to install patches and filters, these events had direct measurable costs in terms of increased bandwidth loads as measured at example edge networks. Though this paper documents the lethal power of the largest DDoS attacks observed to date, our conclusions include a positive one. The network research and operations community worked to actively mitigate the effects of these attacks and these efforts have had a visible impact in diminishing the vulnerable amplifier population and reducing attack traffic. There are, however, limits to the effectiveness of such remediation efforts, as the tapering of mitigation shows. Since rapid remediation is how such attack vectors are thwarted, we are interested in future work examining why some networks remediate faster than others.

Acknowledgments

This work was supported in part by the Department of Homeland Security Science and Technology Directorate under contract numbers D08PC75388, FA8750-12-2-0314, FA8750-12-2-0235, and N66001-13-C-3001; the National Science Foundation under contract numbers CNS 1111699, CNS 091639, CNS 08311174, CNS 0751116, CNS 1330142, and CNS 1255153; and the Department of the Navy under contract N000.14-09-1-1042. We would like to thank Jared Mauch for sharing the OpenNTPProject.org dataset as well as Kirk Soluk and team at Arbor Networks for sharing traffic and attack statistics. Finally, we are grateful to Roland Dobbins, Christian Rossow, Denis Foo Kune, anonymous reviewers, and our shepherd, Sharon Goldberg, for valuable feedback on earlier drafts.

10. REFERENCES

[1] Front Range GigaPop. http://www.frgp.net/frgp-overview-2014-03-27.pdf.

[2] Open NTP Project. http://openntpproject.org/.

[3] Open Resolver Project. http://openresolverproject.org/.

[4] Arbor Networks Solution Brief: DDoS Attacks in the Gaming Industry, 2013. www.arbornetworks.com/docman-component/doc_download/687-gaming-company-defends-against-ddos-attacks.

[5] Hack Forums "Server Stress Testing" marketplace forum, Aug. 2014. http://www.hackforums.net/forumdisplay.php?fid=232.

[6] The OVH offering expands with new lines of dedicated serers., Feb 2014. https://www.ovh.com/us/newsroom/cp1355.the_ovh_offering_expands_with_new_lines_of_dedicated_servers.

[7] M. Allman. Comments on Bufferbloat. *ACM Computer Communication Review*, 43(1), Jan. 2013.

[8] D. Anstee, A. Cockburn, G. Sockrider, and C. Morales. Arbor Networks Worldwide Infrastructure Security Report, 2014. http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf.

[9] Arbor Networks. www.arbornetworks.com.

[10] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. The internet motion sensor: A distributed blackhole monitoring system. In *Proceedings of Network and Distributed System Security Symposium (NDSS '05)*, pages 167–179, 2005.

[11] K. Benson, A. Dainotti, k. Claffy, and E. Aben. Gaining Insight into AS-level Outages Through Analysis of Internet Background Radiation. In *Proceedings of the 2012 ACM Conference on CoNEXT Student Workshop*, CoNEXT Student '12, 2012.

[12] S. O. Blog. Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks, Dec 2013. http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks.

[13] L. Constantin. OVH's Own NTP Servers Used in Attack, Feb 2014. http://news.techworld.com/security/3501549/attackers-use-ntp-reflection-in-huge-ddos-attack/.

[14] J. Czyz, K. Lady, S. G. Miller, M. Bailey, M. Kallitsis, and M. Karir. Understanding IPv6 Internet Background Radiation. In *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC'13), Barcelona, Spain*, 2013.

[15] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé. Analysis of Country-wide Internet Outages Caused by Censorship. In *Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference (IMC'11)*, pages 1–18. ACM, 2011.

[16] X. Dimitropoulos, P. Hurley, A. Kind, and M. P. Stoecklin. On the 95-percentile billing method. In *Proceedings of the Passive and Active Network Measurement Conference (PAM'09)*, 2009.

[17] J. Fleury. Good News: Vulnerable NTP Servers Closing Down, Feb 2014. http://blog.cloudflare.com/good-news-vulnerable-ntp-servers-closing-down.

[18] D. Goodin. New DoS attacks taking down game sites deliver crippling 100Gbps floods, Jan 2014. http://arstechnica.com/security/2014/01/new-dos-attacks-taking-down-game-sites-deliver-crippling-100-gbps-floods/.

[19] M. Karami and D. McCoy. Understanding the Emerging Threat of DDoS-as-a-Service. In *Presented as part of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats*. USENIX, 2013.

[20] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. In *Proceedings of the 23rd USENIX Security Symposium*, August 2014.

[21] Z. M. Mao, V. Sekar, O. Spatscheck, J. Van Der Merwe, and R. Vasudevan. Analyzing Large DDoS Attacks Using Multiple Data Sources. In *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*, pages 161–168. ACM, 2006.

[22] Merit Network, Inc. www.merit.edu.

[23] D. Mills, J. Martin, J. Burbank, and W. Kasch. Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC 5905, 2010.

[24] M. Mimoso. Volume of NTP Amplification Attacks Getting Louder, Apr 2014. http://threatpost.com/volume-of-ntp-amplification-attacks-getting-louder/105763.

[25] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage. Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS)*, 24(2):115–139, 2006.

[26] K. Orland. Multiple gaming platforms hit with apparent DDoS attacks, Jan 2014. http://arstechnica.com/gaming/2014/01/multiple-gaming-platforms-hit-with-apparent-ddos-attacks/.

[27] V. Paxson. An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review*, 31(3):38–47, 2001.

[28] N. Perlroth. Tally of Cyber Extortion Attacks on Tech Companies Grows, Jun 2014. http://bits.blogs.nytimes.com/2014/06/19/tally-of-cyber-extortion-attacks-on-tech-companies-grows/.

[29] K. Poulsen. FBI busts alleged DDoS Mafia, Aug. 2004. http://www.securityfocus.com/news/9411.

[30] M. Prince. Technical Details Behind a 400Gbps NTP Amplification DDoS Attack, Feb 2014. http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack.

[31] Prolexic. Prolexic Quarterly Global DDoS Attack Report: Q1 2014, Apr. 2014. http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q1.html.

[32] C. Rossow. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *Proceedings of the 2014 Network and Distributed System Security Symposium, NDSS*, San Diego, CA, 2014.

[33] C. Systems. Cisco Event Response: Network Time Protocol Amplification Distributed Denial of Service Attacks, Feb. 2014. http://www.cisco.com/web/about/security/intelligence/ERP-NTP-DDoS.html.

[34] The Spamhaus Project - PBL. http://www.spamhaus.org/pbl/.

[35] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Houston. Internet Background Radiation Revisited. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement (IMC '10)*, Melbourne, Australia, November 2010.

[36] J. Zhang, Z. Durumeric, M. Bailey, M. Karir, and M. Liu. On the Mismanagement and Maliciousness of Networks. In *Proceedings of the Network and Distributed System Security Symposium (NDSS '14)*, San Diego, CA, February 2014.