This is an Accepted Manuscript of an article published by Taylor & Francis Group in Deviant Behavior on 9 May 2016, available online:
http://www.tandfonline.com/10.1080/01639625.2016.1169829

Exploring the provision of online booter services

Alice Hutchings[1] and Richard Clayton[2]

Abstract

This research uses differential association, techniques of neutralisation and rational choice theory to study those who operate 'booter services': websites that illegally offer denial-of-service attacks for a fee. Booter services provide 'easy money' for the young males that run them. The operators claim they provide legitimate services for network testing, despite acknowledging that their services are used to attack other targets. Booter services are advertised through the online communities where the skills are learnt and definitions favourable towards offending are shared. Some financial services proactively frustrate the provision of booter services, by closing the accounts used for receiving payments.

Keywords

Denial of service attacks, booter services, differential association, techniques of neutralisation, rational choice theory, cybercrime

[1] Computer Laboratory, University of Cambridge, Cambridge CB3 0FD, UK
email: alice.hutchings@cl.cam.ac.uk

[2] Computer Laboratory, University of Cambridge, Cambridge CB3 0FD, UK
email: richard.clayton@cl.cam.ac.uk

Introduction

Distributed denial of service (DDoS) attacks involve overloading a website or computer system with so much bogus traffic that legitimate access is unlikely to succeed. The websites selling DDoS attacks for a fee are termed 'booter' or 'stresser' services. Booter comes from the malicious act of 'booting' a games player out of an online game, but the 'stresser' nomenclature has a benign meaning in that it refers to stress tests performed against one's own servers to assess their resilience. We use 'booter' in this paper to reflect the reality of the way in which these services are used.

Booter services: An overview

Booter services have been previously studied by Karami and McCoy (2013a; 2013b), and they give a detailed technical account of the technical methods used to send large amounts of bogus traffic to overwhelm the DDoS victim. The services we study in this paper were mainly using amplification techniques – small request packets are sent to a third-party computer, which returns (reflects) a much larger response, often 10 to 20 times the size. However, the source of the requests is forged so that the responses go to the victim. By using many reflectors in parallel the booter service can overwhelm many victims simultaneously using just a single server to generate the request packets.

The booter services we studied offered their customers a range of membership options, from basic to premium subscriptions with the higher levels allowing users to request longer attacks and attacks on more than just one target at a time. Payment by PayPal is generally possible; however alternative payment options are usually available, including digital currencies such as Bitcoin. Entry level pricing allowing 10 minute attacks on one target at a time was typically priced at less than US$ 5.00 a month.

DDoS attacks have been used in extortion, with an attack that prevents a business from operating being followed by a demand for payment to make the attack cease. Extortion has worked best during crucial times for businesses, such as before big sporting events for betting websites (Menn 2010). Some businesses anticipate such attacks and purchase DDoS protection services from companies such as CloudFlare (CloudFlare 2014). DDoS attacks against government websites have been used as a method of protest, such as attacks against the website of the Australian Federal Parliament by Anonymous under the codename 'Operation Titstorm' in response to plans to filter online material (Hardy 2010).

However, as Karami and McCoy (2013b) make clear, an important aspect of DDoS attacks is their use by online gaming competitors who cheat by preventing good opponents from participating, by disrupting the opposing teams' communications (TeamSpeak) servers or by disrupting the game servers themselves. They analysed a leaked database from one of the booter services which documented 48,000 attacks against 11,000 victims over a 52 day period. The service received an income equivalent to US$ 7,727 per month. They concluded that the majority of the users were gamers, who used short-lived attacks of up to 10 minutes. Similarly, the majority of victims were game servers and forums, although other booters, government websites, and journalists had been targeted. Relevant though this information is, it is for just one booter service (and one that allowed their database to be compromised) so it is problematic to scale it up. To estimate the overall size of the booter market, Santanna and Sperotto (2014) identified 59 booters operational from October 2013 to mid-2014. Of these, 34 were reachable at all times, while the remaining 25 were, at times, offline.

The crime

DDoS attacks are criminal in many jurisdictions and the legislation addresses both those providing services for hire and those that use the services. In the United States, s1030(a)(5) of the *U.S. Code Title 18* creates an offence for knowingly causing the transmission of a program, information, code or command that causes damage without authorisation to a protected computer. Similarly, s3 of the *Computer Misuse Act* 1990 in the UK and s477.3 of the *Criminal Code Act* 1995 (Commonwealth) in Australia criminalise 'unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer' and 'unauthorised impairment of electronic communication' respectively. Both the UK and Australian legislation provides penalties of up to 10 years imprisonment. The maximum available US punishment scales up with the type of harm caused, from 10 years and/or a fine, up to life imprisonment if the conduct results in death.

Arrests and convictions for DDoS attacks date back many years, with the 'Mafia Boy' attacks on Amazon, eBay etc. being one of the earliest cases to make headlines in 2001 (Verton 2002). The first known arrest relating to booter services was in 2010, in the United Kingdom (BBC News 2010). A 17 year old male was arrested after a DDoS attack against an online game using a booter service. It appears that he was a user, rather than the operator, of the booter service. The outcome of the case is unknown.

In Australia in 2014, a 21 year old male was charged by police after he allegedly accessed the servers of an online game without authorisation (Chamberlin and Donaghey 2014). Along with usernames, email addresses, salted password hashes and transaction records, it was alleged that he obtained, and then sold, IP addresses of the users, that could be used on booter services to gain an advantage against

adversaries. It is alleged that he had received 880 payments for the data. Again, the outcome of this case is not known, although enquiries have been made.

Our contribution

What is missing from the research by Karami and McCoy (2013a; 2013b), and proposed by Santanna and Sperotto (2014), is the backstory of those that provide these services. As noted by Holt and Bossler (2014), there has been little research into the offenders who commit complex forms of cybercrime. We use criminology theory to explore how and why offenders begin providing booter services.

In order to understand more about the provision of booter services, we asked those providing the services to tell us about themselves and their activities. This has been a successful way of understanding offline crimes such as burglary (Bennett and Wright 1984; Wright and Decker 1994). We used both online and interactive surveys and our experimental design informs future research into online offender populations by demonstrating how well each method performed. Our research is also unusual because it includes the entire known, albeit small, population of offenders. Booter services are provided through publicly accessible websites, and are advertised on forums where their potential customers are active. We invited the operators of every one of these websites to take part, and thus it is the first research into active cybercrime offenders for which a response rate can be determined.

Criminological theories

We use a number of criminological theories to inform our research into the provision of booter services. We use multiple theories as each provides unique and complementary insights into the nature of online crime. These include learning and the influence of others (Sutherland's (1949) theory of differential association), how offenders perceive the wrongfulness of their actions (Sykes and Matza's (1957)

techniques of neutralisation), and the drive for gain with (dis)regard for the consequences (Clarke and Cornish's (1985) rational choice theory).

Differential association

The key point from Sutherland's theory of differential association is that criminal behaviour is normal behaviour learnt in interaction with others (Vold et al. 2002). The theory consists of nine specific points. Summarised, these points are that criminal behaviour is learnt in interaction with other persons in intimate personal groups. What is learnt includes both the techniques of committing crime, and "motives, drives, rationalisations and attitudes" (Sutherland et al. 1992:89) either favourable or unfavourable to committing crime. Crime is committed when those definitions favourable to committing crime exceeds those unfavourable to crime (Sutherland et al. 1992).

There are two basic elements of differential association. The first is the cognitive element, or the content of what is learnt, such as "specific techniques for committing crimes; appropriate motives, drives, rationalisations, and attitudes; and more general definitions favourable to law violation" (Vold et al. 2002:160). Sutherland did not specify the learning mechanisms, simply stating that "the process of learning criminal behaviour … involves all of the mechanisms that are involved in any other learning" (Sutherland et al. 1992:90). The second element of differential association is the associations with other people in intimate personal groups where the learning takes place (Vold et al. 2002).

In explaining why different people exposed to the same social conditions may or may not conduct criminal behaviour, Sutherland claimed that it is the meanings that they give to these conditions that they experience that determines whether they violate the law. These meanings vary with the "frequency, duration, priority and

intensity" (Sutherland et al. 1992:89) of the associations with criminal groups. Sutherland supported this argument with qualitative research techniques (Vold et al. 2002).

Research indicates that high tech cybercrime offenders learn from each other and share information between themselves (Holt 2007; Hutchings 2014; Jordan and Taylor 1998; Levin et al. 2012). There are many well-developed online communities which are used for learning and sharing information and ideologies, recruiting others to commit offences, and trading tools (Holt 2007; Hutchings and Holt 2015; Levin et al. 2012). The online social communities where differential association and learning takes place tend to be male-dominated and less accepting of those that identify as female (Hutchings 2013a). These communities are based on a subculture of gaming and online interaction that relates to the young age of the participants (Hutchings 2014).

Hollinger (1993), while not organising his study of software piracy and unauthorised computer account access around a theoretical perspective, included variables measuring participants' friends' involvement in these types of crime, as well as self-reported involvement. Hollinger (1993) found that as the number of friends who were involved in unauthorised access to computer accounts increase, so did the likelihood that the participant would report partaking in this activity. Similarly, Holt et al. (2012) found that deviant peer associations within a student population were related to self-reported cybercrime.

Techniques of neutralisation

Sykes and Matza's (1957) theory, techniques of neutralisation, is that offenders learn to use techniques to justify or neutralise acts that might otherwise produce feelings of shame or guilt, and distinguish between "appropriate and inappropriate targets for…

deviance" (Sykes and Matza 1957:666). These techniques include to deny responsibility, to deny injury, to deny the victim, to condemn the condemners, and to appeal to higher loyalties (Sykes and Matza 1957).

Sykes and Matza (1957) argued that techniques of neutralisations were an extension of legal defences to crime, such as provocation or self-defence, which were seen as legitimate by those utilising them but not by the justice system. An interesting defence that has been raised by some defendants accused of computer-related crime, sometimes successfully, is that of addiction to computers, which they argued compelled them to act in the way that they did (Smith et al. 2004). Such an excuse would relate to the technique denial of responsibility posed by Sykes and Matza (1957).

McQuade (2006:160) states that techniques of neutralisation is a sound explanation for computer crime as the physical removal from the victim allows the offender to deny injury or deny the victim with ease:

> *Since they cannot see the Internet or the people who create content, victims, if they are contemplated at all, become faceless entities, computer systems, or perhaps corporations rather than real people whose livelihoods and wellbeing are compromised…*

Yar (2005) also states that hackers' self-purported motivations for offending may be forms of neutralisations aimed at overcoming guilt. Yar (2005:391) describes these motivations as:

> *Intellectual curiosity, the desire for expanding the boundaries of knowledge, a commitment to the free flow and exchange of information, resistance to political authoritarianism and corporate domination, and the aim of*

improving computer security by exposing the laxity and ineptitude of those charged with safeguarding socially sensitive data.

Additional neutralisations proposed by Grabosky (2005) include blaming the victim as being deserving of attack, claiming that no harm was done by simply accessing data, that corporate victims could afford losses, or claiming that everyone else did it.

A study by Turgeman-Goldschmidt (2009) into the use of techniques of neutralisation by offenders engaged in hacking, software piracy and phone phreaking found evidence that these offenders: deny injury by claiming that "downloading information is copying rather than stealing"; deny the victim by justifying their actions as revenge or targeting sites owned by the 'enemy', such as Nazis and Microsoft; condemn the condemners, such as those who prevent access to the information that they are seeking; and appeal to higher loyalties, especially the hacker ethic of freedom of information. However, Turgeman-Goldschmidt (2009) found no evidence that these offenders engaged in denial of responsibility.

In comparison, Walkley (2005) analysed techniques of neutralisation to determine its explanatory power in relation hacking and internet fraud, concluding that there was strong support for denial of responsibility and mixed support for the other techniques of neutralisation. Using open source data Walkley (2005) claimed that, when internet addiction, as a mental health problem, has been used as a defence in court, the defendants were neutralising their actions by denying responsibility. Walkley (2005) also stated that two defendants, who claimed that their computer had been infected with a virus or trojan which had caused the damage they were charged with, were also engaging in denial of responsibility, despite the fact that in both instances the defendants had been acquitted and therefore were found not to have been responsible at all.

The techniques of neutralisation that Hutchings (2013b) found in use by cybercrime offenders include denial of injury (as there is no loss to individual victims) and denial of the victim (as they do not secure their systems, are undertaking questionable activities, or are perceived to have done them wrong). Offenders sometimes avoid targets when they are seen as undeserving of victimisation or there is the potential for innocent parties to be harmed. Use of condemnation of the condemners as a technique of neutralisation is evidenced where it is accused that the victim has caused harm to others, for example if a military site is being attacked. Offenders also appeal to higher loyalties when their actions are believed to be for the common good, such as increasing transparency or revealing vulnerabilities. However in support of Turgeman-Goldschmidt's (2009) findings, Hutchings (2013b) found little evidence for the use of denial of responsibility. For example, active offenders advised that they consider themselves to be addicted to computers, however they do not perceive this as warranting a legal defence.

Rational choice theory

Rational choice theory assumes that offenders calculate the perceived costs and benefits of crime with the assumption that they seek some type of advantage from their actions, be it "money, sex or excitement" (Cornish and Clarke 1987:935). Clarke and Cornish's rational choice theory looks at how offenders in particular situations make these calculations (Vold et al. 2002). The theory acknowledges that offenders' perceptions of costs and benefits can be subjective, "…constrained as they are by time, the offender's cognitive abilities, and the availability of relevant information…" (Cornish and Clarke 1987:933), and therefore may not be rational at all (Akers and Sellers 2004).

Other "choice-structuring properties" (Cornish and Clarke 1987:935) are offence specific. To demonstrate, when offenders weigh up the type and amount of benefit likely against the perceived risk of detection and punishment, they take into consideration their skills and the skills needed to successfully commit the offence, and the availability of necessary equipment or situations (Cornish and Clarke 1987). In addition, each of these considerations may not have equal weight. For example, a high likelihood of detection may be more influential in deterring crime than harsh punishments (Clarke 1997).

Research into cybercrime has found that offenders generally perceive the likelihood of being detected as low, and this holds greater weight than the harshness of available punishments (Hollinger 1993; Hutchings 2013a; McQuade 2006; Skinner and Fream 1997). Benefits obtained from general offence types are mainly financial, while those engaged in more technically challenging types of offending enjoy a greater range of benefits. These include skill development, fun and excitement, social status, power and sexual gratification (Hutchings 2013b). Hutchings (2013a) found that offenders desist from cybercrime when they no longer receive benefits from offending, or when costs outweigh benefits. For example, some offenders stop when they no longer experience excitement or obtain a sense of achievement from their activities. The costs to offenders are not limited to the punishments metered out by the criminal justice system. As offenders believe that the likelihood of detection is low, costs associated with offending are mainly social in nature, including the amount of time they spend online, which interferes with legitimate employment or intimate relationships. Costs also include feelings of guilt or shame, which may previously have been mediated by being online, as offenders are not in physical contact with victims.

Our survey of booter operators

We employed a mixed method, cross-sectional design, examining the provision of booter services within the population at one point in time. Data were collected from July to September 2014.

We started by compiling a list of booter services. These services are openly advertised – the operators do not find it necessary to hide in the 'dark web' but seek to be as easy to locate as possible. We ran searches for relevant keywords (booter, stresser and DDoS), identified existing lists of booter services, and visited several online criminal forums where booters are advertised to determine which services were being promoted (or indeed mentioned in comments as being superior to the new service). This gave us an initial list of 45 operational booter services, but we repeated this phase a few weeks later and eventually identified 63 distinct websites, albeit it became clear some of the operators were running more than one website so there were perhaps just 40 to 50 individuals involved in the business.

We set up a pseudonymous account on every website, but we found that in only a handful of cases could we determine contact details for the owner either from the website contents, the domain registration records or the PayPal address offered for payments. Fortunately, almost all of the websites had online contact forms that provided a way for customers to report technical issues or discuss billing problems, and we mainly used these contact forms as a way of reaching the website operators.

Recruitment

We wanted to understand how to get the highest possible level of response to this type of survey so we randomly assigned our population into two groups. One group (n=32) was sent an explanatory message along with a link to an online (Survey Monkey) survey, while the other group (n=31) was sent the same explanation of our aims, but

was invited to participate in a real time, online, interactive interview. Participants were provided with a unique URL for the online survey to allow us to know if the link was shared with anyone else.

The original intention was to collect data for a period of four weeks. Each group was to receive an invitation for the method that they had been assigned (online survey or interview), and after two weeks they would also be offered the alternative way to participate, in order to maximise the response rate, with a total of four invitations to participate. In practice, data collection continued for longer than intended. This was due to the varied availability of the sites. On average, 2.5 invitations were sent for each website, with a maximum of four invitations. Of the population of 63 that were invited to participate, 7 declined to do so, 25 did not reply to the invitations, 7 did not receive all four invitations as their websites went offline during the data collection period, and 12 sites did not receive any invitations as their websites were either offline, or they did not have means available to contact them.

In total, 13 responses were received with 7 from the online survey group. However, 2 of these used the same unique URL, apparently because they ran the site together. Of the 6 responses from the interactive interview group, 4 opted for the later online survey option. In the end 2 participants opted for the interactive survey, while the remaining 11 completed the online survey. This is an overall response rate of 25% from the population size of 51 who received at least one invitation to participate.

The survey of booter service providers

Our main aim was to understand the motivations of the people operating these websites, their perceptions of the (il)legality, the market for their services and the economic benefits they might receive. We also wanted to understand the time commitment, how they became involved in the business, whether they work with

other people, along with practical details about how the customer-facing websites and backend services were set up.

The survey used for this research was constructed using a mix of closed and open-ended questions, in order to encourage a broad range of responses. The survey included 32 items, and participants could opt not to answer any of the questions that were asked. Throughout the survey, the services were referred to as 'stresser services'. It is not believed that this choice of terminology affected participants' responses, as they readily acknowledged that their services were used for online attacks, and the term 'booter' was used repeatedly in participants' open-ended responses.

The data were analysed using quantitative and qualitative analysis procedures. The content from the qualitative analysis in the results section are provided verbatim. As the population size is relatively small, the quantitative analysis conducted is primarily descriptive.

Results

Participant characteristics

Three participants did not answer any questions relating to their characteristics. The remaining ten participants were rather homogeneous with regards to age and gender. Eight participants were male, and two selected the 'other' category (with the supplied responses being 'alien' and 'Trigender Pyrofox', a reference to a *Cyanide and Happiness* webcomic). Nine participants were in the 16 to 24 age group, while the other was aged 25 to 34. Seven participants responded to the question asking what date they started providing these services. These responses were used to calculate the number of years that they had been operating for, which ranged from 0.67 to 3.01 years ($n = 7$, $M = 1.64$, $SD = 0.75$). Five participants advised that they lived in North

America, two were in Europe, while the remaining participants lived in Asia, Africa, and Australia. Eight participants were students, while two were working at some other place of employment.

Participants were asked how they rated their computer and technical proficiency. Only one participant believed that they were 'below proficient', with the reason for this self-rating being *"still a kid got a lot more to learn"*. Another two selected 'proficient'. One explained that although he could know a lot more than he currently did, he knew a lot more than the average person. The other stated that he could get done whatever he wanted to get done, if he could get himself to spend the time on it. Seven participants self-rated themselves as 'advanced'. When supplying reasons for this rating, three participants referred to knowledge of web development, computer networks, operating systems, and programming languages. One participant referred to future aspirations:

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

For some, the pathway to offending was gradual, with an escalation in offending. Some first began by using booter services, before offering these services themselves. One participant described how he started offering these services to clients of his web hosting company, and later made them publicly available. The following participant was a user of these services, began providing a small service himself, and now offers multiple services to others:

> *First, I use to host Game servers. After using stresser stuff for my servers, I did a deep research on it and decided to open my own stresser to provide stress testing service to other. After seeing profit in it, I decided to open two*

more stresser to expand. Currently, I'm running three stresser and a hosting company.

Nine participants responded to the question about whether they provide these services on other websites. Six participants provided these services on the one site only, while three provided services on one or more additional sites. One of these participants advised that:

I manage the back end system such as dedicated servers and ensuring the service operates for multiple other stresser services that I'm sure they'd like to remain unnamed, but yes. [Interviewer asked a question about how many sites]*: 5, which includes the one you're current interviewing me about.*

Seven participants advised that they provided other online services, in addition to stresser services. One specified that they did not provide any additional services, and five did not answer this question. Combinations of legitimate and illegal, or potentially illegal, services were listed. On the more lawful side, there were coding services, pentesting services, hosting virtual private servers, web development, webhosting, resolvers, and Minecraft server hosting. Participants also advised that they provided 'Stressing API' services, setup stressing servers, phone number geo locators and PayPal limitation services (it is presumed that this refers to restoring limited PayPal accounts). One participant stated:

I would rather not divulge the names of other companies I am involved in, however, I can say that I am involved in providing DDoS protection services, high availability web hosting, dedicated server hosting, and virtural server hosting.

Later, the same participant sent the following advertisement over Skype to the account we used for our interview (and doubtless to others as well):

Offering FaceBook Hacking [Service] *minimal for a job is $30.*

Differential association

Two main themes arose from the question as to how participants became involved in providing booter services. These included the influence of others, and exposure to these services through gaming and online communities. In relation to the influence of others, participants were either told about the potential to make money from the provision of these services by a friend, or knew somebody who was already in the business:

> *my friend told me that making stressers for companies that need to stress test their servers was very profitable so that is why i got involved.*

> *The original founder of the service I'm involved with was a close friend of mine, and about 3 years ago he started the service (he is no longer involved, he left in early 2012), and at the time I was beginning my interest in web development and at that time, most of the services offered same functionality and design and I helped him create an eye-catching product.*

Participants also reported using the services before being provided with an opportunity to become involved:

> *I became involved by looking at the stresser dashboard the owner was offering to positions and i felt like i would be a great moderator.*

and becoming exposed through online gaming forums:

> *I used to be on a minecraft forum and I was trying to make money.*

Two participants referred to learning new skills to be able to provide booter services, for example:

> *To gain extra knowledge on the subject for my networking class, as well as providing a service for people who would like to pentest there own network.*

Techniques of neutralisation

The one question that every respondent answered was "What are your primary motivations for offering stresser services?" Here, the majority of participants provided responses that attempted to neutralise or excuse their behaviour, perhaps reflecting their reasons for participating in the research. The primary motivation, as claimed by eight participants, was the provision of services for the purpose of network testing. Here, participants appealed to higher loyalties, by claiming that they provided services that were for the common good, namely that their actions provided more secure systems overall:

> *Our primary Motive is to provide service to those who want to check there network security and we have many clients who bought this service to have a good and secure network !*

Definitions favourable to offending, and uses of techniques of neutralisation were explored when asking about perceptions of legality. First, participants were asked if they thought provision of their services should be against the law, and whether it was against the law in their location. Only one participant believed that providing these services should be against the law. When asked about whether stress tests against specific targets, namely game servers, TeamSpeak (intra-team communication) servers, and against individual Internet users or organisations, should be against the law, only two participants believed that stress tests against all three targets should be illegal, while some other participants believed that it should be legal to conduct stress targets against some targets, but not others. Responses are shown in Table 1.

[insert Table 1 here]

Five participants believed that providing these services was not against the law in their location. When asked about whether the use of these services against different

targets two respondents believed that all three examples provided were illegal in their jurisdiction.

[insert Table 2 here]

Eight participants answered the question about how appropriate it was to provide these services to anyone who wished to buy them, on a scale from totally inappropriate to totally appropriate. One participant answered that it was totally inappropriate (a score of one), five answered totally appropriate (score of 10), and the average score was 7.75 (*SD* = 3.66). When asked about how appropriate providing stresser tests for use against the various targets were, participants on average viewed these as being less appropriate when compared to the provision of stresser services in general. While one participant believed that it was 'absolutely appropriate' to provide these services for use against all three targets, another three participants believed that it was 'absolutely inappropriate' to do so. These results are shown in Table 3.

[insert Table 3 here]

Nine participants advised how they came to their views about the legality and appropriateness of providing these services in general. Three participants spoke about how there was a legitimate need for stress testing, and as such it should not be illegal to provide these services, for example:

> *If you'd like further explanation, because it can assist a lot of data centers, server owners small and large prepare for an actual threatening attack that can cripple their networks for long periods of time resulting in financial loss, if they are prepared before an actual attack strikes, less damage will be done.*

One participant denied responsibility for how the services offered were used. It was claimed that it was how the services were applied that should determine the legality, however it should be the end user that is responsible:

Because, there are people who legitimately need to test the stress of there servers, its just the way that you use these tools that make them malicious or illegal.

Another participant denied injury, advised that he was acting within the bounds of the law as he would provide logs to law enforcement upon request:

My stresser keeps logs like almost every other stresser. If someone breaks the law and the police come to me I have the logs for them, nothing to hide. I've seen this happen to other booter owners I know.

One participant used the technique of condemning the condemners, saying that in comparison to other online content, it was not so bad:

Freedom of the human rights and before you ban stressers ban pornography and other disgusting forms of videos

One participant had a range of arguments about his perceptions of the legalities of providing these services, which largely denied responsibility. His arguments were that only large corporations cared about it, that hosting companies should start taking responsibility and protect their clients against attacks, that the responsibility falls upon the user of the service, not the provider, and that the site's terms and conditions protect the provider (this last point was also made by another participant):

No... it happens so much every day that only large corporations ever even make claims against those commiting these acts (mostly due to having excess money they can just throw around). I strongly believe that this issue is not going away anytime soon. Personally, I would produce more than 5 Gbps of bandwidth from my home connection, now sure, I actually know what I'm doing, but this just goes to show it is a serious problem. Hosting companies need to start taking responsibility for their otherwise unknowning clients and

help protect them from these threats. This is techically incorrect... the way the law is writen, the responsibility fall on the end user. Yes, it is close, but our Terms and Conditions have been reviewed by our attorney to be legally sound.

When asked if they had any other remarks about how proper, wrong or illegal the provision of these services are, or should be, seven participants provided their views. One respondent stated that all attacks on a network that are not owned by the attacker should be illegal, and therefore it didn't matter what the server was used for:

All Attacks to a outbound network that is not owned by you should be illegal so splitting up what networks can and cant be stressed thats dumb.

Another participant agreed that it was wrong to use stresser services against the examples provided, namely game servers, TeamSpeak servers and individual Internet users or organisations. He advised that he had been receiving abuse reports, and was now advising users that they should not be testing networks without permission:

I think it's wrong and at the beginning of this project when my friend and I ran it, we frankly did not have any indiciation we didn't permit this but as time progressed, I've written in places that it should only be used in a testing environment where you're test loading your network and preparing for an actual attack, ensuring you have explicit permission from device and facility owners. We've handled a lot of reports within the past 6 months regarding this and we do our best to handle the abuse.

Another participant claimed that it was not up to the provider of the service to determine whether the users are acting illegally:

I'm saying I don't know on the last three against the law because there are obviously certain servers that they could illegally test and certain servers that

they could test legally. It's not for me to decide whether they are attacking something illegally, there isn't a way I can.

Rational choice theory

Financial gain was reported as a reason for operating booter sites by six participants. Two participants referred to earning between US$300 to US$500, and US$200 to US$300, per day. Another described it as 'easy money':

Mainly financial purposes, its easy money. When I first started doing stresser services though it was just for the kick of making a good stresser and all profits from the stresser would go back into more attack servers, at this point though I don't care about that and just want easy money.

Financial gain was not the only benefit of providing booter services, with another participant advising that he also benefited from feelings of excitement:

Well lets be real, My primary motivations is money. We offer these services to people who are willing to pay large sums of money to keep targets offline and kids who want to feel like they are hackers. We do try market these services towards a more legitimate user base but we know where the money comes from. For a network nerd such as myself seeing what stressers can do to networks in real time is a very exciting and fun thing to do and I actually get excited when I find out that someone is using the service for that rather than to be a thorn in the side of the internet.

Ten participants answered what percentage of their income is provided by their services, in an average month. The responses were fairly evenly distributed. Three participants reported that zero to 10 percent of their income is provided by these services, while two participants received between 91 to 100 percent of their income

this way. The remaining respondents reported 21 to 30 percent (n = 1), 31 to 40 percent (n = 1), 61 to 70 percent (n = 2) and 81 to 90 percent (n = 1).

Participants were asked, in an average month, how many 'stress tests' (i.e. DDoS attacks) were performed, the number of cumulative seconds tests are performed for, and the number of individual accounts that request tests. There was a large amount of variability, particularly as one participant reported very few tests, which was consistent with other responses this participant had provided. Responses to these questions for this participant were therefore removed, and the subsequent results are provided in Table 4. Here, the number of cumulative seconds tests are performed for has been recalculated as hours. Also included in Table 4 are calculations for the number of tests per account, and the number of seconds per test.

[insert Table 4 here]

The cost per subscription for up to one month was calculated for all 63 sites. The currency used was US dollars, as this was listed by the majority of the sites, and the conversion rate as of 24 September 2014 was used for the sites that used alternative currencies. One outlier was removed from the data, as it was 5.3 standard deviations above the mean. The cost was positively skewed, ranging from 0.19¢ to $14.99 per subscription, with a median cost of $4.00 per subscription ($n$ = 62, M = 4.57, SD = 3.40, 95% CI [3.71, 5.43]).

Income per month was estimated by using the 95% confidence intervals for the cost of subscriptions for the sites ($3.71 to $5.43 per account), multiplied by the number of accounts per month reported by the participants. One outlier was identified and removed, as it was 2.3 standard deviations above the mean. The median values for the remaining six participants who reported the number of individual accounts that requested stress tests were used. With the outlier removed, the median number of

accounts per month was 1,000 (n = 6, M = 1,047.2, SD = 686.2). It is estimated that, in an average month, the sites earned between $3,705.25 and $5,430.67. This is a conservative estimate, using the lowest tier of pricing offered by the booter sites.

In relation to costs, participants were asked how many hours they spent maintaining the website in an average month. Ten participants responded to this question, with responses ranging from one to 400 hours per month (M = 112.30, SD = 130.51). The most disruption reported by participants in the operation of their services was in relation to payment methods, with seven participants advising that these had changed over time. Of these, six had trouble accepting payments through PayPal, the preferred payment method. For example:

> *Paypal is always closing us down for running stressers, it's really a problem as that is our main way to get paid.*

One participant advised that he changed his PayPal email every week in order to continue to receive payments:

> *Change paypal email every week, tried other processors, did not work at all.*

Another participant advised that his payment methods had changed when Liberty Reserve had been shut down, and that he had recently begun accepting credit cards and digital currencies:

> *We've been accepting PayPal since the beginning, we used to accept Liberty Reserve which was a popular payment processor until it was shutdown, and most recently we've began accepting a lot of crypto currency payments (Bitcoin, Litecoin) and as well as credit card payments.*

About the customer-facing site

Participants were asked what methods were used for the stress tests. Ten participants responded to this question, reporting between three and 11 methods in use (M = 5.60,

SD = 2.32). The most commonly used methods included DNS reflection (*n* = 8), SYN flood (*n* = 6), HTTP GET/HEAD/POST flood (*n* = 7), R.U.D.Y (slow HTTP form submission) (*n* = 7), and Slowloris (slow HTTP interaction) (*n* = 8). When asked about why their methods had changed over time, the main themes related to efficiency, displacement, popularity, and ease of use. Two participants referred to efficiency, including the power of different methods, and use of resources compared to damage caused. For example:

> *Chargen is the most efficient amplification method, dns reflection hits about the same as chargen but it uses up the servers whole port (we use 100mbit servers) chargen will hit the same while only sending about 1/6 of the servers capacity. when also have udp syn ssyn essyn hulk rudy arme slowloris get head post (we use chargen for udp because it's much more efficient), I have taken out all layer 7 attacks because they use so many resources and no-one really uses them.*

Four participants also described how they displaced from one method to another. Displacement occurred when reflection servers were updated and patched. The following example also refers to the use of CloudFlare as a reason for changing methods:

> *The methods have been changed as increase in protection. At first, we use L7 methoods for website but after apache updates and cloudflare service, we moved on to DNS/NTP reflection,*

Two participants referred to the popularity of the methods being taken up, with one saying that some methods had been requested by users. The other stated that:

> *Since the start, there's been many different amplification/reflection such as earlier this year when using NTP servers as an amplification method became*

extremely popular. As of right now we do offer the most recent methods of DDoS (except SNMP amplification) for the service.

Finally, one participant included ease of use as a reason for using a particular method:

they have become more advanced, powerful, able to cause more damage, and easier to use and implement.

The participants were asked how their customer-facing site was set up, for example, if they used existing source code, or wrote their own code with or without the assistance of others. Eight participants responded to this question, with three advising that they had written the code by themselves. Another advised that he had written the code by himself, but had previously used code by an unknown author. One participant advised that while he coded the website on his own, he used ragebooter source code (which was stolen in 2012 and made publicly available) as an example:

I'm a PHP Developer so I have coded it on my own. I did use rage booter source code as a sample to see how things work out.

Two participants had written the code in collaboration with someone else. One had previously used, and the other raised security concerns about, open source:

i partnered up with my buddy who owns a booter and ended up living 10 minutes away from me. We both had our own stressers at the time and ended up meeting up one day. I was using open source until i started working with him.

We coded our own source code from scratch with a limited number of developers... this helps avoid security flaws that are common with open source projects.

The remaining participant advised that he had paid US$40 for someone to write the code for him:

Some kid from the UK coded me a source for $40, although it was a pretty sloppy job and mainly re themed vDos / ragebooter it got the job done, all you really need is a nice-looking theme and kids will be buying like mad.

Nine participants responded to the question about how the service was set up, with six advising that they had done the coding themselves. Another advised that the code was written predominantly by a friend of his:

i actually got pretty lucky and met one of the biggest booter owns and became good friends with him and didn't have to write much of my own.

One participant paid someone to build the customer-facing websites and to automate the provisioning of the DDoS attacks themselves (using scripting languages to invoke commands):

At first, we used API on rent. After learning all stuff how it's operated, we made our own setup. We paid someone to setup our servers and scripts.

Another had 'in house engineers' who wrote the code for the services:

Our service runs off of dedicated servers running our custom coded scripts... they are all setup with our in house engineers

Ten participants responded to the question about where they advertised these services. Two participants mentioned online forums, and a further three specifically mentioned the website hackforums.net. Two participants advised that they received enough business through word of mouth. Two participants advertised on YouTube, and one also on Twitter. One participant used affiliate marketing. Two participants advised that they did not advertise at all, with one stating that:

We do not advertise at this time, we believe that if someone is looking for our service, they will find it

Ten participants answered the question about how the majority of visitors landed on their site. The most common response option selected was search engines (n = 4). Two participants selected 'visiting the URL directly', while a further two did not know. Two selected 'other', with one stating:

> *How the fuck did you get to it? I don't even advertise it anywhere and have no idea how you even found it*

Three participants ran the site on their own, with no others, four ran the site with one other person, and three with two or more other people. Three participants declined to answer this question.

Participants were asked to estimate the percentage breakdown of tests performed against game servers, TeamSpeak servers, individual Internet users or organisations, and other targets. The response options were limited so that the total had to equal 100. Six participants responded to this question. On average, it was estimated that most of the services targeted individual Internet users or organisations (M = 40.17, SD = 36.79, range = 1-95). This was closely followed by game servers, which received, on average, an estimated 37.0 percent of stress tests (SD = 35.27, range = 5-97). Targets categorised as 'other' received an average of 23.5 percent of stress tests (SD = 38.18, range = 0-100), followed by TeamSpeak servers, which on average received 16.0 percent of stress tests (SD = 19.95, range 0-50).

Discussion and conclusion

Many cybercrimes are not unique, in that they reflect crimes that previously took place in physical space. However, it is the environment, or the "bottle", to borrow Grabosky's (2001) analogy, in which offenders operate that makes these types of offences distinctive. For example, an individual cannot necessarily engage in offending that requires a high level of technical knowledge without first obtaining that

requisite knowledge. The provision of booter services is one such example of a niche, high tech, crime type. However, it is not just the technical knowledge that is required, but information about the market for DDoS attacks, and how to monetise this.

With an interest in computers, technology or gaming, would-be-offenders begin by communicating online, during which they learn the techniques to commit cybercrime as well as share the definitions favourable towards offending and techniques of neutralisation. It is through associating with others, and communicating on online communities, that offenders learn about booter services. All of the booter service providers are young and male. Age and gender corresponds with the demographics found on the online communities where differential association takes place.

Offending is gradual, from using booter services, to providing services themselves, and sometimes escalating to other types of online offending behaviour. Offenders also indicate that they have internalised the techniques of neutralisation. Participants neutralise their actions by appealing to higher loyalties, claiming that they are providing an important service for network testing. The most commonly used technique is denial of responsibility. While this was the least used neutralisation technique found in Turgeman-Goldschmidt's (2009) or Hutchings' (2013b) earlier research, it reflects the type of behaviour that the offender is engaged in.

We found a comparable number of booter services as those found by Santanna and Sperotto (2014), supporting our claim that our survey captured the entire known population of offenders offering booter services. The income and operational model that we found was consistent with Karami and McCoy's description (2013a). The most commonly reported way to advertise booter services is through the online

communities where skills are learnt and definitions favourable towards offending are shared.

The provision of booter services is maintained by the 'easy money', with little cost in terms of time spent maintaining the sites. While the estimated income arising from this study is lower than that found by Karami and McCoy (2013a), we took a conservative approach in our calculations. Also, the one booter service that informed Karami and McCoy (2013a) research may not be typical of booter services in general, as it had been targeted and the data subsequently leaked. The most frustration that is faced by participants is in relation to receiving this easy money, as PayPal frequently disrupts the receipt of their payments. On the other hand, one company that claims to prevent denial of service attacks actually helps facilitate them, with many of the sites using CloudFlare to protect themselves against denial of service attacks, presumably by competitors. Participants do not indicate at all that they are concerned about law enforcement taking action against them, with many believing that their actions are not criminal. Participants try to minimise the harm of their activities, such as claiming that they offer the services for stress testing. However, it is clear from the other responses provided that their services are primarily used for attacks against systems not owned by the users, and the services are not advertised for network testing.

We wanted to understand how best to run surveys for future work with similar offenders and we found that the option to participate in an online survey attracted a much higher response rate. However, the interviews resulted in more complete data, and allowed the interviewer to explore particular areas in more depth. It is believed that the survey may have been more convenient for participants, as it could be completed immediately, rather than making a time to participate in an interview. Our response rate was 25%, although since some respondents were running multiple

systems it may have been even more than this. It was much higher than we had anticipated, which we attribute to the nature of the behaviour being researched and the limited amount of law enforcement activity against booter service provision.

This work has attempted to overcome some of the significant challenges found in this area of research. However, a number of limitations remain. First, despite attempting to contact the entire known population of active booter services, the small sample size makes it difficult to explore relationships within the data. Also, despite the high response rate (for an active offender population), there may be a self-selection bias, in that those that chose to participate may differ from those that declined.

There are also concerns that some respondents participated in the research so as to use it as a platform for excusing their behaviours. Therefore, the neutralisations that are presented may instead be defences against their actions. Another limitation is in determining the time-order sequence. This limitation applies to many prior studies examining the theorised causal explanations of crime. It is acknowledged that the best way to test the causal ordering is a longitudinal design; however this was not feasible for the current study.

Acknowledgements

The work would not have been possible without the invaluable assistance of Ross Anderson. It was supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131]. The opinions, findings, and

conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

References

Akers, Ronald L. and Christine S. Sellers. 2004. *Criminological Theories: Introduction, Evaluation and Application*. Los Angeles: Roxbury Publishing Company.

BBC News. 2010. "Call of Duty Cyber Attack Prompts Arrest of Boy, 17." Retrieved July 1, 2015 (http://www.bbc.co.uk/news/uk-england-manchester-11961333).

Bennett, Trevor and Richard Wright. 1984. *Burglars on Burglary*. Aldershot: Gower Publishing Company.

Chamberlin, Thomas and Kathleen Donaghey. 2014. "Mother of Accused Denies Hack Attack on Riot Games and Theft of Player Information." Retrieved July 1, 2015 (http://www.theaustralian.com.au/news/mother-of-accused-denies-hack-attack-on-riot-games-and-theft-of-player-information/story-e6frg6n6-1226860625835).

Clarke, Ronald V. and Derek B. Cornish. 1985. "Modeling Offenders' Decisions: A Framework for Research and Policy." *Crime and Justice* 6:147-85.

Clarke, Ronald V. 1997. "Introduction." Pp. 1-43 in *Situational Crime Prevention: Successful Case Studies*, edited by Ronald V. Clarke. Monsey: Criminal Justice Press.

CloudFlare. 2014. "Cloudflare Advanced Ddos Protection." Retrieved July 1, 2015 (https://www.cloudflare.com/ddos).

Cornish, Derek B. and Ronald V. Clarke. 1987. "Understanding Crime Displacement: An Application of Rational Choice Theory." *Criminology* 25:933-47.

Grabosky, Peter. 2005. "The Global Cyber-Crime Problem: The Socio-Economic Impact." Pp. 29-56 in *Cyber-Crime: The Challenge in Asia*, edited by Roderic Broadhurst and Peter Grabosky. Aberdeen: Hong Kong University Press.

———. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social Legal Studies* 10:243-49.

Hardy, Keiran. 2010. "Operation Titstorm: Hactivism or Cyber-Terrorism?" *UNSW Law Journal* 33:474-502.

Hollinger, Richard C. 1993. "Crime by Computer: Correlates of Software Piracy and Unauthorised Account Access." *Security Journal* 4:2-12.

Holt, Thomas J., Adam M. Bossler and David C. May. 2012. "Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance." *American Journal of Criminal Justice* 37:378-95.

Holt, Thomas J. and Adam M. Bossler. 2014. "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behavior* 35:20-40.

Holt, Thomas J. 2007. "Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures." *Deviant Behavior* 28:171-98.

Hutchings, Alice. 2013a. *Theory and Crime: Does It Compute?* Doctoral dissertation. Griffith University, Brisbane.

———. 2013b. "Hacking and Fraud: Qualitative Analysis of Online Offending and Victimization." Pp. 93-114 in *Global Criminology: Crime and Victimization in the Globalized Era*, edited by K. Jaishankar and Natti Ronel. Boca Raton: CRC Press.

———. 2014. "Crime from the Keyboard: Organised Cybercrime, Co-Offending, Initiation and Knowledge Transmission." *Crime, Law & Social Change* 62:1-20.

Hutchings, Alice and Thomas J. Holt. 2015. "A Crime Script Analysis of the Online Stolen Data Market." *British Journal of Criminology* 55:596-614.

Jordan, Tim and Paul Taylor. 1998. "A Sociology of Hackers." *The Sociological Review* 46:757-80.

Karami, Mohammad and Damon McCoy. 2013a. "Understanding the Emerging Threat of DDoS-as-a-Service." Proceedings of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats.

———. 2013b. "Rent to Pwn: Analyzing Commodity Booter DDoS Services."*;login* 38:20-23.

Levin, Rachel, Jonathan Richardson, Gary Warner and Kent Kerley. 2012. "Explaining Cybercrime through the Lens of Differential Association Theory, Hadidi44-2. Php Paypal Case Study." Proceedings of the IEEE eCrime Researchers Summit (eCrime).

McQuade, Samuel C. 2006. *Understanding and Managing Cybercrime*. Boston: Pearson Education, Inc.

Menn, Joseph. 2010. *Fatal System Error*. New York: PublicAffairs.

Santanna, José Jair and Anna Sperotto. 2014. "Characterizing and Mitigating the Ddos-as-a-Service Phenomenon." Proceedings of the 8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security.

Skinner, William F. and Anne M. Fream. 1997. "A Social Learning Theory Analysis of Computer Crime among College Students." *Journal of Research in Crime and Delinquency* 34:495-518.

Smith, Russell G., Peter Grabosky and Gregor Urbas. 2004. *Cyber Criminals on Trial*. Cambridge: Cambridge University Press.

Sutherland, Edwin H. 1949. *White Collar Crime: The Uncut Version*. New Haven: Yale University Press.

Sutherland, Edwin H., Donald R. Cressey and David F. Luckenbill. 1992. *Principles of Criminology*. Lanham: General Hall.

Sykes, Gresham M. and David Matza. 1957. "Techniques of Neutralization: A Theory of Delinquency." *American Sociological Review* 22:664-70.

Turgeman-Goldschmidt, Orly. 2009. "The Rhetoric of Hackers' Neutralisations." Pp. 317-335 in *Crimes of the Internet*, edited by Frank Schmalleger and Michael Pittaro. New Jersey: Pearson Education, Inc.

Verton, Dan. 2002. *The Hacker Diaries*. New York: McGraw-Hill, Inc.

Vold, George B., Thomas J. Bernard and Jeffrey B. Snipes. 2002. *Theoretical Criminology*. New York: Oxford University Press, Inc.

Walkley, Sascha. 2005. *Regulating Cyberspace: An Approach to Studying Criminal Behaviour on the Internet*. Doctoral dissertation. Australian National University: Canberra.

Wright, Richard T. and Scott Decker. 1994. *Burglars on the Job: Streetlife and Residential Break-Ins*. Boston: Northeastern University Press.

Yar, Majid. 2005. "Computer Hacking: Just Another Case of Juvenile Delinquency?" *The Howard Journal* 44:387-99.

Table 1: Beliefs About Whether Tests Against Different Targets Should be Illegal

Should the following be against the law?	Yes	No
Provision of stresser services in general (n = 10)	1 (10.0%)	9 (90.0%)
Stresser tests against game servers (n = 8)	3 (37.5%)	5 (62.5%)
Stresser tests against TeamSpeak servers (n = 8)	4 (50.0%)	4 (50.0%)
Stresser tests against individual Internet users or organisations (n = 8)	4 (50.0%)	4 (50.0%)

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 organisations (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 organisations (n = 8)	4.88	4.45	1-10

Table 4: Stresser Tests in an Average Month

For an average month	M	SD	Range
Number of stresser tests performed (n = 8)	171,713.63	269,581.41	200-754,768
Number of cumulative hours stresser tests are performed for (n = 7)	1,590.20	2,915.77	0.8-7,790
Number of individual accounts requesting stresser tests (n = 7)	5,018.57	10,526.00	20-28,847
Number of tests per account (n = 7)	90.56	173.91	10-483
Number of seconds per test (n = 7)	229.64	406.38	0-1,000