References

[1] MaxMind: IP Geolocation and Online Fraud Prevention. `http://dev.maxmind.com/`.

[2] RIPE Stat: Information about specific IP addresses and prefixes. `https://stat.ripe.net/`.

[3] The New Threat: Targeted Internet Traffic Misdirection. `http://research.dyn.com/2013/11/mitm-internet-hijacking/`.

[4] UK traffic diverted through Ukraine. `http://research.dyn.com/2015/03/uk-traffic-diverted-ukraine/`.

[5] R. Albert, H. Jeong, and A.-L. Barabási. Error and attack tolerance of complex networks. *nature*, 406(6794):378–382, 2000.

[6] K. R. Butler, T. R. Farley, P. McDaniel, and J. Rexford. A survey of bgp security issues and solutions. *Proceedings of the IEEE*, 98(1):100–122, 2010.

[7] F. Cangialosi, T. Chung, D. R. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson. Measurement and analysis of private key sharing in the HTTPS ecosystem. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 628–640, 2016.

[8] R. Cohen, K. Erez, D. B. Avraham, and S. Havlin. Breakdown of the Internet under Intentional Attack. *Physical Review Letters*, 86(16):3682–3685, Apr. 2001.

[9] L. Daigle. WHOIS Protocol Specification. RFC 3912 (Draft Standard), Sept. 2004.

[10] S. Frey, Y. Elkhatib, A. Rashid, K. Follis, J. Vidler, N. Race, and C. Edwards. It bends but would it break? topological analysis of bgp infrastructures in europe. In *2016 IEEE European Symposium on Security and Privacy (Euro S&P 16)*, pages 423–438, March 2016.

[11] E. Hjelmvik. China's man-on-the-side attack on github. `http://bit.ly/2kx4zAE`, 2015.

[12] W. Jiang, D. Lee, and S. Hu. Large-scale longitudinal analysis of soap-based and restful web services. In *Web Services (ICWS), 2012 IEEE 19th International Conference on*, pages 218–225, June 2012.

[13] S.-C. Kil, Hyunyoungand Oh, E. Elmacioglu, W. Nam, and D. Lee. Graph theoretic topological analysis of web service networks. *World Wide Web*, 12(3):321–343, 2009.

[14] S. Landau. Making sense from snowden: What's significant in the nsa surveillance revelations. *IEEE Security Privacy*, 11(4):54–63, July 2013.

[15] S. Liu, I. Foster, S. Savage, G. M. Voelker, and L. K. Saul. Who is .com?: Learning to parse whois records. In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, IMC '15, pages 369–380, New York, NY, USA, 2015. ACM.

[16] B. Marczak, N. Weaver, J. Dalek, R. Ensafi, D. Fifield, S. McKune, A. Rey, J. Scott-Railton, R. Deibert, and V. Paxson. An analysis of china's "great cannon". In *5th USENIX Workshop on Free and Open Communications on the Internet (FOCI 15)*, Washington, D.C., Aug. 2015. USENIX Association.

[17] G. Nakibly, J. Schcolnik, and Y. Rubin. Website-targeted false content injection by network operators. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 227–244, Austin, TX, Aug. 2016. USENIX Association.

[18] A. Natarajan, P. Ning, Y. Liu, S. Jajodia, and S. E. Hutchinson. NSDMiner: Automated discovery of Network Service Dependencies. In *Proceedings of the IEEE INFOCOM 2012, Orlando, FL, USA, March 25-30, 2012*, pages 2507–2515, 2012.

[19] J. Newland. Large scale ddos attack on github.com. `https://github.com/blog/1981-large-scale-ddos-attack-on-github-com`, 2015.

[20] N. Nikiforakis, L. Invernizzi, A. Kapravelos, S. Van Acker, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna. You are what you include: Large-scale evaluation of remote javascript inclusions. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 736–747, New York, NY, USA, 2012. ACM.

[21] A. Noroozian, M. Korczyński, C. H. Gañan, D. Makita, K. Yoshioka, and M. van Eeten. *Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service*, pages 368–389. Springer International Publishing, Cham, 2016.

[22] G. Pellegrino, C. Rossow, F. J. Ryba, T. C. Schmidt, and M. Wählisch. Cashing out the great cannon? on browser-based ddos attacks and economics. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, Washington, D.C., Aug. 2015. USENIX Association.

[23] G. Pellegrino, C. Tschürtz, E. Bodden, and C. Rossow. *jÄk: Using Dynamic Analysis to Crawl and Test Modern Web Applications*, pages 295–316. Springer International Publishing, Cham, 2015.

[24] D. A. Wheeler and G. N. Larsen. Techniques for cyber attack attribution. Technical report, DTIC Document, 2003.

[25] A. Zand, G. Vigna, R. A. Kemmerer, and C. Kruegel. Rippler: Delay injection for service dependency detection. In *2014 IEEE Conference on Computer Communications, INFOCOM 2014, Toronto, Canada, April 27 - May 2, 2014*, pages 2157–2165, 2014.

[26] J. Zhao, J. Wu, M. Chen, Z. Fang, X. Zhang, and K. Xu. K-core-based attack to the internet: Is it more malicious than degree-based attack? *World Wide Web*, 18(3):749–766, 2015.