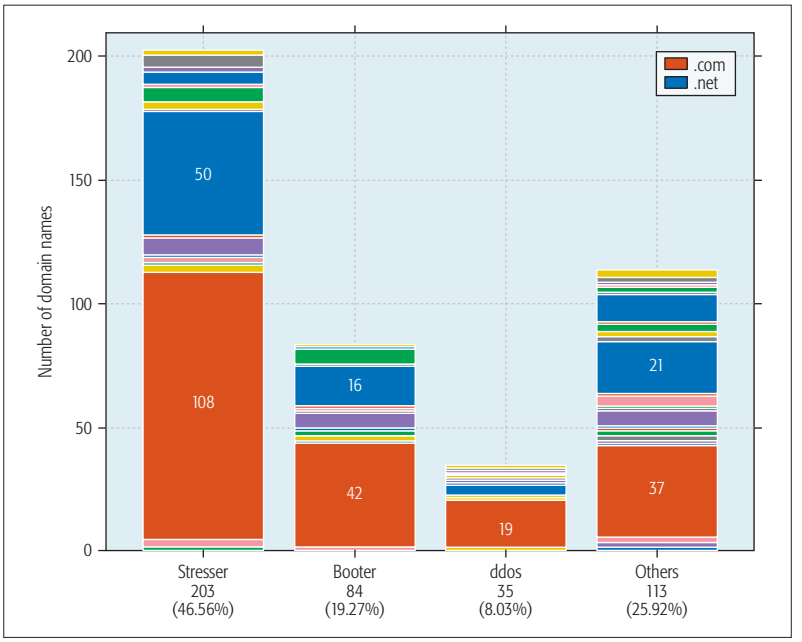

Figure 3. Domain word composition and TLDs distribution (.com and .net highlighted).

That is, by filtering registrations based on these three terms, a very small percentage of legitimate registrations would be affected. However, Booter owners could overcome these actions by adopting alternative terminologies. By analyzing Booters' Whois information, we observe that almost 70 percent of all Booters are within the top 10 registrars, as can be seen in Fig. 4, if Enom, GoDaddy, and Namecheap decided to act against Booters, around 50 percent of all Booters would be affected.

When looking at the IP addresses and ASs related to 202 (online) Booter domain names, we also noticed that some companies would have a higher impact if they got involved in mitigation actions. For example, CloudFlare is involved with at least 76 Booters (37 percent). The fraction of Booters behind CloudFlare dropped significantly compared to a previous study [5]: 88 percent — 52 out of 59 Booters (in that study, 49 Booters

It is extremely easy to find Booter websites through public web search engines, such as Google, Bing, and Yahoo. To prevent users from interacting with Booters, search engines could notify them that hiring or even accessing Booter "services" would potentially have legal implications.

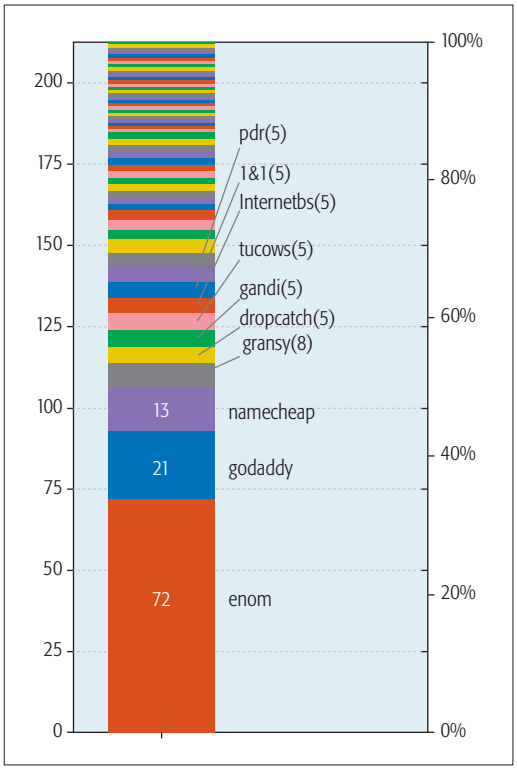

Figure 4. Registrars analysis based on Whois information.

are part of the 37 percent seen in the current analysis). Given that Booters typically attack each other [7], competing for market shares or even to simply show off their attack power, we believe that if CloudFlare (and other CBSPs) stopped protecting Booters, these would eventually take each other offline — or at least have their reachability compromised. However, this action would only have an impact if all CBSPs decide to get involved, leaving no options to Booters but being out of a DDoS protection service.

Booters behind CBSPs require a more refined investigation in order to determine the web hosting company where their websites are actually hosted (ASs). To determine the web hosting companies specifically obscured by CloudFlare, we used the CloudPiercer initiative (http://cloudpiercer.org, accessed 21 March 2017) [14], which applies several metrics to look up actual (or historical) IP addresses. Using this methodology, we found out that 24 web hosting companies host 47 Booters (out of 76 in CloudFlare), as depicted in the middle (zoom-in) graph of Fig. 5. The other 29 Booters are also likely to be protected and hosted by CloudFlare. Merging web hosting companies in Fig. 5 (ASs) with the discovered hidden ASs, we observe that the top 10 web hosting companies do not change (their ranks do, however). For example, comparing the left and right graphs in Fig. 5, it can be observed that OVH and GoDaddy gain 6 and 2 positions, respectively. The main takeaway message from this analysis is that if the top web hosting companies enroll in effective mitigation actions (e.g., simply stop hosting alleged Booters), a high percentage of Booters would go offline. However, Booters could, again, adapt to such an action by moving to other hosting companies.

Payment Systems

Payment systems are one of the main elements of the Booter ecosystem. In 2015, Karami *et al.* [1] reported a joint effort made with PayPal by which Paypal accounts allegedly belonging to Booter owners were deactivated. This operation was very successful, momentarily reducing the number of payments and attacks by Booters. However, Booters have partially overcome this mitigation action. For example, only one Booter among those listed in Fig. 1 still offer PayPal as a payment option. Other Booters now use various crypto-currencies, such as Bitcoin, Litecoin, and Dogecoin. This change in the payment system makes it harder to trace Booter owners by following the money they earn. The action by PayPal had a positive impact on the Booter ecosystem, given that only a small number of Booter clients have Bitcoin wallets. In addition, based on the profile of a typical Booter client, we believe that not many of them would be willing to create a Bitcoin wallet to simply perform attacks.

Web Searching Companies

It is extremely easy to find Booter websites through public web search engines, such as Google, Bing, and Yahoo. To prevent users from interacting with Booters, search engines could notify them that hiring or even accessing Booter "services" would potentially have legal implications. This action is similar to one currently done for "unsafe sites" in Google Chrome (https://support.google.com/chrome/answer/99020/, accessed 21 March 2017), and could reduce the number of accesses to Booters and, ultimately, the number of attacks launched by Booters.

DNS Resolver Operators

A straightforward way to prevent users from accessing Booters is by blacklisting Booter domain names at DNS resolvers. In this way, when an IP address resolution is needed for a blacklisted domain name, the resolution is refused. Booter websites would still be reachable via alternative DNS resolvers that do not block the resolution, or via VPNs or the Tor browser. However, considering that Booters under CBSPs can block access from VPNs and Tor nodes, this action by DNS resolver operators could ultimately result in a significant reduction of the number of attacks from Booters.

It is very important to highlight that the mitigation actions described in this section might require a court order before they are put in place. For example, CloudFlare's CEO stated that "it is tricky when private organizations act as law enforcement" and that "they comply with any court order" (https://www.youtube.com/watch?v=Wr-PrSqI16A, accessed 21 March 2017). Although the legitimacy of services offered by Booters is still debatable, Douglas *et al.* [11] state that it is unlikely that Booters provide legal and ethical services, because their back-end infrastructures are composed of compromised machines or misused systems (e.g., botnets, DNS resolvers, NTP servers, and Webshells). Determining the back-end infrastructure (or parts of it) of a Booter can be done by hiring an attack against a controlled environment, as was done in previous works [3–5].

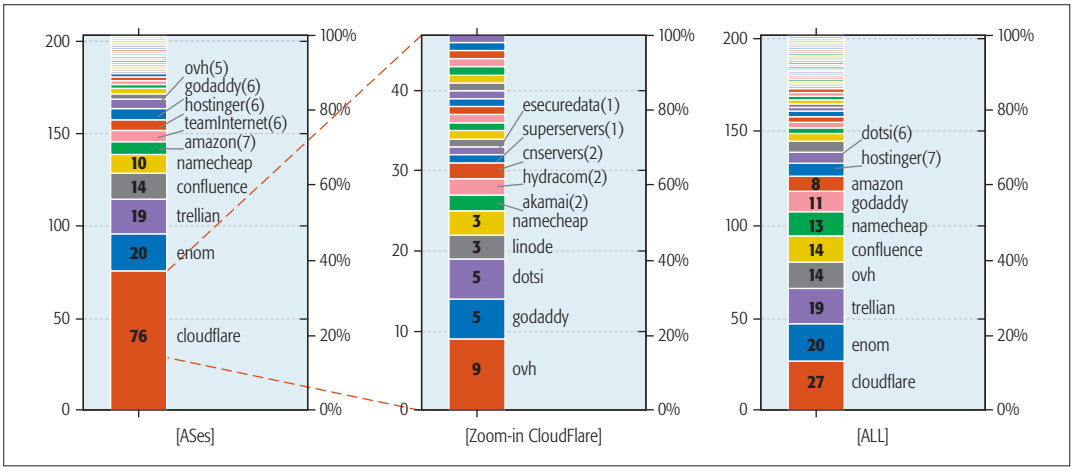

Figure 5. Web hosting analysis based on ASs (left), with zoom-in on the ASs hidden by CloudFlare (middle), and the overall merged results (right).

Lessons Learned

In this article, we have two goals. Our first objective is to identify Booters "under the radar" of security actions that should face mitigation in a higher priority order. Our second objective is to determine organizations that (in) directly interact with Booters and could act to mitigate Booters.

To achieve the first goal, we propose a heuristic based on website popularity, maximum attack rate, price range, and domain creation and expiration. Using this heuristic and a set of premises, we identified 33 Booter domain names that should face mitigation with higher priority, and provided arguments to justify the need for such mitigation actions. We showed that Booters "under the radar" pose a potential risk and, as such, we consider proactive mitigation to be the best course of action.

Concerning the second goal, we learned that dismantling the entire Booter ecosystem is very challenging. None of the mitigation actions mentioned above could eliminate, on a standalone basis, the Booter phenomenon. However, if some of them were actually deployed, we would certainly see a decrease in Booter operations, similar to what happened after PayPal's operation against Booters in 2015. This decrease would be mostly caused by lay users (i.e., Booter clients) that would not be able to overcome challenges imposed by the mitigation actions. While technically skilled users would still find a way to use Booter services, they remain a minority.

Booter owners are likely to find ways to overcome any mitigation action. Booters can profit from relatively safe business when not calling too much attention from society and security specialists. To date, legal actions against both Booter owners and clients have been taken only in cases where large corporations were targeted by DDoS attacks. In this article, we raise awareness about the hundreds of silent Booters, safely operating "under the radar" of security actions, that could at any point in time cause substantial damage to any system in the Internet. We hope that our findings will foster further discussions and effective actions against Booters.

In this article, we raised awareness about the hundreds of silent Booters, safely operating "under the radar" of security actions, that could at any point in time cause substantial damage to any system in the Internet. We hope that our findings will foster further discussions and effective actions against Booters.

Acknowledgments

This work is funded by the FLAMINGO (EU FP7 ICT- 318488) and D3 (NWO 628001018) projects. Ricardo de O. Schmidt's research is also funded by the SAND (http://www.sand-project.nl) and NWO DAS (http://www.das-project.nl) projects. Special thanks go to the teams of Farsight Security, Cloudpiercer, and Mattijs Jonker for assisting us in the experiments and providing valuable information.

References

[1] M. Karami, P. Youngsam, and D. McCoy, "Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services," *Proc. Int'l. Conf. World Wide Web*, 2016.

[2] B. Krebs, "Alleged vDOS Proprietors Arrested in Israel," http://krebsonsecurity:com/2016/09/alleged-vdos-proprietors-arrested-in-israel/#more-36288, 2016, accessed 21 Mar. 2017.

[3] M. Karami and D. McCoy, "Understanding the Emerging Threat of DDoS-as-a-Service," *Proc. USENIX Wksp. Large-Scale Exploits and Emergent Threats*, 2013.

[4] V. Bukac *et al.*, "Service in Denial — Clouds Going with the Winds," *Network and System Security*, 2015.

[5] J. J. Santanna *et al.*, "Booters-An Analysis of DDoS-as-a-Service Attacks," *Proc. IFIP/IEEE Symp. Integrated Network and Service Management*, 2015.

[6] A. Noroozian *et al.*, "No Who Gets the Boot? Analysing Victimization by DDoS-as-a-Service," *Proc. Int'l. Symp. Research in Attacks, Intrusions, and Defenses*, 2016.

[7] J. J. Santanna *et al.*, "Inside Booters: An Analysis on Operational Databases," *Proc. IFIP/IEEE Int'l. Symp. Integrated Network Management*, 2015.

[8] J. J. Santanna *et al.*, "Booter Blacklist: Unveiling DDoS-for-Hire Websites," *Proc. Intl. Conf. Network and Service Management*, 2016.

[9] L. Krämer *et al.*, "AmpPot: Monitoring and Defending Against Amplification DDoS Attacks," *Research in Attacks, Intrusions, and Defenses*, 2015.

[10] J. Krupp, M. Backes, and C. Rossow, "Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks," *Comp, and Commun. Security*, ser. CCS '16. ACM, 2016.

[11] D. Douglas *et al.*, "Booters: Can Anything Justify Distributed Denial-of-Service (DDoS) Attacks for Hire?" *J. Info., Commun. and Ethics in Society*, vol. 15, no. 1, 2017.

[12] A. Pras *et al.*, "DDoS 3.0 — How Terrorists Bring Down the Internet," *Proc. Int'l. GI/ITG Conf.*, MMB and DFT, 2016.

[13] R. van Rijswijk-Deij *et al.*, "A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements," *IEEE JSAC*, vol. 34, no. 7, 2016.

[14] T. Vissers *et al.*, "Maneuvering Around Clouds: Bypassing Cloud-Based Security Prwoviders," *Proc. Conf. Comp. and Commun. Security*, 2015.

Biography

José Jair Santanna is a Ph.D. candidate in the Design and Analysis of Communication Systems Group at the University of Twente, the Netherlands. His research interests are in the areas of Internet security, management and measurements, and (big) data analysis.

Ricardo de Oliveira Schmidt is a postdoctoral researcher within the chair of Design and Analysis of Communication Systems, University of Twente, and a research engineer at SIDN Labs, the Netherlands. He obtained his Ph.D. from the University of Twente in 2014. His research interests are in Internet security, management, and measurements.

Daphne Tuncer is a research associate in the Communications and Information Systems Group, Department of Electronic and Electrical Engineering, University College London (UCL), United Kingdom. She obtained her Ph.D. in electronic and electrical engineering from UCL in November 2013. Her research interests are in the areas of software-defined networks (in particular applied to network resource management), cache/content management, and adaptive network resource management.

Anna Sperotto is an assistant professor at the Design and Analysis of Communication Systems Group of the University of Twente. She received a Ph.D. degree from the University of Twente in 2010, with the thesis *Flow-Based Intrusion Detection*. Her research interests include network security, network measurements, and traffic monitoring and modeling.

Lisandro Zambenedetti Granville is an associate professor at the Federal University of Rio Grande do Sul. He served as TPC Co-Chair of IFIP/IEEE DSOM 2007 and IFIP/IEEE NOMS 2010, and as General Co-Chair of IFIP/IEEE CNSM 2014. He is Chair of IEEE ComSoc's Committee on Network Operations and Management, Co-Chair of the IRTF's Network Management Research Group, and President of the Brazilian Computer Society. His interests include network management, software-defined networking, and network functions virtualization.

Aiko Pras is a professor Internet security at the University of Twente, where he is a member of the Design and Analysis of Communication Systems (DACS) group. His research interests include Internet security, measurements, and management. He is chairing the IFIP Technical Committee on Communications Systems (IFIP-TC6), and has been Chair of the EU Future Internet cluster and coordinator of the European Network of Excellence on Management of the Future Internet. He serves on many steering committees and editorial boards.