Exploring the provision of online booter services

Paper by Dr Alice Hutchings and Dr Richard Clayton

Presented by Chongyang Shi

November 13, 2017

Historical Context: Booter Services

- Distributed Denial of Service (DDoS) attacks have been around since late last century. (Yan et al., 2000) [1]
- Booters are low-cost short-duration DDoS attacks sold as a service, with their name coined by Karami and McCoy in 2013. [2]
- Often used for petty reasons such as disrupting an online gaming opponent. [3, p. 1163]
- Provisioning and use are illegal under Computer Misuse Act 1990 and others.

Historical Context: Assessing the Scale of Operations

Leaked database from a single operator:

- 48,000 attacks, 11,000 victims over 52 days, yielding US$7,727 per month.
- Most users were gamers using short attacks up to 10 minutes.

While the technical methods behind these services have been studied in detail [2], the scales and motivations of their operators had not been studied.

- The need for a more comprehensive study into the booter service "industry".
- There have been few research into cybercrime offenders themselves overall. [4]

Key Definition: DDoS Attacks

- DDoS attacks seek to prevent legitimate access to the victim server by sending an overwhelming amount of requests.
- DDoS attacks can be amplified by forging packet headers to achieve reflection.
- Reflected attacks cost less to initiate and cost more to filter – vastly favouring the attacker.
- Reflector attacks exploit the unauthenticated nature of common protocols.
- Other types of attacks also seen offered by booter services, such as HTTP flood on Layer 7, but far less "efficient".

Key Definition: Criminology Theories

Traditional criminology theories will be used to study booter service operators:

- Differential association
- Techniques of neutralisation
- Rational choice theory

Key Definition: Differential Association

Sutherland's theory of differential association [5]:

- Criminal behaviour is normal behaviour learnt in interaction with others in intimate personal groups.
- Different people respond to criminal behaviours of peers differently. Response also dependent on frequency of association.
- Online communities have made differential association easier for cybercrime offenders.
- Demographic features of these communities.
- Greater the differential association, greater the likelihood of self-reporting their participation.

Key Definition: Techniques of Neutralisation

Sykes and Matza's theory on techniques of neutralisation [6]:

- Offenders learn to use techniques to justify or neutralise acts to mitigate feelings of shame or guilt.
- Offenders may distinguish between "appropriate and inappropriate" targets.
- Techniques include denying responsibility, injury or victims; condemning the condemners; appealing to higher loyalties.
- Computer as a medium makes neutralisation easier.
- Some techniques more frequently observed in cybercrime offenders than others.

Key Definition: Rational Choice Theory

Cornish and Clarke's theory of rational choice [7]:

- Offenders calculate the perceived cost and benefits of crime, in seeking some kind of advantage.
- Offenders assess their skills and resources against perceived risk.
- Risk of detection and risk of punishment may bear different weights.
- Cybercrime: usually low perceived risk, benefits primarily financial.
- Personal gratification gained from committing skilled crimes.

The Study: Overview

- Conducted from July to September 2014.
- Mixed method and cross-sectional design.
- Attempt to examine the entire population of booter service operators.
- Data analysed with quantitative (limited due to sample size) and qualitative analysis.

Results: Recruiting Participants

How the f— did you get to it? I don't even advertise it anywhere and have no idea how you even found it.

A booter service operator participating anonymously in the study

The Study: Recruiting Participants

- Focused on openly advertised operators only, operators in hidden services not surveyed.
- Keyword search, online criminal forums.
- Collection process conducted more than once to find more operators.
- Some booter services may be operated by the same operator.
- Operators contacted via public/customer contact information.

The Study: Conducting the Survey

- Aim of study explained to the contacted operators.
- Randomised invitations to either an online survey or an interactive interview.
- Alternative participation method sent if no response.
- 63 invited, 13 responses (from 12 unique sites), 11 completed the survey, while 2 were interviewed.
- Overall response rate 25%, higher than expected.

The Study: Purpose of the Survey

The survey aims to understand:

- Motivations of booter service operators.
- Perceptions of legality in operating booter services.
- Market and economic benefits.
- Time commitment, reasons for involvement, methods of involvement.
- Technical aspects of their services.

All questions were optional to encourage involvement.

Results: Participant Characteristics

Because in the future I don't plan on having a job so shitty that I need to resort to reviewing f—— booters.

A booter service operator when asked about future aspirations

Results: Participant Characteristics

General demographics of participants:

- Barring creative responses, it is apparent that all participants are male.
- All between 16 and 34 years old.
- Most operated a booter service for less than 3 years.
- From 5 different continents.
- Mostly student, but also include two with other employments.

Results: Participant Characteristics

- Most operators consider themselves to have a high level of technical proficiency.
- Originating from related skills such as web development and OS/networks knowledge.
- Some have a gradual pathway to offending, starting as a user of these services.
- Some provide backbone services to other booter service operators.
- Many operators also operate other online services, both legal and illegal.

Results: Differential Association Analysis

- Booter service operators often start offending under the influence of others, or through exposure to these services via gaming and online communities.
- Some had peers already in the business, and were introduced to profit potentials.
- Learning technical skills and providing legitimate pentest tools were also motivations.

Results: Techniques of Neutralisation

- Majority of operators surveyed attempted to neutralise or excuse their behaviour.
- Appealing to higher loyalties: providing service "for the common good" to create more secure systems overall.
- Perceptions of legality: some operators believe that booter services are not illegal in their jurisdiction, or vary by target of attack.
- Denying responsibility: some believe that the users of their services are responsible for using it for purposes other than stressing their own networks.
- Condemning the condemner: one participants questions the severity of booter services when compared with online pornography and other illegal activities.

Results: Techniques of Neutralisation

- Cross-comparison of responses also reveal interesting observations.
- Booter service operators consider the use of their services against different types of targets differ in legality and moral correctness.
- In denying responsibility, many booter service operators believe that it would be illegal to use their services against third-party targets, but it will not be up to them to police it, echoing appeals to higher loyalties.

Table 2. Beliefs about whether tests against different targets are illegal.

Are the following against the law in your location?	*Yes*	*No*	*Don't know*
Provision of stresser services in general (n = 9)	1 (11.1%)	5 (55.6%)	3 (33.3%)
Stresser tests against game servers (n = 8)	2 (25.0%)	3 (37.5%)	3 (37.5%)
Stresser tests against TeamSpeak servers (n = 8)	2 (25.0%)	3 (37.5%)	3 (37.5%)
Stresser tests against individual Internet users or organizations (n = 8)	2 (25.0%)	3 (37.5%)	3 (37.5%)

Table 3. Appropriateness of tests against different targets.

How appropriate are the following, on a scale of one (totally inappropriate) to ten (totally appropriate)?	*M*	*SD*	*Range*
Provision of stresser services to anyone who wished to buy them (n = 8)	7.75	3.66	1–10
Stresser tests against game servers (n = 8)	4.88	3.52	1–10
Stresser tests against TeamSpeak servers (n = 8)	4.00	3.51	1–10
Stresser tests against individual Internet users or organizations (n = 8)	4.88	4.45	1–10

Results: Rational Choice analysis

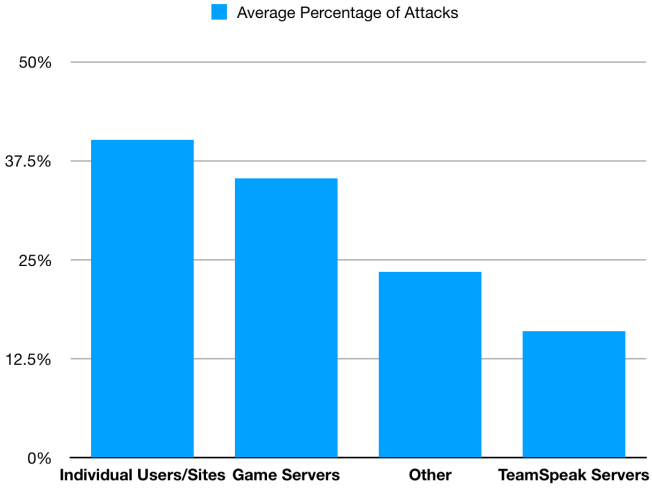
- Financial gains appear to be the prime motivation for booter service operators.
- Conservative estimate of income is between US$3705.25 and US$5430.67.
- However, it is not a significant income source to all operators, the responses were evenly distributed.
- Operators invest vastly different amounts of time into maintaining their service.
- Technical excitement is also a motivation to some operators.

Results: Service Architecture

- Both Layer 3/4 and Layer 7 DDoS attacks offered by operators.
- Generally moving away from Layer 7 due to increased accessibility of DDoS protection products.
- Technically proficient operators programmed their own systems, while others paid for others to code.
- Some operators run services on their own, others have collaborators.
- Search engine and URL access are primary methods of reaching the services.

Results: Attack Targets

Aggregated percentages of attack targets:



Selected Cited Papers

Prior analysis of Booter services, mostly on technical aspects:

- *Understanding the Emerging Threat of DDoS-as-a-Service*, Karami and McCoy, 2013 [2]
- *Rent to Pwn: Analyzing Commodity Booter DDoS Services*, Karami and McCoy, 2013 [8]
- *Characterizing and mitigating the DDoS-as-a-service phenomenon*, Santanna and Sperotto, 2014 [9]

Criminology theories used:

- Differential association: Sutherland, 1949 [5]
- Techniques of neutralisation: Sykes and Matza, 1957 [6]
- Rational choice theory: Cornish and Clarke, 1987 [7]

Several of the authors' previous works are also ingrained in the criminology analysis.

Current Context

Characteristics of Booter victims (primarily residential users, content popularity has little effect):
Who gets the boot? Analyzing victimization by DDoS-as-a-Service A. Noroozian et al., 2016 [10]

Automatic identification of Booter services (identifying more potential booter services with crawling):
Booter blacklist: Unveiling DDoS-for-hire websites, J. J. Santanna et al., 2016 [11]

Collecting research data from illicit sources:
Ethical issues in research using datasets of illicit origin, D. R. Thomas et al., 2017 [12]

Critique

Owing to the illicit nature of the services studied, the limited sample size makes ascertaining the conclusions difficult:

- Sample size
  - 63 services manually identified, 13 responses, most questions not answered by all participants.
  - Deriving statistically significant data is difficult.
  - Could automatic booter service identification [11] help?
- Sample coverage
  - While most booter services are openly advertised, would it be possible to assess the scale of their operations on hidden services ("the dark web")?
  - All participants operate in English, would the characteristics of operations of non-English booter services differ?
  - As identified by the authors, the self-selection bias may affect responses used in criminology analysis.

Suggested Discussions

- Are there ways to understand the motivations of illicit service operators while avoiding the self-selection bias inevitable resulted by surveying them?
- To control the growth of booter services, what technical solutions are available to increase the perceived risk of operating booter services, or to reduce differential association of these communities?

References I

- J. Yan *et al.*, "The xenoservice-a distributed defeat for distributed denial of service," in *Proceedings of ISW*, vol. 2000. sn, 2000.
- M. Karami and D. McCoy, "Understanding the emerging threat of ddos-as-a-service." in *LEET*, 2013.
- A. Hutchings and R. Clayton, "Exploring the provision of online booter services," *Deviant Behavior*, vol. 37, no. 10, pp. 1163–1178, 2016.
- T. J. Holt and A. M. Bossler, "An assessment of the current state of cybercrime scholarship," *Deviant Behavior*, vol. 35, no. 1, pp. 20–40, 2014.
- E. H. Sutherland, G. Geis, and C. Goff, *White collar crime: The uncut version*. Yale University Press New Haven, CT, 1983, vol. 58.
- G. M. Sykes and D. Matza, "Techniques of neutralization: A theory of delinquency," *American sociological review*, vol. 22, no. 6, pp. 664–670, 1957.

References II

- D. B. Cornish and R. V. Clarke, "Understanding crime displacement: An application of rational choice theory," *Criminology*, vol. 25, no. 4, pp. 933–948, 1987.
- M. Karami and D. McCoy, "Rent to pwn: Analyzing commodity booter ddos services," *login:: the magazine of USENIX & SAGE*, vol. 38, no. 6, pp. 20–23, 2013.
- J. J. Santanna and A. Sperotto, "Characterizing and mitigating the ddos-as-a-service phenomenon," in *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, 2014, pp. 74–78.
- A. Noroozian *et al.*, "Who gets the boot? analyzing victimization by ddos-as-a-service," in *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 2016, pp. 368–389.
- J. J. Santanna *et al.*, "Booter blacklist: Unveiling ddos-for-hire websites," in *Network and Service Management (CNSM), 2016 12th International Conference on*. IEEE, 2016, pp. 144–152.

References III

D. R. Thomas *et al.*, "Ethical issues in research using datasets of illicit origin," 2017.