Defining the Profile of Potential Cybercriminals

COL Thomas Hyslip, Ph.D. & Thomas J. Holt, Ph.D.

In 2009, when Cyber Command was established as a sub-unified combatant command of the U.S. Strategic Command, a Pentagon spokesman said, "The power to disrupt and destroy, once the sole province of nations, now also rests with small groups and individuals, from terrorist groups to organized crime to industrial spies to hacker activists, to teenage hackers" [1].

On May 4, the Department of Defense (DoD) announced that Cyber Command has been elevated to a unified combatant command, which "demonstrates to international partners and adversaries our stake in cyberspace and shows that DoD is prioritizing efforts to build cyber defense and resilience [2]."

DoD may benefit from studies focused on hackers and cybercriminals who pose a threat to the DoD Information Network and the internet at large. Denial of service attacks may affect field operations and access to resources, prompting DoD to address their potential for harm. This study presents the findings of a survey of a population of potential cybercriminals who conduct distributed denial of service attacks (DDoS) using what are known as booter and stresser services.

A considerable amount of research has focused on DDoS attacks and their underlying infrastructures, such as botnet malware [3-6]. Much of this work has focused on the use of network traffic data to identify and prevent DDoS attacks [7-12]. Consequently, DDoS attack methods and techniques have adapted to overcome the development of new defense and prevention techniques [13]. In fact, attackers are beginning to exploit vulnerabilities in Internet of Things devices, such as webcams, using botnets to enable large-scale DDoS attacks from diverse devices [14].

One type of new DDoS attack uses open internet servers—such as Network Time Protocol (NTP) and Domain Name System (DNS) servers—to "reflect" attacks off them and onto a target [15]. This technique not only masks the Internet Protocol (IP) address of the originating offender(s) but also amplifies the volume of attack traffic [15].

This method of DDoS attack has become very popular [16], and cybercriminals have embraced it, referring to it as either a booter or a stresser [17]. The colloquial name given to these attacks originated with booter because online game players used these attack methods to "boot" their gaming opponents offline by targeting the game server [18,19].

As booters gained popularity and notoriety, the hacking community began to refer to them as stressers because the attacks could be used as a way to stress-test their own web server.

Image Credit | Photo Illustration created by HDIAC and adapted from Adobe Stock.

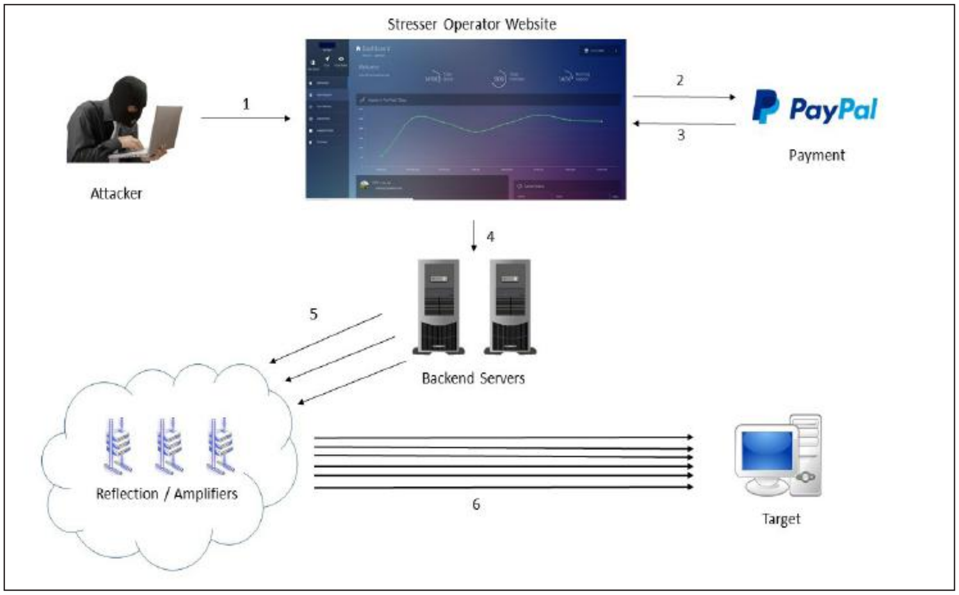


Figure 1. Structure of a Stresser DDoS-for-hire service

Individuals capable of operating these attacks began offering them up for lease on a subscription-fee basis so that customers could launch their own attacks (see Figure 1 for detail). The subscription service allows users with little or no technical skill to launch DDoS attacks by simply entering the IP address or domain name into the stresser website. Furthermore, because there is no restriction on which IP addresses or servers a stresser can target, they have been used to conduct massive DDoS attacks using the reflective technique, contributing to a significant increase in the number of reported DDoS attacks [20].

There are several noteworthy examples of booter and stresser attacks in action. For example, in 2014, the hacking group Lizard Squad attacked Sony's PlayStation Network and Microsoft's Xbox Live with a massive DDoS attack via their new Lizard Stresser, which left users unable to access services for days, resulting in Sony and Microsoft revenue loss [21]. And In 2015, the Bang Stresser was used to attack the BBC website, in what hacktivists claimed to be the largest DDoS attack ever reported, at 602 Gigabits per second (Gbps) [22].

This same method could be used to limit the availability of any critical online service, particularly those within DoD networks that provide real-time or critical connectivity to units within the field [23]. Director of the Defense Information Systems Agency and Commander of the Joint Force Headquarters DoD Information Network Lieutenant General Alan R. Lynn noted the threat to DoD from DDoS attacks and their growing sophistication and size [24]. LTG Lynn stated that as of January 2018, DoD was defending against attacks as high as 600 Gbps on internet access points, and they are preparing for 1 Terabit per second attacks [24].

Previous Research

As stressers gained notoriety, computer science researchers began to focus their efforts on the detection and disruption of stresser services. Multiple studies investigated the strength and capability of stressers by launching and capturing their own attacks [16, 17, 25], while other research efforts analyzed the underlying infrastructure required to carry out DDoS attacks [19, 26-28]. Rossow and Gortz identified 14 User Datagram Protocol (UDP) protocols for amplification attacks and the existence of millions of vulnerable amplification servers. They also measured the amplification factor for the 14 different protocols, recording an increase of 4,000 percent for the NTP protocol [16]. Ryba et al. reported stresser amplification attacks exceeding 400 Gbps, increasing internet latency across Europe [29].

These studies demonstrate that stressers have grown in number, size, and strength since their inception, and that they continue to pose a threat to the internet and its end users. Such technical analyses do not, however, provide insight into the human actors who operate stressers or into the customers who lease their services. To that end, Hutchings and Clayton surveyed a small sample of booter operators to explore how and why they operate these attack services. Booter operators interviewed as part of this research acknowledged that although they presented their offerings as legitimate network stressing services, their resources were mainly used to illicitly attack internet targets [18].

Such preliminary work is useful, but additional insight is needed to better understand the motivations, methods, and background of those who operate and use stresser services. Since booter operations simplify the process of attacks, it is vital to know the technical competencies of their user base and the operators.

Research on hacker subcultures suggests that individuals are judged within the community on the basis of their programming skill and expertise; those with more knowledge are granted elevated social status [30-33]. It is possible that those with greater skill are more likely to operate booter services, although their customers may be equally knowledgeable, simply opting to pay for the service rather than possess and manage the required infrastructure on their own.

Alternatively, booter customers may have relatively low skill, needing to purchase a service because they cannot cultivate it themselves. It is also essential to identify commonly reported attack targets and the rationales behind attacks in order to determine whether customers seek to target their own networks (as the booter advertiser claims) or to attack commercial, government, or military infrastructures. These insights better contextualize the actors who would use a stresser in a real attack.

Furthermore, DoD recognizes that a need exists for greater threat intelligence in cyber defense, and cultural studies of computer criminals helps to fill this gap [34, 35]. Understanding the demographics and motivations of actors may help DoD intelligence agencies identify potential adversaries. At the same time, identifying the attack targets and network protocols used to facilitate attacks can provide threat intelligence to help defend the DoD Information Network [36].

Our Contribution

Early research conducted on booters revealed that the users were primarily online gamers, but subsequent expansions in the use of booters, especially in large DDoS attacks against commercial targets, raises the following questions.

1. Who are the users of stressers?

2. Why do they use stressers (i.e., motivation)?

3. What do they use the stressers for (i.e., target)?

Methodology

We obtained 59,009 publicly available email addresses of registered users from 15 stresser services. An email was sent to each address that included a link to an anonymous survey hosted by Survey Monkey. The first round of emails was sent Nov. 27–29, 2016, and invited recipients to participate in a research study on stressers and booters. The email specified that responses would be used solely for research purposes.

Although the initial sample consisted of 59,009 email addresses, 8,018 of these were not valid based on bounce-back notices. A second email was sent Dec. 2, 2016, as a reminder to complete the survey before its Dec. 30, 2016 closing. Of all messages sent, 5,226 emails were verified as received and opened. This response rate was expected, as the email database was publicly available and included junk/false addresses.

Eight hundred and twenty one individuals began the survey and answered at least one question, resulting in at least 250 responses to each question. This decrease from the total of respondents who had any engagement with a survey question to those who completed it falls within the expected response rate for online survey studies; furthermore, it is a high response rate for an anonymous survey conducted among a population of active offenders [37, 38]. After discounting the 8,018 invalid email addresses, the effective response rate was 1.87 percent (821 of 43,891), which is unsurprising as prior research notes that individuals engaged in cybercrime are less likely to participate in research out of concern for their safety [18, 31, 39]. The nature of the survey may limit generalizability of the data. However, the responses provide essential insight into an underexamined phenomenon.

This sample of individuals, at minimum, had registered an account with a stresser—or may have used a stresser to launch a DDoS attack. Thus, questions were structured to understand the extent to which the respondent both used stresser services and facilitated their operations. The survey consisted of 22 multiple choice questions and one open comment box for follow-up requests. The questions covered the use of stressers and requested information regarding respondent skill level, payment type, attack protocols used, attack targets, motivation for use, and demographic data.

Results

Respondents were asked to provide their demographic characteristics in an attempt to quantify the overall makeup of the population. The majority of respondents reported living within the U.S. or U.K.—in keeping with evidence drawn from law enforcement investigations and arrest records over the last three years.

Respondents who reported their age were primarily in their late teens or 20s, were male (88 percent), and white (63 percent), corresponding to prior research findings on the ages of the hacker population as a whole [18, 32, 40]. The majority of respondents reported an education level beyond that of high school.

Respondents were also asked to rank their skill level from 1 to 10, with 10 being the most skilled. We acknowledge these results may be skewed, as skill level was self-reported. Indeed, the most commonly reported skill level was 10. However, the next most common response was 1, suggesting that most respondents answered in an honest fashion. While it is possible some respondents falsified response(s), such an idea runs counter to the broader empirical literature that indicates hackers prefer to make their abilities known [27, 29].

The overwhelming majority of respondents (89.2 percent) indicated they had used booter services, which makes sense given their addresses were associated with a database of service provider clients. The majority of those who had used a booter (65.2 percent) paid for the service. While a substantial amount of attention has been paid to the use of cryptocurrencies in cybercrime, the majority of respondents paid for stresser services via Paypal—a pattern corroborated by prior research on booters [25]. Cryptocurrencies were used with less frequency than PayPal, and Bitcoin was the most-used cryptocurrency.

Eighty-seven percent of respondents answered in the affirmative when asked, “Were you able to use the booter or stresser to test systems?” The question was written to be less accusatory and used the term "test systems" rather than "attack systems."

Relatedly, there was some distribution of responses related to stress testing systems with 17 percent of respondents (n=232) having stressed only one system, while 47 percent stressed more than 10. Almost half of stresser customers used them to attack multiple computer systems. Additionally, there appears to be limited fidelity within the community, as 29 percent of respondents reported having accounts with more than five vendors, followed by 25 percent having accounts with two stressers.

Interestingly, 74 percent of the respondents noted the booter worked as advertised, which suggests that not all vendors may be accurate in their advertising. While some in the general public may assume there is no trust between criminal actors, it is an important factor in the underground market for cybercrime services. As a result, if a service provider is unable to deliver on an advertised product, it may reduce the overall customer base over time.

The majority of customers used common attack methods, most notably UDP, DNS, and NTP attacks. Other less common methods, such as VSE, RST, and QUIC, were observed but in much smaller numbers. This matches previous research that examined network captures of stresser attacks and supports the notion that stressers utilize different attacks depending on the nature of their target and the reflection servers available to complete the attack [16, 17].

The reported motivations were also varied (as shown in Figure 2). Customers

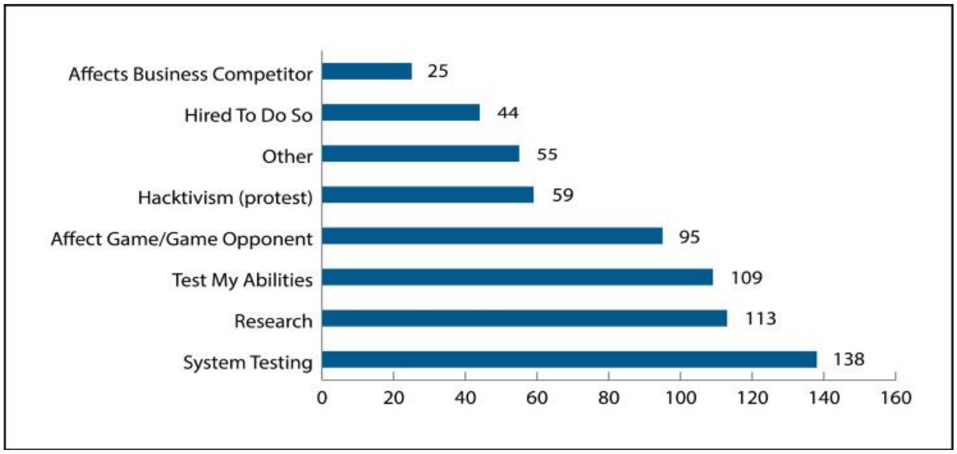


Figure 2. Participant response to, "What was your motivation to use a booter or stresser?"

(n=230) primarily reported using stressors to test their system, conduct research, or test their individual abilities. In addition, 41 percent of respondents used a booter to affect a game or gaming opponent. Such a motive is in keeping with the original use of booter services by hackers [25].

More nefarious motivations were also reported, with 26 percent of respondents reporting they used it for hacktivism or protest. (In this case, hacktivism refers to the use of hacking in support of a specific belief or activist agenda.) Nineteen percent of respondents also noted they were hired by someone else to use the stresser, and 11 percent were motivated to use the stresser to affect a business competitor.

Given that individuals who registered with a service may have done so as an interested client or potential competitor, respondents were asked if they have ever operated their own booter or stresser service. A majority of respondents (54 percent) reported they ran their own operation, suggesting there may be a low barrier to entry to engage in this form of cybercrime-as-service. Additionally, 64 percent of respondents assisted booter operations in some fashion.

Furthermore, 76.4 percent of respondents reported they have been targeted by a stresser operator. This finding supports prior research that suggests hackers may target one another either because of perceived slights or real conflicts between actors [30-32].

When asked what resource they used a stresser against (see Figure 2), the majority of respondents reported either targeting themselves or a game server. More than 52 percent of respondents reported using a stresser to attack a private or commercial website/webserver, and 26 percent reported attacking another type of business server, such as an email or file server. Seventeen percent of respondents reported use of the stresser to attack a government-owned website or webserver [20].

Cross tabulation was used to examine the relationship between attacker motivation and target (see Table 1). The majority who reported targeting themselves were motivated by system testing, research, and the desire to test their abilities. There was a more equal distribution of motives for those targeting game, business, and government servers.

Also, a plurality of respondents who were motivated by hacktivism or protest reported a commercial website as their primary target of attack. Respondents also attacked themselves in order to determine whether their infrastructure could withstand the

What was your motivation?	Yourself	Game	Business Server	Commercial Website	Government Website	Other
Research	27%	17%	13%	20%	9%	13%
System Testing	28%	17%	13%	21%	8%	13%
Affect Game/ Opponent	16%	27%	11%	21%	9%	16%
Hacktivism/ Protest	17%	20%	13%	24%	12%	14%
Affect Business Competitor	15%	18%	17%	19%	14%	17%
Test Abilities	22%	21%	12%	22%	9%	15%
Hired to Do So	19%	18%	17%	19%	12%	15%
Other	17%	18%	13%	21%	9%	22%

Table 1. Attacker motivations versus targets of attack.

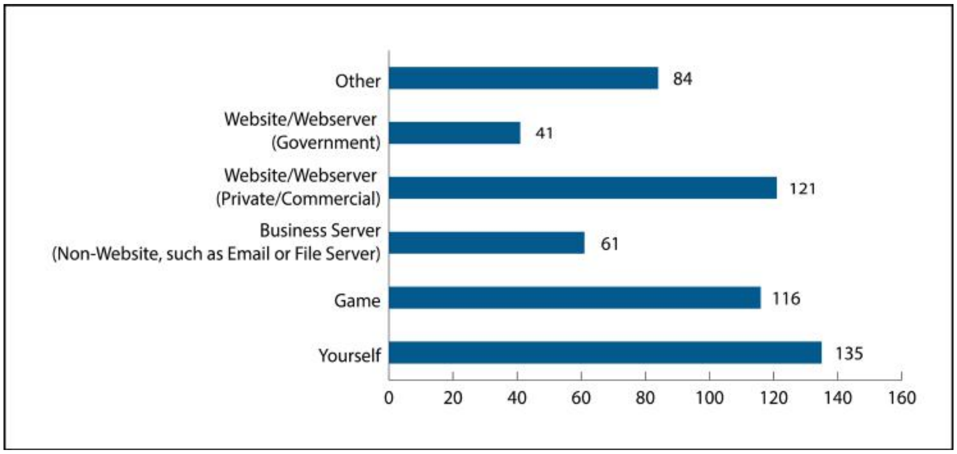


Figure 3. Participant response to, "What did you use the stresser/booter on?"

traffic, which corresponds to the notion that these services can stress-test sites.

Discussion and Conclusion

The rise of booter and stresser services evidences the evolution of cyberthreats and the rise of cybercrime-as-service providers. Although the technical dynamics of these attack types are commonly researched [19, 20], few have examined the characteristics of the clientele of the stresser to understand the human actors behind these attacks [18]. This analysis addresses this issue through a survey delivered to individuals who registered an email address with one or more of 15 select stresser operators. The results of the survey show that most of the respondents reported they are young, white males, which is in keeping with prior research on the hacker community [30-33]. Most of them did not, however, use stressers simply to test their own infrastructure or attack online game opponents [18, 19]. Nearly a quarter of respondents cited hacktivism as their motive when using stressers, and 10 percent tried to affect a business competitor.

This attack type is likely fueled by the ease of access to stressers, the low cost, anonymity, and simplicity of use [18, 24]. This as a potential asymmetric threat that could be used by any potential enemy actor, including those with nation-state sponsorship. Hiring a booter would provide the attacker, and the nation-state, with plausible deniability for the attack as the stresser operator may not know their clientele [18].

It is also clear that criminal actors may seek to leverage the power of a stresser or booter to more effectively target critical infrastructure without the need to cultivate advanced technical skills [23]. Such an attack could originate from an ideologically motivated organization, such as a jihadist group, or those without a specific political agenda, such as the group Anonymous. In fact, over the last decade, members of Anonymous repeatedly utilized large DDoS attacks against commercial and government entities in response to perceived wrongs, including attacks against the National Security Agency and the FBI [41, 42]. Many of these attacks were enabled through Anonymous' stand-alone DDoS tool—the Low Orbit Ion Cannon.

Groups like Anonymous may serve as a template for other attackers, which may partially account for the hundreds of new hacktivist groups established over the last few years [43, 44]. These groups do not hesitate to attack military and government infrastructure and may use stressers as a more effective and inexpensive attack resource [43, 44]. To that end, the number and strength of stressers has grown concurrently with the emergence of new hacktivist groups.

This may create an operational environment where hacktivists do not invest time or resources to build their own tools or develop skills to engage in attacks. Instead, they can quickly and easily launch massive DDoS attacks that are bounced off millions of vulnerable internet servers at a low cost [16]. Thus, additional research is needed to understand the human actors behind large-scale DDoS attacks and their decision-making [18, 23, 30, 31]. Such information can improve our knowledge of the rationale of attackers, which may provide insight into why and how these methods can be used to take down critical infrastructure components.

References

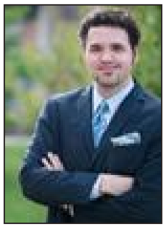
1. Gray, A. (2009, June 23). Pentagon approves creation of cyber command. Reuters. Retrieved from https://www.reuters.com/article/us-usa-pentagon-cyber/pentagon-approves-creation-of-cyber-command-idUSTRE55M78920090624
2. Lange, K. (2018, May 3). Cybercom becomes DoD's 10th unified combatant command [DoD Live web log post]. Retrieved from http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/
3. Leder, F., Werner, R., & Martini, P. (2009, June). Proactive botnet countermeasures an offensive approach. *Proceedings of the Conference on Cyber Warfare 2009*, Tallinn, Estonia. Retrieved from http://www.ccdcoe.org/publications/virtualbattlefield/15_LEDER_Proactive_Coutnermeasures.pdf
4. Gu, G., Porras, P., Yegneswaran, V., Fong, M., & Lee, W. (2007, August). BotHunter: Detecting malware infection through IDS-driven dialog correlation. *Proceedings of the 16th USENEX Security Symposium*, Boston, MA. Retrieved from https://www.usenix.org/legacy/events/sec07/tech/full_papers/gu/gu.pdf
5. Dittrich, D. (2012, April). So you want to take over a botnet . . . *Proceedings of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats, LEET '12*, San Jose, CA. Retrieved from https://www.usenix.org/system/files/conference/leet12/leet12-final23.pdf
6. Zeng, Y. (2012). *On detection of current and next-generation botnets* (Doctoral dissertation). University of Michigan. Retrieved from http://deepblue.lib.umich.edu/handle/2027.42/91382
7. Rossow, C., & Dietrich, C. J. (2013, July). PROVEX: Detecting botnets with encrypted command and control channels. *Detection of Intrusions and Malware, and Vulnerability Assessment Lecture Notes in Computer Science*, 21-40. doi:10.1007/978-3-642-39235-1_2
8. Gu, G., Zhang, J., & Lee, W. (2008, February). BotSinffer: Detecting botnet command and control channels in network traffic. *Proceedings of the 15th Annual Network and Distributed System Security Symposium*, San Diego, CA. Retrieved from http://www.isoc.org/isoc/conferences/ndss/08/proceedings.shtml
9. Feily, M., Shahrestani, A., & Ramadass, S. (2009, June). A survey of botnet and botnet detection. *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, 268-273. doi:10.1109/SECURWARE.2009.48
10. Brezo, F., Santos, I., Bringas, P. G., & Val, J. L. (2011, Aug). Challenges and limitations in current botnet detection. *2011 22nd Inter-*

national Workshop on Database and Expert Systems Applications, 95-101. doi:10.1109/DEXA.2011.19

11. Zhang, J. (2012, August). *Effective and scalable botnet detection in network traffic* (Doctoral dissertation, 2012). Georgia Institute of Technology. Retrieved from ProQuest Dissertations and Theses database. (AAT 1115317916)
12. Lu, C., & Brooks, R. R. (2013). Timing analysis in P2P botnet traffic using probabilistic context-free grammars. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 1-4. doi:10.1145/2459976.2459992
13. Dittrich, D. (2012, April). So you want to take over a botnet. *Proceedings of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats*. Retrieved from https://www.usenix.org/system/files/conference/leet12/leet12-final23.pdf
14. European Union Agency for Network and Information Security. (2016, November 3). Major DDoS attacks involving IOT devices. Retrieved from https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices
15. United States Computer Emergency Readiness Team. (2014, January 17). Alert (TA14-017A): UDP-Based Amplification Attacks. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-017A
16. Rossow, C. (2014, February). Amplification hell: Revisiting network protocols for DDoS abuse. *Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium*. doi:10.14722/ndss.2014.23233
17. Hyslip, T., & Holt, T. (2018). Assessing the capacity of DDoS-for-hire services in cybercrime markets. *Deviant Behavior*. Manuscript submitted for publication.
18. Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, 37(10), 1163-1178. doi:10.1080/01639625.2016.1169829
19. Karami, M. & McCoy, D. (2013, August). Understanding the emerging threat of DDoS-as-a-Service. USENIX Workshop on Large-Scale Exploits and Emergent Threats, Berkeley, CA. Retreived from https://www.usenix.org/conference/leet13/workshop-program/presentation/karami
20. Arbor Networks (2015, January). *Arbor Networks 10th Annual Worldwide Infrastructure Security Report* Finds 50X Increase in DDoS Attack Size in Past Decade [Press release]. Retrieved from https://www.enhancedonlinenews.com/news/eon/20150127005614/en/Arbor-Networks/Worldwide-Infrastructure-Security-Report/WISR
21. Turnton, W. (2014, December 30). Lizard Squad's Xbox Live, PSN attacks were a 'marketing scheme' for new DDoS service. The Daily Dot. Retrieved from http://www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/
22. Whitaker, Z. (2016, January). BBC, Trump web attacks "just the start," says hacktivist group. ZDNet. Retrieved from https://www.zdnet.com/article/attackers-targeting-bbc-donald-trump-amazon-web-services/
23. Denning, D. (2010). Cyber-conflict as an emergent social problem. In T.J. Holt and B. Schell (eds), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 170-186). Hershey, PA: IGI-Global
24. Karami, M., Park, Y., & McCoy, D. (2015, August). Stress testing the booters: Understanding and undermining the business of DDoS services. *Proceedings of the 25th International Conference on World Wide Web*, 1033-1043. doi:10.1145/2872427.2883004
25. Schwartz, S. A. (2018, January 17). DOD hit with 36M malicious emails daily, prepares for massive DDoS attack. Retrieved from https://www.ciodive.com/news/dod-hit-with-36m-malicious-emails-daily-prepares-for-massive-ddos-attack/514844/
26. Kovacs, E. (2015, July 1). Attackers abuse RIPv1 protocol for DDoS reflection: Akamai. Security Week. Retrieved from http://www.securityweek.com/attackers-abuse-ripv1-protocol-ddos-reflection-akamai
27. Kravtsov, P. (2015, October 16). A look at the new WordPress brute force amplification attack. Retrieved from https://blog.cloudflare.com/a-look-at-the-new-wordpress-brute-force-amplification-attack/
28. Santanna, J., RiJswijk-Deij, R. V., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015, May). Booters — An analysis of DDoS-as-a-service attacks. *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. doi: 10.1109/INM.2015.7140298
29. Ryba, F., Orlinkski, M., Wahlisch, M., Rossow, C., & Schmidt, T. (2016, May). Amplification and DRDoS attack defense - - A survey and new perspectives. Retrieved from https://arxiv.org/abs/1505.07892
30. Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, *4*(1&2), 643-656
31. Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198. doi:10.1080/01639620601131065
32. Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780. doi:10.1111/1467-954x.00139
33. Steinmetz, K. F. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime*. New York, NY: New York University Press.
34. Pomerleau, M. (2018, January 12). Defensive cyber continues to mature, still lags offensive cyber. Fifth Domain. Retrieved from https://www.fifthdomain.com/dod/cybercom/2018/01/12/defensive-cyber-continues-to-mature-still-lags-offensive-cyber/
35. Pomerleau, M. (2017, June 19). Cyber protection teams need intelligence, say officials. C4ISRNET. Retrieved from https://www.c4isrnet.com/disa/disa-vision-guide/2017/06/19/cyber-protection-teams-need-more-intelligence-say-officials/
36. Pomerleau, M. (2017, June 15). DoD cyber defense arm establishes intel/ops fusion cellC4ISRNET. Retrieved from https://www.c4isrnet.com/disa/disa-vision-guide/2017/06/15/dod-cyber-defense-arm-establishes-intel-ops-fusion-cell/
37. Curtin, R., Presser, S., & Singer, E. (2005). Changes in telephone survey nonresponse over the past quarter century. *Public Opinion Quarterly*, *69*(1), 87-98. doi:10.1093/poq/nfi002
38. Zan, H., & Fan, J. X. (2010). Cohort effects of household expenditures on food away from home. *Journal of Consumer Affairs*, *44*(1), 213-233. doi:10.1111/j.1745-6606.2010.01163.x
39. Pruitt, M. V. (2007). Deviant research: Deception, male internet escorts, and response rates. *Deviant Behavior*, *29*(1), 70-82. doi:10.1080/01639620701457782
40. Greenwood, C. (2017, April 21). How the average age of British hackers is only 17... and they start at 13 with web-connected games consoles. *Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-4434526/How-average-age-British-hackers-17.html
41. Harkinson, J. (2012, January 20). How and why Anonymous took down the FBI'swebsite. MotherJones. Retrieved from http://www.motherjones.com/crime-justice/2012/01/inside-anonymous-largest-attack-ever-fbi-megaupload-mega-upload/
42. Sheets, C. A. (2013, October 25). NSA Website down following apparent DDoS attack possibly by Anonymous of a foreign government. International Business Times. Retrieved from http://www.ibtimes.com/nsa-website-down-following-apparent-ddos-attack-possibly-anonymous-or-foreign-government-1442452
43. Lohrmann, D. (2017, February 22). The dramatic rise in hacktivism. Techcrunch. Retrieved from https://techcrunch.com/2017/02/22/the-dramatic-rise-in-hacktivism/
44. Bergal, J. (2017, January 10). Hacktivists launch more cyberattacks against local, state government. PBS. Retrieved from https://www.pbs.org/newshour/nation/hacktivists-launch-cyberattacks-local-state-governments

COL Thomas S. Hyslip, Ph.D.
Adjunct Professor, Norwich University

Thomas S. Hyslip is an adjunct professor in the College of Graduate and Continuing Studies at Norwich University, specializing in cybersecurity, cybercrime, and critical infrastructure protection (Ph.D., Capitol College). Hyslip works full time as federal agent specializing in cybercrime investigations and forensics and is also a Colonel in the U.S. Army Reserve.



Thomas J. Holt, Ph.D.
Professor, Michigan State University

Thomas J. Holt is a professor in the School of Criminal Justice at Michigan State University, specializing in cybercrime, cyberterrorism, and policy responses to these threats (Ph.D., University of Missouri-Saint Louis). His work has appeared in numerous academic journals, including *British Journal of Criminology*, *Crime & Delinquency*, *Deviant Behavior*, and *Terrorism & Political Violence*. He is also the author of multiple books and has presented his work in various academic and practitioner conferences around the world.

Homeland Defense & Security
Information Analysis Center

Pre-awarded, Pre-competed

Core Analysis Task

Visit hdiac.org or contact info@hdiac.org for more information

Image Credit *Photo Illustration created by HDIAC and adapted from U.S. Marines Photo by Lance Cpl. Zachery Laning. (available for viewing at http://www.marines.mil/Photos/igphoto/2001753020/).*