# REFERENCES

Alexa, "Alexa web information company," , 2016, URL `http://www.alexa.com/topsites`.

Amoroso, E., "Intrusion detection: an introduction to internet surveillance, correlation, trace back, traps, and response," *Intrusion. Net Book*, 1999.

Anderson, J. P., "Computer security threat monitoring and surveillance," Technical report, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, 1980.

Barr, D., "RFC 1912: Common DNS operational and configuration errors," *The Pennsylvania State University, Pennsylvania*, 1996.

Bartolini, N., Casalicchio, E., and Tucci, S., "A walk through content delivery networks," in "Performance Tools and Applications to Networked Systems," pp. 1–25, Springer, 2004.

Bestavros, A. and Mehrotra, S., "DNS-based internet client clustering and characterization," in "Workload Characterization, 2001. WWC-4. 2001 IEEE International Workshop on," pp. 159–168, IEEE, 2001.

Bilge, L., Sen, S., Balzarotti, D., Kirda, E., and Kruegel, C., "EXPOSURE: a passive DNS analysis service to detect and report malicious domains," *ACM Transactions on Information and System Security (TISSEC)*, volume 16(4) p. 14, 2014.

Buyya, R., Pathan, M., and Vakali, A., *Content delivery networks*, volume 9, Springer Science & Business Media, 2008.

Callahan, T., Allman, M., and Rabinovich, M., "On modern DNS behavior and properties," *ACM SIGCOMM Computer Communication Review*, volume 43(3) pp. 7–15, 2013.

Cappelli, D. M., Moore, A. P., and Trzeciak, R. F., *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, Addison-Wesley, 2012.

Cheshire, S. and Krochmal, M., "RFC 6762: Multicast DNS," *Internet Engineering Task Force (IETF) standard*, 2013.

Clearswift, "Clearswift Insider Threat Index 2015 International Edition," , 2015, URL http://pages.clearswift.com/FY16-CITI-Int-Report.html.

Dellaert, F., "The expectation maximization algorithm," , 2002.

Do, C. B. and Batzoglou, S., "What is the expectation maximization algorithm?" *Nature biotechnology*, volume 26(8) pp. 897–899, 2008.

Dutta, D., Dutta, P., and Sil, J., "Categorical Feature Reduction Using Multi Objective Genetic Algorithm in Cluster Analysis," in "Transactions on Computational Science XXI," pp. 164–189, Springer, 2013.

Edmonds, R., "ISC passive DNS architecture," *Internet Systems Consortium, Inc., Tech. Rep*, 2012.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., and Witten, I. H., "The WEKA data mining software: an update," *ACM SIGKDD explorations newsletter*, volume 11(1) pp. 10–18, 2009.

Hands, N. M., Yang, B., and Hansen, R. A., "A Study on Botnets Utilizing DNS," in "Proceedings of the 4th Annual ACM Conference on Research in Information Technology," pp. 23–28, ACM, 2015.

Keeney, M., *Insider threat study: Computer system sabotage in critical infrastructure sectors*, US Secret Service and CERT Coordination Center, 2005.

Kurose, J. F., *Computer Networking: A Top-Down Approach Featuring the Internet, 3/E*, Pearson Education India, 2005.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., and Wolff, S., "A brief history of the Internet," *ACM SIGCOMM Computer Communication Review*, volume 39(5) pp. 22–31, 2009.

Leung, C., "Big data mining and analytics," *Encyclopedia of business analytics and optimization. IGI Global*, pp. 328–337, 2014.

Liu, C. and Albitz, P., *DNS and Bind*, O'Reilly Media, Inc., 2006.

mariadb, "MariaDB," , 2016, URL https://mariadb.org/.

MaxMind, "GeoIP legacy python extension API," , 2014, URL https://github.com/maxmind/geoip-api-python.

McLachlan, G. and Krishnan, T., *The EM algorithm and extensions*, volume 382, John Wiley & Sons, 2007.

Mell, P. and Kent, K., "Guide to Malware Incident Prevention and Handling," , 2005.

Mitchell, M., *An introduction to genetic algorithms*, MIT press, 1998.

Mockapetris, P. V., "Domain names-concepts and facilities," , 1987.

Mundie, D. A., Perl, S. J., and Huth, C., "Insider Threat Defined: Discovering the Prototypical Case." *JoWUA*, volume 5(2) pp. 7–23, 2014.

Neumann, P. G. and Parker, D. B., "A summary of computer misuse techniques," in "Proceedings of the 12th National Computer Security Conference," pp. 396–407, Baltimore, MD, USA, 1989.

Pai, S., Di Troia, F., Visaggio, C. A., Austin, T. H., and Stamp, M., "Clustering for malware classification," *Journal of Computer Virology and Hacking Techniques*, pp. 1–13, 2016.

Perdisci, R., Corona, I., Dagon, D., and Lee, W., "Detecting malicious flux service networks through passive analysis of recursive dns traces," in "Computer Security Applications Conference, 2009. ACSAC'09. Annual," pp. 311–320, IEEE, 2009.

Phyo, A. and Furnell, S., "A detection-oriented classification of insider it misuse," in "Third Security Conference," Citeseer, 2004.

Plonka, D. and Barford, P., "Context-aware clustering of DNS query traffic," in "Proceedings of the 8th ACM SIGCOMM conference on Internet measurement," pp. 217–230, ACM, 2008.

python, "Python software foundation," , 2016, URL `https://www.python.org/`.

Singh, Y. K., *Fundamental of research methodology and statistics*, New Age International, 2006.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., and Vigna, G., "Your botnet is my botnet: analysis of a botnet takeover," in "Proceedings of the 16th ACM conference on Computer and communications security," pp. 635–647, ACM, 2009.

Symantec, "Internet Security Threat Report 2015 Symantec," , 2015, URL `https://www.symantec.com/security_response/publications/threatreport.jsp`.

Thomas, M. and Mohaisen, A., "Kindred domains: detecting and clustering botnet domains using DNS traffic," in "Proceedings of the 23rd International Conference on World Wide Web," pp. 707–712, ACM, 2014.

WEKA, "WEKA data mining software," , 2016, URL `http://weka.wikispaces.com/ARFF+%28book+version%29`.

Young, W., Memory, A., Goldberg, H., and Senator, T., "Detecting Unknown Insider Threat Scenarios," in "Security and Privacy Workshops (SPW), 2014 IEEE," pp. 277–288, 2014.

Yuchi, X., Wang, X., Lee, X., and Yan, B., "A New Statistical Approach to DNS Traffic Anomaly Detection," pp. 302–313, 2010.

Zhao, G., Xu, K., Xu, L., and Wu, B., "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis," volume 3 pp. 1132–1142, 2015.