THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 14 | Number 2 Article 2

6-30-2019

Examining the Correlates of Failed DRDoS Attacks

Thomas Hyslip
Norwich University, thyslip@norwich.edu

Thomas Holt
Michigan State University, holtt@msu.edu

Examining the Correlates of Failed DRDoS Attacks

Thomas S. Hyslip
Norwich University
Northfield, VT
thyslip@norwich.edu

Thomas J. Holt
School of Criminal Justice
Michigan State University
East Lansing, MI
Holtt@msu.edu

ABSTRACT

Over the last decade, there has been a rise in cybercrime services offered on a fee-for-service basis, enabling individuals to direct attacks against various targets. One of the recent services offered involves stresser or booter operators, which offer distributed reflected denial of service (DRDoS) attacks on an hourly or subscription basis. These attacks involve the use of malicious traffic reflected off of webservers to increase the volume of traffic, which is directed toward websites and servers rendering them unusable. Researchers have examined DRDoS attacks using real-time data, though few have considered the experience of their customers and the factors associated with the likelihood of successful attack outcomes. This study examines this issue using a binary logistic regression analysis of survey responses from a population of stresser clients. The implications of this study for our understanding of the social factors underlying cyberattacks is discussed in depth.

Keywords: DRDoS, cybercrime, booter operators, malicious traffic, logistic regression

1. INTRODUCTION

Over the last decade, the landscape of cybercrime has changed as a result of the establishment of tools that enable attacks to be performed on a fee-for-service basis. There are myriad studies demonstrating the range of services available in underground cybercrime markets, ranging from spam email distribution to malicious software to personal information and credit card data (Dhanjani & Rios, 2008; Franklin, Paxson, Perrig, & Savage, 2007; Herley & Florencio, 2010; Holt, 2013; Holt & Lampke, 2010; Holz, Engelberth, & Freling, 2009; Honeynet Research Alliance, 2003; Motoyama, McCoy, Levchenko, Savage, & Voelker, 2011; Thomas & Martin, 2006). Service providers readily earn millions of dollars selling attack tools or personal information due to the demand from interested parties looking to quickly and efficiently target individuals and corporations alike (Franklin et al., 2007; Holt, Smirnova, & Chua, 2016; Holz et al., 2009; Moore, Clayton, & Anderson, 2009).

Research on cybercrime services demonstrates that they are largely driven by social relationships between buyers and sellers,

whether they operate in forums (Holt, 2013; Holt & Lampke, 2010; Holt et al., 2016; Motoyama et al., 2011; Yip, Webber & Shadbolt, 2013), IRC (Franklin et al., 2006; Honeynet Research Alliance, 2003; Holz et al., 2009), or on sites hosted on Tor, or the Dark Web (Li & Chen, 2014; Smirnova & Holt, 2017). Specifically, buyers frequently post reviews of their experience with a vendor, with an emphasis on the quality of products relative to their costs, and the speed with which vendors respond to queries (e.g., Holt, 2013; Holt & Lampke, 2010; Hutchings & Holt, 2015). The tone of feedback has a strong influence on the perceived reputation of vendors, with negative feedback minimizing their ability to sell within a given market (Franklin et al., 2007; Herley & Florencio, 2010; Holt & Lampke, 2010; Motoyama et al., 2011). In fact, some forums offer product testers who actively evaluate the claims of vendors' tools or data and post their reviews to help legitimize quality vendors and marginalize those offering poor quality goods (Holt et al., 2016).

The need to purchase functional data and effective services are somewhat obvious: buyers seek the greatest value and return on their initial investment (e.g., Smirnova & Holt, 2017). This is particularly critical when considering stolen financial information or malicious software that acquires sensitive data or provides backdoor remote access to victim machines. In the event the data or service does not work, the buyer will have minimal recourse to recoup their losses. Other forms of cybercrime-as-service attacks may not be as dependent upon this dynamic, particularly if the only goal of the attack is to shut down access to a resource. This is frequently the case with so-called "stresser" or "booter" services that offer distributed reflective denial of service (DRDoS) attacks for a fee (Hutchings & Clayton, 2016; Karimi & McCoy, 2013; Rossow & Gurtz, 2014; Santanna, Rijswijk-Deij, Hofstede, & Sperotto, 2015).

These attacks enable service providers to perform high- volume Distributed Denial of Service attacks against web-based targets with minimal resources, while simultaneously hiding the origin of the attacks. During an attack, the target is flooded with more requests than can be completed in millisecond intervals by using vulnerable servers and devices such as home routers to reflect and amplify the volume of requests during the attacks. Since the target cannot respond to the attack requests, legitimate users are also unable to utilize the resource as well. DRDoS attacks can cost companies millions of dollars in lost revenue and may embarrass the victim as well due to perceptions over their inability to stop the attack (e.g., Arbor Networks, 2015).

The fee-for-service model of booters and stressers primarily operate on a subscription basis, where customers pay for weeks or months of service during which they can launch attacks at will (Arbor Networks 2016; Hutchings & Clayton, 2016; Karimi, Park, & McCoy, 2015; Rossow & Gortz, 2014; Santanna et al., 2015). Customers are also given options as to the type of attack that will be performed on the basis of specific Internet protocol vulnerabilities that can be used to send requests. Though the attack type may vary, the primary outcome of the attack is the same: keeping others from using a web server or on-line resource. As a consequence, booter clients may not be interested in the accuracy with which an attack takes place, but whether the service is made unavailable.

Though research examining booters and stressers has increased (Hutchings & Clayton 2016; Karimi & McCoy, 2013; Karimi et al., 2015; Rossow & Gortz, 2014; Santanna et al., 2015), few have considered whether their customers were satisfied with the service or achieved their specified goals. Evidence suggests that the majority of DRDoS services are functional, with only a small proportion either failing or utilizing a different attack method than what was initially ordered (Karimi et al., 2015; Santanna et al., 2015). Thus, this exploratory analysis attempted to identify the foreground and situational dynamics associated

with customers' perceptions of failed attacks performed by booter and stresser service providers. Using survey data collected from individuals who appeared to have purchased DRDoS service subscriptions, the findings demonstrate that the practices of vendors have a greater impact on the likelihood of failure than those of the customer. The results reinforce the broader literature on cybercrime as a service, and the implications of this study for our understanding of cybercrimiality are considered in detail.

2. PRIOR RESEARCH ON STRESSORS AND BOOTERS

The operation of booter and stresser services are somewhat different from existing DDoS attacks commonly associated with either botnet malware (Karimi & McCoy, 2013; Karimi et al., 2015; Santanna et al., 2015) or stand-alone tools such as the Low Orbit Ion Cannon associated with Anonymous (Mansfield-Devine, 2011). Both DRDoS and DDoS attacks utilize thousands of connection requests to a targeted server, launched from multiple IP addresses every second. Stresser services, however, do not launch attacks from infected computers as with botnets. Instead, they utilize powerful backend servers to "reflect" or amplify the quantity of traffic to the targeted system through the use of malformed packets with spoofed IP addresses (US CERT, 2014).

These backend servers are not controlled by attackers but are part of existing Internet service providers' infrastructure that can be vulnerable to this form of attack. Certain network protocols can be hijacked by attackers as a means to send attack traffic. In fact, fifteen different network protocols have been used to reflect and amplify attacks, most of which are extremely common and used by major websites (Rossow & Gortz, 2014; US CERT, 2014). The various protocols available work to an attacker's advantage, as stressor operators changed their attack methods in progress if they are unsuccessful due to vendors and website operators patching known security flaws (Hutchings & Clayton, 2016).

The flexibility afforded to stresser operators in terms of attack protocols would suggest they have a high likelihood of general success knocking targets off-line. This is supported by recent research analyzing actual attack traffic against live targets (Karimi & McCoy, 2013; Santanna et al., 2015). At the same time, the information customers need to determine what booter and stresser operator to work with may not be readily available as service providers typically advertise their services via personal websites (Hutchings & Anderson, 2016). Unlike with forums and other interactive cybercrime markets, individual websites allow operators to control the number of negative reviews or critical comments over their services that can be viewed (Hutchings & Anderson, 2016; Smirnova & Holt, 2017). These conditions may constrain buyer decision-making and lead certain factors associated with both the vendor and the prospective buyer to be a strong determinant in whether an attack fails or succeeds.

To that end, certain characteristics of the stresser or booter service provider may have some association to an attack failure. For instance, some stresser operators offer free attacks using a small number of common attack protocols as a means for clients to validate the seller's claims (Hutchings & Clayton, 2016). The same process has been noted in stolen data markets operating in forums and on-line spaces, though individuals who offer free data may be more likely to cheat their customers and provide no data after receiving payment from the customer (Herley & Florencio, 2010; Holt et al., 2016). All stressers do not offer free tests, suggesting that the availability of testing services may be associated with a more reliable stresser operator.

In much the same way, some stresser operators allow their customers to test their service at no cost for a set period of minutes to validate their claims. Tests of data or services

in traditional cybercrime-as-service markets appear to be a way to establish a vendor's reliability and may be associated with higher prices for data (Holt, Smirnova & Chua, 2013). In the event a vendor does not offer a test, the customer takes a risk that the vendor has exaggerated their claims. As a result, an absence of testing services may be more likely to increase the risk of attack failure.

The ability to communicate with the vendor should also influence success as research demonstrates a strong connection between vendor communications and their overall reputation in cybercrime-as-service markets generally (Holt, 2013; Holt & Lampke, 2010; Yip et al., 2013). Those who are difficult to contact or are slow to respond may be more likely to be rip-off artists or simply unconcerned about the potential for customer feedback to influence their market position. Booter and stresser operators may be more open to contact with their clients due to the potential for attacks to be launched in different ways to achieve the same attack objective: elimination of a resource (Hutchings & Clayton, 2016). If an attack is successful on its initial launch, the customer has no need to contact the vendor. Thus, attempts to contact stresser operators may be a predictor of failure as the attack may not have worked as advertised.

A potential customer's knowledge of booters and stressers may have a mixed relationship to the likelihood of a stresser attack's success. Individuals with a greater comprehension of the technical aspects of a certain form of attack and a service may be better able to recognize accurate descriptions of attacks posted by vendors. At the same time, the availability of tests and free attacks renders the need for deep technical knowledge moot as customers can shop across vendors until they find a provider that works (Franklin et al., 2007; Holt & Lampke, 2010). Thus, knowledge may have a limited relationship to attack failure.

The target a customer has identified for an attack may also have a relationship to the likelihood of success. Larger organizations and government resources may be resilient against web-based DRDoS attacks because of their use of cloud-based security infrastructure to offload malicious traffic has decreased the utility of some forms of DDoS attacks (Graham-Cumming, 2014). In recent years, DRDoS services have also been employed against on-line gaming servers as a way to target competing players and knock them off-line during play (Hutchings & Clayton, 2016; Karami & McCoy, 2013). These targets may be more easily affected, as could individually be owned or operated web servers because of variations in their infrastructure and security configurations.

The motivation of an attacker may also have some relationship to the success of an attack. DDoS attacks have value as an expressive attack tool, as they may be used for either economic gain, ideological agendas, or simply revenge against an opponent or enemy (Rossow & Gortz, 2014). Individuals seeking to profit from an attack may be less dependent on a successful attack and simply on the threat of an attack taking place in order to profit (Ianelli & Hackworth, 2005; Segura & Lahuerta, 2010). Individuals seeking to express an ideological belief may be more reliant on an attack's success in order to communicate their opinion (Denning, 2011; Woo et al., 2004). At the same time, they may be interested in targeting resources that have more robust infrastructure and security tools to withstand an attack of all but the largest magnitude (Graham-Cumming, 2014). These attack types may be more likely to fail depending on the nature of the attack. Individuals seeking revenge may be more likely to target game servers or peers, thereby making them more likely to succeed.

These hypotheses are based on assumptions about the nature of attackers and booter/stresser operators, though the research to-date is limited. As a result, there is a need for empirical inquiry to address this gap in our knowledge about the nature of cybercrime-as-service operations. This study attempted to

examine these issues using a unique convenience sample of booter and stresser clientele.

3. DATA AND METHODS

A unique sampling methodology was employed to develop a sample of stresser clients for this analysis. While prior studies either hired booter services to examine attack traffic (e.g. Karimi & McCoy, 2013; Santanna et al., 2015) or contacted vendors to conduct interviews (Hutchings & Clayton, 2016), such strategies do not provide insights from their customers. We researchers identified a cracked database of stresser customers that was posted online, containing 51,909 unique email addresses. This provided a robust sample of individuals who were at least interested in learning more about stressers, or may have used that specific service provider.

These email addresses were sent a message inviting the recipient to participate in an anonymous online survey to understand stresser service operations between November 27 and 29, 2016. The email message informed the respondent that a research study was being conducted on stressers and booters, the survey was anonymous, and the information would only be used for research purposes. The first question of the survey was embedded in the email message and if the respondent answered the first question, they were directed to the remainder of the survey on the Survey Monkey webpage. The survey consisted of 22 multiple choice questions and one comment box for follow up requests. The questions related to the use of stresser and booters and included the respondent's skill level, type of payment used, attack protocols used, targets of attacks, motivation for usage, and demographics. A reminder message was sent on December 2, 2016, as a reminder to the complete the survey which closed on December 30, 2016.

Of the initial sample of messages sent, 5,226 emails were verified as received and opened. This is sensible given the fact that the database containing those emails had been posted publicly and may have included junk email addresses abandoned by users. Also, the researchers have no way to validate whether the addresses belonged to 59,000 individuals, or involved multiple accounts owned by a single person. Of those, 821 individuals completed the survey, and 218 remained due to listwise deletion. While this is a substantial drop-off in respondents, it is not outside of expectations for

Table 1: Descriptive Statistics (N= 201)

Variable	Mean	SD	Min	Max
Did stresser not work	.233	.424	0	1
Pay to use	.651	.477	0	1
Could you test	.915	.278	0	1
Contact Stresser	.323	.468	0	1
Knowledge	7.611	2.353	1	10
Target				
Self	.577	.495	0	1
Game	.502	.501	0	1
Business Server	.263	.441	0	1
Website or Server	.527	.500	0	1
Government Website	.164	.371	0	1
Other	.343	.475	0	1
Motive				
Research	.482	.500	0	1
System Testing	.592	.492	0	1
Affect Game or Opponent	.427	.496	0	1
Hacktivism	.228	.421	0	1
Affect Business Competitor	.114	.319	0	1
Test My Abilities	.457	.499	0	1

response rates in traditional on-line survey studies (Curtin, Presser, & Singer, 2005; Fan & Zan, 2010) and in a population of active offenders generally. Prior scholarship notes that individuals engaged in cybercrime are less likely to participate in research out of concern for their safety (e.g., Holt, 2007; Hutchings & Clayton, 2016; Pruitt, 2007). Though the small sample limits the generalizability of the data, the responses provide essential insights into an under-examined phenomenon using a convenient yet purposive set of respondents.

Dependent Variable

To understand the extent to which stresser services worked, respondents were

asked: "Did the Booter or Stresser work as advertised?" (0-no; 1-yes). Since the majority of respondents (75%) claimed the attack they used was functional, the item was reverse coded (1=no) to examine the factors associated with failed attacks (see Table 1 for descriptive statistics). This issue is of particular interest as a small proportion of research demonstrates booter attack methods may fail (Santanna et al., 2015). Therefore research is needed to understand the extent to which attacks appear successful to the customer, regardless of whether the attack traffic matched what was advertised.

Independent variables

Respondents were asked several questions regarding their experience with the use of a stressor or booter to identify any factors of the service may be associated with the likelihood of failure. The broader research on data markets and cybercrime as service markets demonstrates some association between certain vendor behaviors and greater levels of trust or reliability. These measures were included to understand the extent to which they may be associated with booter and stresser operations. Specifically, respondents were asked, "Did you pay a fee to use the booter or stresser" (0=no; 1=yes). This is included as stressers operate at no cost, and research on other forms of cybercrime as service that operate on a free basis may be less likely to be successful (Herley & Florencio, 2010). Participants were also asked "Were you able to use the stresser or booter to test systems?" to understand the relationship between product testing and functionality (0=no; 1=yes). Evidence suggests product testing in data markets may be associated with greater trust in the vendor (Holt et al., 2016), thus this variable was included to examine its ties to booter services. A measure was also included to understand whether a customer had to contact the vendor: "Did you ever need to contact the operator of the booter or stresser for questions or help?" (0=no; 1=yes). We hypothesize that vendor contact would be associated with an increased risk of attack failure as they may need to either 1) report the attack failed, or 2) seek an explanation as to why or how the attack did not succeed. Finally, a measure for customer knowledge was included as a 10 point scale (1=low; 10=high) to understand the extent to which more understanding of booter operations may be associated with failure.

Six measures were included to examine the extent to which the target of an RDDoS attack may be associated with failure. Specifically, respondents were asked: "What did you use the stresser/booter on?" with six response categories: 1) Yourself, 2) Game, 3) Business Server (non website, such as Email or File Server), 4) Private/commercial Website / Webserver, 5) Govt website or web server, and 6) Other. A binary response was used (0=no; 1=yes) to test the hypothesis that certain targets, such as commercial websites and government servers may be more resilient to attack rendering attacks more likely to fail.

Finally, a set of seven measures were included to examine the relationship between an actor's motivation for performing an attack and their likelihood of failure. Respondents were asked "What was the motivation behind use of the booter/stresser?" with seven responses: 1) research; 2) system testing; 3) affecting game/game opponent; 4) hacktivism (protest); 5) affect business competitor; 6) test my abilities; and 7) other. These motivations correspond to the broader reasons why actors may employ either booter or stresser services (Hutchings & Clayton, 2016), or those of the hacker community generally (Holt & Kilger, 2012). Each item was treated as a binary (0=no; 1=yes) and included to understand whether any motivation corresponded to the likelihood of a failed attack.

4. FINDINGS

To examine any relationship between vendor-specific conditions, attitudes of the individual customer, and failed attacks, a binary logistic regression analysis was conducted. Multicollinearity did not appear to bias the parameter estimates as the independent variables were not strongly correlated with one another. Additionally, the highest VIF was .508, while the lowest tolerance was 1.980 suggesting no issues with multicollinearity generally.

All variables were included simultaneously in a binary logistic regression model, which found that customers who were not able to test the stresser's services were more likely to report a failed attack, reinforcing the literature regarding stolen data and cybercrime as service market vendor reliability (see Table 2; Holt & Lampke, 2010; Holt et al., 2016). Additionally, customers who contacted the vendor were more likely to experience failure, supporting our hypothesis that individuals only make contact in the event of failure.

Table 2: Binary Logistic Regression Model (N= 201)

Variable	B	S.E.	Exp(B)
Pay to use	-.370	.471	.691
Could you test	.233	.661	.107**
Contact Stresser	1.271	.448	3.564**
Knowledge	-.079	.087	.924
Target			
Self	.044	.441	1.045
Game	-.059	.516	.943
Business Server	.105	.514	1.111
Website or Server	.458	.463	1.196
Government Website	-.438	.653	.645
Other	.179	.436	1.196
Motive			
Research	.530	.441	1.698
System Testing	-.071	.465	.931
Affect Game or Opponent	.424	.535	1.528
Hacktivism	-1.565	.596	.209**
Affect Business Competitor	.763	.698	2.145
Test My Abilities	-.254	.413	.755
Other	-.121	.538	.886
Constant	.812	.814	2.253
Pseudo R^2	.234		

p=.05*; p=.01**;-2LL = 184.774; $\chi 2(7) = 33.859$**

No significant relationships were observed between target type and attack failure, suggesting that the nature of a target has little influence on resilience or success. With respect to the motivational measures, only one significant relationship was present: hacktivism. The relationship was negative, meaning those who were not motivated by an ideological or activist-related agenda were more likely to report failure. This was unexpected as an ideologically motivated actor may be more likely to target a government or industry target (e.g. Jordan & Taylor, 2004), which may be more likely to withstand an attack.

5. DISCUSSION AND CONCLUSIONS

Criminological scholarship examining the market for personal data and services based around hacking and cybercrime tools has increased over the last decade (Franklin et al., 2007; Holt, 2013; Holt & Lampke, 2010; Motoyama et al., 2011). These studies demonstrate that human factors drive cybercriminality, particularly reviews of service providers on the basis of the quality of their products and services (Holt et al., 2016; Motoyama et al., 2011). Recent research has identified the emergence of a new form of fee-for-service attack vendors offering DRDoS attacks, offering paid denial of service attacks against websites and services that are difficult to mitigate (Karimi & McCoy, 2013; Karimi et al., 2015; Santanna et al., 2013). Given that research has found these attacks to be largely successful with functionality that corresponds to what customers may order, it is necessary to consider what factors may be associated with failed attacks. This study attempted to address this issue through an examination of customer experiences within a population of individuals who utilized stresser or booter services.

Using a unique survey of DRDoS customers, the findings demonstrate that failure appears to be associated with the stresser or booter operator rather than that of the client. Specifically, customers who used vendors that did not allow tests of their services in advance were more likely to experience failed attacks. These findings reflect evidence from prior research on illicit markets for data and malware as buyers who can validate a service provider's claims prior to making a purchase were more likely to provide positive reviews and experiences (Herley & Florencio, 2010; Holt, 2013; Holt et al., 2016).

Booter or Stresser customers who had to make contact with a stressor operator were also more likely to report failed attacks. This finding supports the hypothesis that contact between stresser providers may be a sign of failure, which may partially reinforce the literature on illicit data markets. Specifically, customers value the ability to contact vendors so as to ensure successful use of services or data (e.g., Holt, 2013; Holt & Lampke, 2010). Unlike the purchase of data or malware which may require customers to have a degree of technical knowledge, it is likely that DRDoS service customers may simply want to know why the attack did not work. This was reinforced by the fact that knowledge of booter services was non-significant in the model. As a result, the role of contact may be somewhat different compared to other forms of cybercrime-as-service.

Additionally, this study found only one association between customer target preferences, motivations, and the likelihood of attack failure. Those who were not motivated by hacktivism were more likely to fail, which is somewhat surprising given that hacktivists may be more inclined to target corporate or government infrastructure (e.g., Denning, 2010; Jordan & Taylor, 2004). Such resources would theoretically have greater cybersecurity support infrastructure at their disposal to mitigate DRDoS attacks (Graham-Cumming, 2014). However, the fact that no other motivation was significant in the model suggests a need for greater research to disentangle the relationship between motive, targeting, and successful attacks (see also Hutchings & Clayton, 2016).

Taken as a whole, this study suggests that booter and stresser operations share some common dynamics to other forms of cybercrime operating on a fee-for-service basis. Though DRDoS vendors advertise differently from stolen data and malware vendors (Hutchings & Clayton, 2016; Karami & McCoy, 2013; Karami et al., 2015) the likelihood that customers have successful experiences with service providers are driven by the same factors associated vendor behavior rather than that of the customer (Holt et al., 2016). These findings suggest the social factors of cybercrime must be given equal consideration to those of the technical aspects of attacks (Franklin et al., 2007; Holt & Bossler, 2016; Smirnova & Holt, 2017; Yip et al., 2013).

At the same time, the preliminary nature of this study and its limited generalizability demand further study to examine the customers' of booter and stresser services. Specifically, researchers could employ qualitative methods with known customers of service providers to more fully document how success is defined by clients (see also Hutchings & Clayton, 2016). In addition, further study is needed to better define the targets of booter attacks to understand the location, employee size, and other conditions that may affect the likelihood of success. Finally, research is needed to better document the extent of customers' technical proficiency so as to identify whether booters and stressers are servicing primarily unskilled actors or a more diverse population. Such insights would be essential to understand why and how DRDoS service providers continue to thrive, as well as the reasons why individuals may be more willing to pay for this infrastructure on a fee-basis as opposed to building their own for use at will. Such insights can greatly improve our understanding of the social dynamics that shape cybercrime and identify strategies to detect, mitigate, and defend against these threats.

REFERENCES

Arbor Networks. (2015, January). *Arbor Networks 10th Annual Worldwide Infrastructure Security Report Finds 50X Increase in DDoS Attack Size in Past Decade.* [Online] Available at: http://www.arbornetworks.com/arbor-networks-10th-annual-worldwide-infrastructure-security-report-finds-50x-increase-in-ddos-attack-size-in-past-decade

Curtin, R., Presser, S., & Singer, E. (2005). Changes in telephone survey non-response over the past quarter century. *Public Opinion Quarterly*, *69*, 87-98.

Denning, D. E. (2011). Cyber-conflict as an Emergent Social Problem. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 170-186). Hershey, PA: IGI-Global.

Dhanjani, N., & Rios, B. (2008). Bad sushi: Beating phishers at their own game. Presented at the Annual Blackhat Meetings, Las Vegas, Nevada.

Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior, 26,* 132-139.

Franklin, J., Paxson, V., Perrig, A. & Savage, S. (2007). An inquiry into the nature and causes of the wealth of Internet miscreants. *ACM Conference on Computer and Communications Security (CCS),* pp.275-288, Alexandria, VA: ACM.

Graham-Cumming, J. (2014). *Understanding and mitigating NTP-based DDoS attacks.* Cloudflare, January 9, 2014. [Online] Available at: https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

Herley, C., & Florencio, D. (2010). Nobody sells gold for the price of silver:

Dishonesty, uncertainty and the underground economy. In T. Moore, D. J. Pym, & C. Ionnidis (Eds.), *Economics of Information Security and Privacy*, (pp. 35-53). New York: Springer.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28,* 171–198.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*(2), 165-177.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* London: Routledge.

Holt, T. J., Chua, Y.-T., & Smirnova, O. (2013). An exploration of the factors affecting the advertised price for stolen data. *eCrime Researchers Summit (eCRS),* 1-10.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies*, *23,* 33-50.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets. *Deviant Behavior*, *37*, 353-367.

Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones." In M. Backes & P. Ning (Eds.), *Computer Security-ESCORICS*, (pp. 1-18). Berlin and Heidelberg, Springer.

Honeynet Research Alliance. (2003). Profile: Automated Credit Card Fraud. *Know Your Enemy Paper* series. [Online] Available at http://www.honeynet.org/papers/profiles/ccfraud.pdf.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55,* 596-614.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior, 37,* 1163-1178.

Ianelli, N., & Hackworth, A. (2005). Botnets as a vehicle for online crime. *Forensic Computer Science, 1,* 19-39.

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyber wars.* London: Routledge.

Karami, M., & McCoy, D. (2013). Understanding the emerging threat of DDoS-as-a-service. LEET, 2013. [Online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=917A63159F2C3E0172FB5BC0DD62A575?doi=10.1.1.364.1421&rep=rep1&type=pdf

Karami, M., Park, Y., & McCoy, D. (2015, August). Stress testing the booters: Understanding and undermining the business of DDoS services. *Computer Science.* [Online] Available at: https://arxiv.org/pdf/1508.03410v1.pdf

Mansfield-Devine, S. (2011, January). Anonymous: serious threat of mere annoyance? *Network Security, 2011*(1), 4-10. DOI: 10.1016/S1353-4858(11)70004-6

Moore, T., Clayton, R., & Anderson, R.. (2009). The Economics of Online Crime, *Journal of Economic Perspectives, 23,* 3-20.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An Analysis of Underground Forums. *IMC'11*, 71-79.

Pruitt, M. V. (2007). Deviant research: Deception, male internet escorts, and response rates. *Deviant Behavior, 29,* 70-82.

Rossow, C., & Gortz, H. (2014, February). Amplification hell: Revisiting network protocols for DDoS abuse. *Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium*, San Diego, CA. [Online] Available at: http://www.internetsociety.org/sites/default/files/01_5.pdf

Santanna, J., RiJswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville,

L., & Pra, A. (2015, May). Booters - An Analysis of DDoS-as-a-Service Attacks. *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM),* 243-251.

Segura, V., & Lahuerta, J. (2010). Modeling the economic incentives of ddos attacks: Femtocell case study. *Economics of information security and privacy*, 107-119.

Smirnova, O., & Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist, 60,* 1403-1426.

Thomas, R. & Martin, J. (2006). The underground economy: Priceless. *;login: The Usenix Magazine, 31,* 7-17.

U.S. CERT. 2014. *Alert (TA14-017A). UDP-Based Amplification Attacks.* Government Report. Retrieved June 2, 2016 Fromhttps://www.us-cert.gov/ncas/alerts/TA14-017A

Woo, H., Kim, Y., & Dominick, J. (2004). Hackers: Militants or Merry Pranksters? A content analysis of defaced web pages." *Media Psychology, 6,* 63-82.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty, and implications for policing. *Policing and Society, 23,* 1-24.