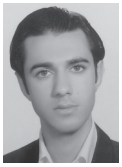
Rent to Pwn

Analyzing Commodity Booter DDoS Services

MOHAMMAD KARAMI AND DAMON MCCOY



Mohammad Karami is a second year PhD student in information security and assurance at George Mason University. His broad research interests include security, trust, and privacy issues in open distributed systems. More recently, he has been working on studying and measuring malicious behavior of financially motivated underground organizations. mkarami@masonlive.gmu.edu

Damon McCoy is an assistant professor in the CS department at George Mason University. Previously he was a Computer Innovation Fellow at the University of California, San Diego. He obtained his PhD from the University of Colorado, Boulder, and his research includes work on anonymous communication systems, cyber-physical security, e-crime, and wireless privacy. mccoy@cs.gmu.edu

Distributed denial-of-service (DDoS) attacks, the practice by which a malicious party attempts to disrupt a host or network service, has become an increasingly common and effective method of attack. In this article, we summarize what we have learned while investigating the phenomenon of what are called booter or stresser services. These booter services began as a tool used by video-game players to gain an advantage by slowing or disrupting their opponents' network connection for a short period of time; however, as these services have become increasingly commercialized, they have morphed into powerful, reliable, and easy to use general purpose DDoS services that can be linked to several attacks against non-gamer Web sites.

We begin with an overview of DDoS techniques. We then outline the common capabilities and infrastructure used by these booter services supported with information found on underground forums that market and review such services. Finally, we present empirical measurements of one particular booter, known as TwBooter, based on a publicly leaked dump of their operational database and our own measurements of their attack capabilities.

Background on DDoS Attack Methods

Well honed DDoS methods can amplify the amount of traffic an attacker is able to generate by an order of magnitude. Also, there are many attacks that take advantage of misconfigured options present in many Web servers to magnify the effectiveness of an attack. Although booter services are not as technologically advanced as cutting-edge DDoS malware, such as Dirt Jumper Drive [3], they implement several of the most effective DDoS attacks. We review a few of the methods that are implemented by most booter services in order to provide an idea of their sophistication.

SYN flood. This form of DoS attack is conducted by rapidly sending large numbers of TCP SYN requests. To make these requests difficult to filter, the IP source address is normally spoofed. The goal of this attack is to force a server to expend a large amount of resources handling these requests, so that it does not have enough resources left to respond to legitimate requests.

DNS reflection. This method enables an attacker to consume all of the victim's bandwidth by amplifying their traffic by a factor of ten or more times the amount of actual traffic the attacker is able to send. The attack takes advantage of several facts. The first is that well-crafted DNS requests can produce DNS replies that are more than ten times larger. The next is that DNS operates over UDP, which is a connectionless protocol; thus the attacker can send a spoofed DNS request that causes the large DNS reply message to be directed to the victim. The last key part of this attack is that there are large numbers of what are called "open DNS resolvers." These are misconfigured DNS resolvers that will provide resolution for clients outside its administrative domain.

HTTP GET/HEAD/POST flood. This attack focuses directly on the Web servers and operates by making a large number of HTTP requests to the Web server, with the goal of triggering database queries or other processes that consume large amounts of server resources.

RUDY/Slowloris. RUDY stands for "aRe yoU Dead Yet," and it again targets Web servers, specifically HTTP forms, with long POST arguments that cause vulnerable servers to exhaust their pool of connections processing these never-ending HTTP POST requests. Another twist on this attack is slowloris, which slowly reads HTTP replies to tie up and exhaust the available pool of connections.

The Underground View of Booter Services

Booter services are relatively easy to locate, and there are countless numbers of them in operation as of the writing of this article. They can be found by Web searches for "booter stresser," and they publicly market themselves as network stress testing services in order to maintain a facade of legitimacy; however, on underground forums, such as hackforums.net, they market themselves as DDoS services that "hit hard" and offer a number of add-on services, such as locating a victim's IP via their Skype ID and a server's real IP address to get around CloudFlare and other anti-DDoS services.

Most of these booter services operate on a subscription model, in which their customers pay a monthly fee that enables them to launch as many DDoS attacks as they want for the month. A basic membership costs around $10–$30 US per month and normally entitles the customer to only one concurrent attack that lasts 30–60 seconds. The subscriber can launch unlimited new attacks after their current one has ended. In order to launch more than one concurrent attack or attacks that last longer (from one to three hours) the customer must purchase more costly premium subscriptions that range in cost from $50–$200 US per month. Most booter services accept payment via PayPal and some accept bitcoins.

On these same underground forums there are advertisements from hosting ISPs that rent servers and are tolerant of launching DDoS attacks. These advertisements and comments from the operators of these booter services indicate that many of them are renting dedicated servers instead of using compromised servers or large botnets for their attack infrastructure. Determining whether a server is rented by an attacker or compromised is difficult; however, from a business perspective, renting servers might make sense because rented servers are likely more stable than compromised servers or botnets.

Additionally, we see many posts on these underground forums from booter service operators claiming they have updated their lists of open DNS resolvers and proxy lists. This provides anecdotal evidence they are exploiting other organizations' misconfigured DNS resolvers for DNS reflection attacks and using public proxies to make it more difficult to filter Web server attacks launched from a small set of dedicated servers via IP address.

Finally, there are posts that indicate many of these booter services are based on code that has leaked or been stolen, such as the asylum booter source code, available at its Web site [1]. This reinforces the fact that there is a low barrier of entry for starting a booter service.

An Analysis of the TwBooter Service

To gain a deeper understanding of booter services, we conducted an empirical analysis of TwBooter (http://booter.tw). 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. Although TwBooter isn't thought to be among the largest booter services, it recently has attracted attention after being linked to a series of DDoS attacks targeting a popular blog on computer security and cybercrime [5] and the Ars Technica Web site [2].

Data Set

Most of our analysis is based on a publicly available SQL dump file of the operational database of the TwBooter service. The data set 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 data set. See our paper [4] for more details on what this data set included.

Duration	Clients	Victims	Attacks
Jan. 2013–Mar. 2013	312	11174	48844

Table 1: Summary of TwBooter data set used in the analysis

Ethics, Legal, Authenticity Implications

When dealing with a leaked data set, many issues must be addressed before using it. Two of the key issues when dealing with potentially stolen data is that the data is used in an ethical and legal fashion. In this case, the data was publicly leaked and previously reported upon, and so we designed a methodology that would minimize any additional harm from our analysis and publication. Specifically, we omitted personal information from our publication, such as email addresses and names of the subscribers, victims (except in the cases were the information was publicly reported), and operators of this service even when these details were known. Another key issue when dealing with data of unknown provenance is checking as much as possible that it is authentic and accurate. For this data set, we contacted three of the victims and confirmed that the data correlated with attacks that they experienced. We also checked to make sure the data was internally consistent. This gives us some confidence that this data is not completely fabricated; however, some of the data could be fabricated or inaccurate.

Attack Infrastructure

Our analysis of the TwBooter leaked data indicates that only 15 distinct servers were used to perform all the attacks launched by this service. This means that TwBooter relies on a smaller set of servers to perform DDoS attacks. Compared to clients, servers utilized for this purpose could be much more effective as they typically have higher computational and bandwidth capacities, making them more capable of starving bandwidth or other resources of a targeted system.

Further analysis shows that only three servers have been active for the entire 52-day period covered by our data. The other servers either left or joined the pool of servers in the middle of the period. A total of nine servers were in active operation as of March 15. The lifetime for the six inactive servers ranged from three days to 16 days, with an average of 11 days. The average lifetime of nine servers that were still active was 32 days. Two of the servers were hosted in the USA and the rest were hosted by an ISP located in the Netherlands. We omit the name of the ISPs because we do not have enough evidence to tell whether the servers have been compromised or have been directly leased from the hosting providers. This supports the anecdotal evidence that booter services have a relatively stable attack infrastructure based on higher powered servers.

Attack Measurement

Although TwBooter implemented 12 different attack types, the ones mentioned above account for more than 96% of all performed attacks. To measure the effectiveness of these attacks, we subscribed to TwBooter and initiated a number of attacks to one of our own servers. Table 2 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 Mb/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 addition to these two flood attacks, we also launched both HTTP GET/POST attacks on our server to see whether proxy servers were utilized by TwBooter. We observed a total of 26,296 distinct proxy servers being used for a five-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	4552899	1,363 bytes	827 Mb/sec
SYN flood	5625086	54 bytes	40 Mb/sec

Table 2: Summary of measured attacks (duration 60 secs)

Customers

A total of 277 active users subscribed to the TwBooter within the time period of the data set. The subscription information and information on the cost of each combination of options allows us to estimate that TwBooter earned $7,727 a month. Assuming they were paying around $250–$300/month each for nine dedicated servers at a hosting ISP, this would be a profitable enterprise.

To make our analysis easier to understand, we classified users into three categories of behavior based on their subscription type: (1) gamers mounting short-lived attacks of no longer than 10 minutes, (2) Web site attackers with attacks lasting between one and two hours, and (3) privileged users with the right to initiate attacks lasting for more than two hours. Some users could not be easily categorized into one of these groups and were excluded from the analysis. The users assigned to one of the three groups account for about 83% of all users.

The intuition behind this method of classification is that TwBooter utilizes high bandwidth servers to mount DDoS attacks. Gamers typically use residential Internet connections to play online games. Considering the limited capacity of a gamers' links, they can be easily overwhelmed with large amounts of traffic originated from one server for a short period of time. For this reason, the majority of TwBooter users targeting gamers have subscribed for short-lived DDoS attacks. We found that users who subscribed for durations of between 10 minutes to less than an hour were difficult to classify, and thus we have left them out of this analysis. Those subscribed for an attack duration of an hour or more are likely to be users targeting Web sites. Interestingly, there are a few users who have the privilege to initiate attacks lasting more than two hours, an option that is not available to ordinary users at registration time.

Table 3 summarizes service usage for the three groups of users. As observed, gamers and Web site 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. Although privileged users tend to target fewer 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.

	Gamers	Web site	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 3: Service usage of the three user groups

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. Although the maximum duration of an attack for gamers and Web site attackers is ten minutes and two 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.

Victims

For each attack record in the data set, the target is specified as either an IP address or a Web site URL. We identified 689 unique Web sites and 10,485 unique IP addresses in the attack records.

To understand what types of Web sites were victims of DDoS attacks initiated by TwBooter's subscribers, we manually visited the top 100 Web sites in terms of the overall time being under attack. Although the type of targeted Web sites is quite diverse, ranging from other booters to governmental agencies, the overwhelming majority of targeted Web sites were either game servers or game forums. In addition to the attacks on the two journalists, we noticed two users ordering attacks on several different governmental Web sites. The primary focus was on two Indian government Web sites and the Web site of the Los Angeles Police Department. Collectively, the three Web sites were under attack for a total duration of 142 hours by these two users.

Conclusion

Our analysis of TwBooter's attack infrastructure, customers, and victims support the anecdotal evidence that these services are popular and profitable services that are upgrading their attack capabilities as their user bases expand. This enables this service and others to expand from their original purpose as tools used to gain an advantage against gaming opponents, and they are now used to target a diverse set of victims ranging from gamers to small- and medium-sized government Web sites. We have other leaked data sets from larger booter services, such as Asylum, that indicate they had customer bases in the thousands and have been used to launch hundreds of thousands of attacks a year.

The biggest transformation these services create is a business model in which attackers can rent and share DDoS infrastructure that is managed by the booter service instead of building and maintaining their own dedicated infrastructure, thus reducing both the technical and monetary barriers to launching DDoS attacks.

Acknowledgments

We thank Jose Nazario and the other reviewers for their insightful comments of our earlier related LEET paper. This work was supported by the National Science Foundation under grant 1237076 and a gift from Google.

References

[1] http://softwaretopic.informer.com/asylum-booter-source/.

[2] 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.

[3] Kelly Jackson Higgins, "DDoS Botnet Now Can Detect Denial-of-Service Defenses": http://www.darkreading.com/attacks-breaches/ddos-botnet-now-can-detect-denial-of-ser/240160466, 2013.

[4] Mohammad Karami and Damon McCoy, "Understanding the Emerging Threat of DDoS-as-a-Service," LEET 2013: https://www.usenix.org/conference/leet13/understanding-emerging-threat-ddos-service.

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