REFERENCES

"GeoIP legacy python extension API,," `https://github.com/maxmind/geoip-api-python.`, 2014, [Online; accessed 27-November-2016].

Ayer, V. M., Miguez, S., and Toby, B. H., "Why scientists should learn to program in Python," *Powder Diffraction*, volume 29(S2) pp. S48–S64, 2014.

Bangia, R., *Dictionary of information technology*, Laxmi Publications, Ltd., 2010.

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.

Berkhin, P., "A survey of clustering data mining techniques," in "Grouping multidimensional data," pp. 25–71, Springer, 2006.

Bilge, L., Kirda, E., Kruegel, C., and Balduzzi, M., "EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis." in "NDSS," , 2011.

Brewer, R., "Advanced persistent threats: minimising the damage," *Network Security*, volume 2014(4) pp. 5–9, 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.

Chandola, V., Banerjee, A., and Kumar, V., "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, volume 41(3) p. 15, 2009.

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., and Wirth, R., "CRISP-DM 1.0 Step-by-step data mining guide," , 2000.

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

Dhamija, R., Tygar, J. D., and Hearst, M., "Why phishing works," in "Proceedings of the SIGCHI conference on Human Factors in computing systems," pp. 581–590, ACM, 2006.

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

Ellens, W., Żuraniewski, P., Sperotto, A., Schotanus, H., Mandjes, M., and Meeuwissen, E., "Flow-based detection of DNS tunnels," in "IFIP International Conference on Autonomous Infrastructure, Management and Security," pp. 124–135, Springer, 2013.

Fayyad, U., Piatetsky-Shapiro, G., and Smyth, P., "From data mining to knowledge discovery in databases," *AI magazine*, volume 17(3) p. 37, 1996.

Fombrun, C. J. and Gardberg, N., "Who's tops in corporate reputation?" *Corporate Reputation Review*, volume 3(1) pp. 13–17, 2000.

Friedberg, I., Skopik, F., Settanni, G., and Fiedler, R., "Combating advanced persistent threats: From network event correlation to incident detection," *Computers & Security*, volume 48 pp. 35–57, 2015.

gartner, "5 style apt," *http://www.gartner.com/newsroom/id/2595015*, volume gartner, 2016.

Giura, P. and Wang, W., "Using large scale distributed computing to unveil advanced persistent threats," *Science Journal*, volume 1(3) pp. 93–105, 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.

Jeun, I., Lee, Y., and Won, D., "A practical study on advanced persistent threats," in "Computer applications for security, control and system engineering," pp. 144–152, Springer, 2012.

John, G. H. and Langley, P., "Intelligence, Morgan Kaufmann Publishers, San Mateo," , 1995.

Kim, J., Lee, T., Kim, H.-g., and Park, H., "Detection of advanced persistent threat by analyzing the big data log," *Advanced Science and Technology Letters*, volume 29 pp. 30–36, 2013.

Kurgan, L. A. and Musilek, P., "A survey of Knowledge Discovery and Data Mining process models," *The Knowledge Engineering Review*, volume 21(01) pp. 1–24, 2006.

Legg, P. A., "Visualizing the insider threat: challenges and tools for identifying malicious user activity," in "Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on," pp. 1–7, IEEE, 2015.

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

Li, F., Lai, A., and Ddl, D., "Evidence of Advanced Persistent Threat: A case study of malware for political espionage," in "Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on," pp. 102–109, IEEE, 2011.

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

Loch, K. D., Carr, H. H., and Warkentin, M. E., "Threats to information systems: today's reality, yesterday's understanding," *Mis Quarterly*, pp. 173–186, 1992.

Mandiant, A., "Exposing One of China's Cyber Espionage Units," *available from intelreport. mandiant. com/Mandiant_APT1_Report. pdf*, 2013.

Mandiant, A., "South East Asia," *available from intelreport. mandiant. com/Mandiant_Report. pdf*, 2014.

Manisha, P. L., "Exploring Classification & Clustering Techniques for Predictive Analytics," , 2016.

Marchetti, M., Pierazzi, F., Colajanni, M., and Guido, A., "Analysis of high volumes of network traffic for Advanced Persistent Threat detection," *Computer Networks*, 2016.

Martin, L., "Cyber Kill Chain®," *URL: http://cyber. lockheedmartin. com/hubfs/Gaining_the_Advantage_Cyber_Kill _Chain. pdf*, 2014.

Mierswa, I., "Rapid Miner." *KI*, volume 23(2) pp. 62–63, 2009.

Mikle, O., Slanỳ, K., Veselỳ, J., Janoušek, T., and Surỳ, O., "Detecting hidden anomalies in DNS communication," *Casalicchio E. DNS EASY*, 2011.

Mikut, R. and Reischl, M., "Data mining tools," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, volume 1(5) pp. 431–443, 2011.

Mirkovic, J. and Reiher, P., "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, volume 34(2) pp. 39–53, 2004.

Mockapetris, P. and Dunlap, K. J., *Development of the domain name system*, volume 18, ACM, 1988.

Moon, D., Im, H., Kim, I., and Park, J. H., "DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks," *The Journal of Supercomputing*, pp. 1–15, 2015.

Nainggolan, L., Mahendra, "Classification anomalous DNS traffic at the internet service provider," , 2016.

Nazario, J. and Holz, T., "As the net churns: Fast-flux botnet observations," in "Malicious and Unwanted Software, 2008. MALWARE 2008. 3rd International Conference on," pp. 24–31, IEEE, 2008.

Niyaz, Q., Sun, W., and Javaid, A. Y., "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)," *arXiv preprint arXiv:1611.07400*, 2016.

O'Leary, M., "DNS and BIND," in "Cyber Operations," pp. 139–175, Springer, 2015.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V. et al., "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, volume 12(Oct) pp. 2825–2830, 2011.

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.

Piatetsky-Shapiro, G. and Parker, G., "Lesson: Data mining, and knowledge discovery: An introduction," *Introduction to Data Mining, KD Nuggets*, 2011.

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.

Quinlan, J. R., *C45*, Morgan Kaufmann, 1992.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A., "Insider threat study: Illicit cyber activity in the banking and finance sector," Technical report, DTIC Document, 2005.

Ross, R., "Managing information security risk," *Organization, mission, and information system view. Gaithersburg, MD*, 2011.

Santosa, E., Lim, "Analysis of Educational Institution DNS Network Traffic for Insider Threats," *IC3INA*, 2016.

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

Sites, "List of DNS parameters," *The list*, 2016a.

Sites, T., "Alexa Rank," *The top*, volume 1M, 2016b.

Sood, A. K. and Enbody, R. J., "Targeted cyberattacks: a superset of advanced persistent threats," *IEEE security & privacy*, volume 11(1) pp. 54–61, 2013.

Steinwart, I., Hush, D., and Scovel, C., "A classification framework for anomaly detection," *Journal of Machine Learning Research*, volume 6(Feb) pp. 211–232, 2005.

Sucuri, "SiteChecker," *https://sucuri.net/*, volume gartner, 2016.

Symantec, "Symantec internet security threat report trends for 2016," *Volume*, volume 22 p. 80, 2016.

Tan, P.-N. et al., *Introduction to data mining*, Pearson Education India, 2006.

Tankard, C., "Advanced persistent threats and how to monitor and deter them," *Network security*, volume 2011(8) pp. 16–19, 2011.

Tiwari, D. and Mallick, B., "SVM and Naïve Bayes Network Traffic Classification using Correlation Information," *International Journal of Computer Applications*, volume 147(3), 2016.

Virvilis, N. and Gritzalis, D., "The big four-what we did wrong in advanced persistent threat detection?" in "Availability, Reliability and Security (ARES), 2013 Eighth International Conference on," pp. 248–254, IEEE, 2013.

Vukalović, J. and Delija, D., "Advanced Persistent Threats-detection and defense," in "Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on," pp. 1324–1330, IEEE, 2015.

Wang, Y., Hu, M.-z., Li, B., and Yan, B.-r., "Tracking anomalous behaviors of name servers by mining DNS traffic," in "International Symposium on Parallel and Distributed Processing and Applications," pp. 351–357, Springer, 2006.

Wright, N. F., "DNS in Computer Forensics," *The Journal of Digital Forensics, Security and Law: JDFSL*, volume 7(2) p. 11, 2012.

Yarochkin, F., Kropotov, V., Huang, Y., Ni, G.-K., Kuo, S.-Y., and Chen, Y., "Investigating DNS traffic anomalies for malicious activities," in "Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on," pp. 1–7, IEEE, 2013.

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