**REFERENCES**

[1] CERT Polska Annual Report 2012. http://www.cert.pl/PDF/Report\_CP\_2012.pdf

[2] SOPHOS homepage <http://www.sophos.com>

[3] Cisco Annual Report 2013. http://www.cisco.com/web/about/ac49/ac20/ac19/ar2013/docs/ 2013\_Annual\_Report.pdf

[4] BYOD: Bring Your Own Device. <http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf>

[5] OWASP Top 10 2013. <https://www.owasp.org/index.php/Top_10_2013-Top_10>

[6] NSG. <http://www.ijcst.com/vol31/4/sridevi.pdf>

[7] LESG. http://www.cs.northwestern.edu/∼ychen/Papers/LESG-ICNP07.pdf

[8] A. Shabtai, E. Menahem and Y. Elovici. F-Sign: automatic, function-based signature generation for malware, systems, man, and cybernetics, Part C: applications and reviews. Transactions on IEEE, 41, 494–508, 2011.

[9] D. Kong, J. Gong, S. Zhu, P. Liu and H. Xi. SAS: semantics aware signature generation for polymorphic worm detection. International Journal of Information Security, 50, 1–19, 2011.

[10] M. Sharma and D. Toshniwal. Pre-clustering algorithm for anomaly detection and clustering that uses variable size buckets. RecentAdvances in Information Technology, 515–519, 2012.

[11] M. H. A. C. Adaniya, M. F. Lima, J. J. P. C. Rodrigues, T. Abrao and M. L. Proenca. Anomaly detection using DSNS and FireflyHarmonic Clustering Algorithm. Communications (ICC), 1183–1187, 2012.

[12] J. Mazel, P. Casas, Y. Labit and P. Owezarski. Sub-space clustering, Inter-Clustering Results Association and anomaly correlation for unsupervised network anomaly detection. Network and Service Management (CNSM), 1–8, 24–28 October 2011.

[13] Kaspersky Lab. Security report. http://www.securelist.com/en/analysis/204792244/Thegeography-of-cybercrime-Western-Europe-and-North-America

[14] ESET threat report 12-2012. http://go.eset.com/us/resources/threat-trends/Global-ThreatTrends-November-2012.pdf

[15] F. Felzenszwalb and P. Huttenlocher. Efficient graph-based image segmentation. International Journal of Computer Vision, 59, 167–181, September 2004.

[16] B. Needleman Saul and D. Wunsch Christian A general method applicable to the search for similarities in the amino acid sequence of two proteins. Journal of Molecular Biology, 48, 443–453, 1970.

[17] CSIC 2010 HTTP Dataset in CSV format. [http://users.aber.ac.uk/pds7/csic\_dataset/csic 2010http.html](http://users.aber.ac.uk/pds7/csic_dataset/csic%202010http.html)

[18] Z. Zhang, J. Li , C. Manikopoulos, J. Jorgenson and J. Ucles. HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. In Proceeding of IEEE Workshop on Information Assurance and Security, 2001.

[19] Adetunmbi Adebayo O., Falaki Samuel O., Adewale Olumide S. and K. Boniface. Network intrusion detection based on rough set and k-nearest neighbour. International Journal of Computing and ICT Research, 2, 60–66, 2008. Downloaded from https://academic.oup.com/jigpal/article-abstract/23/1/45/2893005 by Open University of Hong Kong user on 23 January 2019[11:10 30/12/2014 jzu038.tex] Paper Size: a4 paper Job: JIGPAL Page: 56 45–56 56 Machine learning techniques to detect cyber attacks

[20] J. Ma and G. ZhongXu. Network anomaly detection using dissimilarity-based one-class SVM classifier. ICPPW ’09. International Conference on Parallel Processing Workshops, 2009, 409–414, 22–25 September 2009.

[21] M. Zmyslony, B. Krawczyk and M. Wozniak. Combined classifiers with neural fuser for spam detection. In: Herrero A. et al. (eds.), Advances in Intelligent Systems and Computing, Vol. 189, 245–252, Springer, 2012.

[22] L. Feinstein, D. Schnackenberg, R. Balupari and D. Kindred. Statistical approaches to DDoS attack detection and response. In Proceedings DARPA Information Survivability Conference and Exposition, 2003, 1, 303–314, 2003.

[23] M. Chora´s, L. Saganowski, R. Renk and W. Hołubowicz. Statistical and signal-based network traffic recognition for anomaly detection. Expert Systems, 29, 232–245, 2012.

[24] Y. Xie and S. Z. Yu. A novel model for detecting application layer DDoS attacks. In IMSCCS ’06: Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences Vol. 2 (IMSCCS’06). Washington, DC, USA: IEEE Computer Society, pp. 56–63, 2006.

[25] Y. Qiao, X. W. Xin, Y. Bin and S. Ge. Anomaly intrusion detection method based on HMM. Electronics Letters, 38, 663–664, 2002.

[26] R. Vijayasarathy, S. V. Raghavan and B. Ravindran. A system approach to network modeling for DDoS detection using a Naive Bayesian classifier, Communication Systems and Networks (COMSNETS), 2011 Third International Conference on, pp. 1–10, 4–8 Jan. 2011.

[27] W. Hu, Y. Liao and V. R. Vemuri. Robust anomaly detection using support vector machines. In Proceedings of International Conference on Machine Learning, 2003.

[28] P. Barthakur, M. Dahal and M. K. Ghose. A Framework for P2P Botnet Detection Using SVM. 2012 International Conference, Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) pp.195–200, 10–12 October 2012.

[29] W. Li. Using genetic algorithm for network intrusion detection. C. S. G. Department of Energy, Ed., pp. 1–8, 2004.

[30] M. Chora´s, R. Kozik, D. Puchalski and W. Hołubowicz. Correlation approach for SQL injection attacks detection. In: Herrero A. et al (eds.), Advances in Intelligent and Soft Computing, 189, 177–186, Springer, 2012. [31] H. Nguyen, C. Torrano-Gimenez, G. Álvarez, S. Petrovic and K. Franke. Application of the generic feature selection measure in detection of web attacks. In Proceedings of International Workshop in Computational Intelligence in Security for Information Systems (CISIS 11), LNCS 6694, pp. 25–32, 2011