Understanding the Emerging Threat of DDoS-As-a-Service

Mohammad Karami Damon McCoy
George Mason University

1 Introduction

A denial-of-service (DoS) attack refers to an explicit attempt by a malicious party to deny legitimate users of a service from accessing the service [5, 7]. A distributed denial-of-service (DDoS) attack has the exact same goal but multiple distributed resources are utilized for a more devastating effect [5, 7].

While access to a large number of compromised hosts was traditionally required for launching successful DDoS attacks [4, 8], the emergence of DDoS-As-a-Service [3] in recent years have made DDoS infrastructure capable of generating over 800 MBit/s of traffic accessible to a wide range of malicious actors for a cost as low as $10/month.

In this paper, we investigate the phenomenon of low-cost DDoS-As-a-Service also known as *Booter* services. While we are aware of the existence of the underground economy of Booters, we do not have much insight into their internal operations, including the users of such services, the usage patterns, the attack infrastructure, and the victims [6]. In this paper, we present a brief analysis on the operations of a Booter known as *TwBooter* based on a publicly-leaked dump of their operational database. This data includes the attack infrastructure used for mounting attacks, details on service subscribers, and the targets of attacks. Our analysis reveals that this service earned over $7,500 a month and was used to launch over 48,000 DDoS attacks against 11,000 distinct victims including government websites and news sites in less than two months of operation.

2 Background

The dynamics of the modern Internet have significantly lowered the technical barriers for malicious actors to build DDoS infrastructure and lease it for a small monthly fee, typically ranging from $10-$200, depending on the maximum duration of attack and number of concurrent attacks desired. There are two main components of these Booter services: the attack infrastructure and the code to manage the service and launch attacks. Some Booter services use compromised servers to launch their DDoS attacks along with lists of open proxies to mask their IP addresses. Others simply rent servers to launch their attacks. Most of the services are based on the asylum booter source code, which has leaked onto many file download sites. [1]

Duration	Clients	Victims	Attacks
Jan. 2013 - Mar. 2013	312	11,174	48,844

Table 1: Summary of *twBooter* dataset used in the analysis.

These Booters publicly market themselves as "stress testers", however, in underground forums they advertise themselves as DDoS services. Originally, Booters were used by online gamers to initiate DDoS attacks against their online opponents to gain an in game advantage. However, as we will show Booters are also utilized to mount attacks on medium-sized websites.

The dataset used in this study is associated with a DDoS service provider known as *TwBooter (http://booter.tw)*. This Booter was identified as being responsible for a series of DDoS attacks targeting a popular blog on computer security and cybercrime [2] and the Ars Technica web site [1].

3 Dataset

The dataset used for our analysis is a publicly-available SQL dump file of the operational database of the *TwBooter* service. The dataset covers a period of 52 days ending on March 15, 2013 and contains more than 48,000 attack records. Table 1 provides a summary of the data contained in this dataset.

While the database includes a total of 18 tables, most of our analysis was performed using only three tables: *users* recording information about each subscribed user, *servers* containing information on the servers used for mounting the attacks and *attacks* recording the details of each attempted attack, including the owner, targeted victim, attack type, attack duration, and the server(s) used for launching the attack.

We also received a copy of the operational database dump of another Booter known as *asylumbooter*[2], which covers a period of more than 16 months ending on March 22, 2013 and includes almost half a million attack instances perpetrated by 5,622 subscribers. However, because its records do not contain fine-grained data, such as the IP address of victims and duration of attacks, we do not include it in our analysis.

[1] A copy of the asylum booter source code is available at http://softwaretopic.informer.com/asylum-booter-source/

[2] www.asylumstresser.com

4 Analysis

In this section we will present analysis based on various aspects of *TwBooter's* operations, including the infrastructure leveraged for mounting DDoS attacks, details on service subscribers, and the targets being victimized by the Booter.

4.1 Attack Infrastructure

While it is not uncommon to perform DDoS attacks based on an infrastructure comprised of many compromised clients managed from a central command and control center, *TwBooter* relies on a number of servers to perform DDoS attacks. Compared to clients, servers utilized for this purpose could be much more effective as they typically have much higher computational and bandwidth capacities, making them more capable of starving bandwidth or other resources of a targeted system.

For each attack instance, the dataset contains the list of server(s) and the type of DoS technique used for performing the attack. Based on this data, the two subsequent subsections discuss the details of the infrastructure exploited by *TwBooter* to serve its customer base.

4.1.1 Servers

All the attack instances recorded in the dataset were performed by 15 distinct servers. Only three servers have been active for the whole operation period (January 23rd to March 15th). The other servers either left or joined the pool of servers in the middle of the period. A total of 9 servers were in active operation as of March 15th. The lifetime for the 6 inactive servers ranged from 3 days to 16 days with an average of 11 days. The average lifetime for servers that were still in active operation was 37 days. Two of the servers were hosted in US and rest were hosted by an ISP located in the Netherlands. [3]

Attackers often attempt to hide the identity of offending machines by spoofing the source address field of attack packets or using intermediate proxies for delivering attack packets to targeted victims. As we will show later in the paper, *TwBooter* utilizes both of these techniques.

4.1.2 Attack Types

TwBooter employs a broad range of different techniques for performing DDoS attacks. This includes generic attack types such as SYN flood, UDP flood and amplification attacks, HTTP-based attacks including HTTP POST/GET/HEAD and RUDY (R-U-Dead-Yet) and application specific attacks such as slowloris that targets Apache webservers with a specific misconfiguration. While a total of 12 different attack types exist in the dataset, the above-mentioned attack types account for more than 96% of all performed attacks.

[3]We do not have enough evidence to tell if the servers have been taken over through vulnerability exploitation or have been directly leased from the hosting provider.

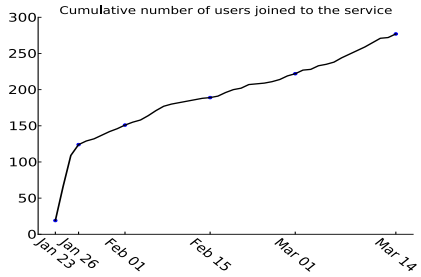

Figure 1: The joining rate of users

4.2 Customers

A total of 312 users were registered with the *TwBooter* within the time period of the dataset. Out of this number, 35 users had no attack records, and therefore were excluded from our analysis. Figure 1 shows the joining rate of users to the service. Here, the date of the first attack record is considered as the join date of each user. Almost half of the users have joined the service during its first week of operation. Booter services typically advertise themselves in underground forums for a while before launching their services and offer special incentives for early users. This could be potentially a reason why there is a spike of users at the beginning of the period. After the first 4 days that has an average joining rate of 31 users per day, the average growth rate of the service is limited to 3.25 users per day. Based on anecdotal data, Booter services usually can not scale up with their user base over time in terms of attack infrastructure and ultimately abandon their business at some point.

Online gamers constitute the primary group of customers served by *TwBooter*. However, as we will see there are smaller groups of customers using the service for purposes other than targeting online gamers.

At the registration time, the users subscribe to a one month license for launching DDoS attacks. Depending on the amount paid, the subscribers can initiate attacks that can last for a limited maximum amount of time. There are several attack duration options available ranging from one minute to two hours. The users can also pay an additional fee to be able to initiate up to three concurrent attacks. There is no limit on the number of sequential attacks that a user can initiate during a month of subscription.

4.2.1 Subscription Type Selection

As pointed to in section 4.1, *TwBooter* utilizes high bandwidth servers to mount DDoS attacks. Gamers typically use residential Internet connections to play online games. Considering the limited capacity of gamers' links, they can be easily overwhelmed with large amounts of traf-

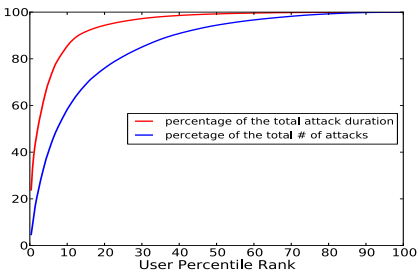

Figure 2: Distribution of users share from perpetrated attacks

fic originated from one or more servers for a short period of time. For this reason, the majority of *TwBooter* users comprised of gamers have subscribed for short-lived DDoS attacks. About 65% of users have chosen attack durations of 10 minutes or less and 32% have selected attack durations of more 10 minutes, up to two hours.

By intuition, the users subscribed for an attack duration of 10 minutes or less are likely gamers and those subscribed for an attack duration of an hour or more (15% of users) are likely users targeting websites. Interestingly, there are a few users who have the privilege to initiate attacks lasting for more than two hours. [4]

In terms of attack concurrency, 74% of users subscribed for only one attack at a time. Again by intuition, most of the users in this group should be gamers since they do not require multiple simultaneous attack sessions to satisfy their goals. Only 9% of the users have chosen the option of initiating two concurrent attacks and 15% of users with the need for higher capacities have subscribed for three concurrent attacks. Again, there are a few privileged users that are allowed to initiate more than three concurrent attacks. The subscription information and information on the cost of each combination of options allows us to estimate that *TwBooter* earned $7,727 a month.

4.2.2 Service Usage Characterization

Figure 2 shows how a small percentage of users are responsible for most of the attacks both in terms of number and duration. The top 2% of users (6 users) in terms of attack duration are responsible for about half of the whole attack time in 52 days (28,154 hours). Not surprisingly, all of the users in the top 2% group are either privileged users or ordinary users subscribed for concurrent attacks of at least one hour. The users of this group have been active for an average of 33.5 days and various websites are their primary attack target. In term of attack count, the top 5% of users (14) are responsible for about 40% of all attacks. The users in this group are a mix of gamers and the website attackers. Ten users of this groups have

[4]Note that this option is not available to ordinary users at registration time.

	Gamers	Website	Privileged
Number of users	180	41	8
Avg distinct targets per day	3.32	3.46	2.86
Avg attacks per day	13	13	16
Avg attack time per day	59 m	14 h	105 h

Table 2: Service usage of the three user groups.

subscribed for an attack duration of half an hour or less and the rest have subscribed for durations of more than an hour. Only three of the users in this group overlap with the members of the top 2% group.

The dataset contains a table recording IP address and user-agent of the browsers used by users to login to the twBooter website. A brief analysis of this table reveals that a considerable portion of users were concerned with keeping their identities unknown. Anonymizing services such as proxies, VPN service or Tor network are the most prevalent means used for this purpose. Almost half of the users (137) have initiated at least 50 attack instances. Among those users, 60% (82) have logged in to the service with at least 10 different IP addresses. The average number of distinct login IP addresses for this group of users is 34.

The rest of this subsection discusses usage patterns for each of the three distinct groups of users identified in the previous subsection: gamers mounting short-lived attacks of no longer than 10 minutes, website attackers with attacks lasting between one and two hours and the privileged users with the right to initiate attacks lasting for more than two hours. Users which could not be easily categorized into one of these groups were excluded from the analysis. The users assigned to one of the three groups account for about 83% of all users.

Table 2 summarizes service usage for the three groups of users. As observed, gamers and website attackers exhibit similar behavior in terms of the average number of attacks initiated per day and the number of distinct victims targeted per day. Users in the third group however behave differently. While privileged users tend to target fewer number of distinct victims per day, they initiate more attack instances on those targets. This is probably attributable to the fact that the privileged users are more likely to utilize concurrent attacks.

In terms of the average number of attacks initiated per day, we observe that users in all of the three groups use the service fairly heavily. As expected, the average amount of time spent having an attack carried out varies significantly among each of the user groups. While the maximum duration of an attack for gamers and website attackers is limited to 10 minutes and 2 hours respectively, we have attack records for privileged users that last for a few days. Besides the privilege of mounting longer lasting attacks, higher attack concurrency could be another factor contributing to the huge average attack time for the group of privileged users.

4.3 Victims

For each attack record in the dataset, the target is specified as either an IP address or a website URL. We identified 689 unique websites and 10,485 unique IP addresses in the attack records.

It is possible for a service subscriber to supply an IP address rather than a website URL when initiating an attack on a website. Consequently, the actual number of websites targeted by *TwBooter* could be higher than the above-mentioned number. However, our investigation to identify the IP addresses hosting a website, revealed that most of such IP addresses were actually websites already included in the list of the 689 identified websites. Based on our observations, the number of unique targeted websites is not expected to be significantly higher than the number identified initially.

To understand what types of websites were victims of DDoS attacks initiated by *TwBooter's* subscribers, we manually visited the top 100 websites in terms of the overall time being under attack. While the type of targeted websites is quite diverse, ranging from other Booters to governmental agencies, the overwhelming majority of targeted websites were either game servers or game forums.

An observation of interest was two users ordering attacks on several different governmental websites. The primary focus was on two Indian goverment websites and the website of Los Angles police department. Collectively, the three websites were under attack for a total duration of 142 hours by these two users. This observation suggests that Booter services are serving customers with different intentions ranging from attacking gamers to small to medium sized goverment websites.

4.3.1 Attack Measurement

In order to measure the effectiveness of these attacks, we subscribed to *TwBooter* and initiated a number of attacks to one of our own servers. Table 3 summarizes the measurement results for both a SYN flood and UDP flood. The UDP flood used a DNS reflection and amplification attack to generate 827 MBit/sec of DNS query response traffic directed at our server by sending out large numbers of forged DNS request queries that included our server's IP address as the IP source address. For the SYN flood, we observed 93,750 TCP SYN requests per second with randomly spoofed IP addresses and port numbers directed at our server in an attempt to utilize all of its memory by forcing it to allocate memory for a huge number of half-open TCP connections.

In addition to these two flood attacks, we also launched both HTTP GET/POST attacks on our server to see if proxy servers were utilized by *TwBooter*. We observed a total of 26,296 distinct proxy servers being used for a 5-minute HTTP GET attack and 21,766 proxy servers for an HTTP POST attack of the same length.

Attack Type	# of packets	Avg. packet size	Volume
UDP Flood	4,552,899	1,363 bytes	827 MBit/sec
SYN Flood	5,625,086	54 bytes	40 MBit/sec

Table 3: Summary of measured attacks (duration 60 secs)

5 Conclusion

In this paper, we presented a brief analysis of the low-cost *TwBooter* service which is capable of generating DDoS attacks that have effectively disrupted several medium-sized web sites along with large numbers of gamers. In addition, our analysis shows that this service earned over $7,500 a month and was used to launch over 48,000 DDoS attacks against 11,000 distinct victims including government websites and news sites in less than two months of operation. Also, we provide evidence that other Booter services, such as *asylum*, have launched over half a million DDoS attacks. It our hope is that this analysis will improve our understanding of these services and the increasing threat these services pose to medium sized web sites.

Acknowledgments

We thank Jose Nazario and the other reviewers for their insightful comments. This work was supported by the National Science Foundation under grant 1237076.

References

[1] Sean 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/, 2013.

[2] Brain Krebs. The obscurest epoch is today. http://krebsonsecurity.com/2013/03/the-obscurest-epoch-is-today/, 2013.

[3] Jason Lackey. 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/, 2010.

[4] Bill McCarty. Botnets: Big and bigger. *Security & Privacy, IEEE*, 1(4):87–90, 2003.

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

[6] Aditya K Sood and Richard J Enbody. Crimeware-as-a-servicea survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, 2013.

[7] Stephen M Specht and Ruby B Lee. Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems*, pages 543–550, 2004.

[8] Vrizlynn L Thing, Morris Sloman, and Naranker Dulay. A survey of bots used for distributed denial of service attacks. In *New Approaches for Security, Privacy and Trust in Complex Environments*, pages 229–240. Springer, 2007.