Daftar Pustaka

Abijah Roseline, S., Geetha, S., Kadry, S. and Nam, Y. (2020), 'Intelligent Vision-based Malware Detection and Classification using Deep Random Forest Paradigm', *IEEE Access* pp. 1–1.

Chen, C. W., Su, C. H., Lee, K. W. and Bair, P. H. (2020), 'Malware Family Classification using Active Learning by Learning', *International Conference on Advanced Communication Technology, ICACT* **2020**, 590–595.

Chumachenko, K. (2017), 'Machine Learning Methods for Malware Detection and Classification', *Proceedings of the 21st Pan-Hellenic Conference on Informatics - PCI 2017* p. 93.

Das, S., Liu, Y., Zhang, W. and Chandramohan, M. (2016), 'Semantics-based online malware detection: Towards efficient real-time protection against malware', *IEEE Transactions on Information Forensics and Security* **11**(2), 289–302.

Han, X., Jin, F., Wang, R., Wang, S. and Yuan, Y. (2021), 'Classification of malware for self-driving systems', *Neurocomputing* **428**, 352–360.

Kim, D., Woo, S., Lee, D. and Chung, T. (2016), Static detection of malware and benign executable using machine learning algorithm, *in* 'INTERNET 2016: The Eighth International Conference on Evolving Internet', pp. 14–19.

Liu, L., sheng Wang, B., Yu, B. and xi Zhong, Q. (2017), 'Automatic malware classification and new malware detection using machine learning', *Frontiers of Information Technology and Electronic Engineering* **18**(9), 1336–1347.

Liu, Y. S., Lai, Y. K., Wang, Z. H. and Yan, H. B. (2019), 'A New Learning Approach to Malware Classification Using Discriminative Feature Extraction', *IEEE Access* **7**(c), 13015–13023.

Mangialardo, R. J. and Duarte, J. C. (2015), 'Integrating static and dynamic malware analysis using machine learning', *IEEE Latin America Transactions* **13**(9), 3080–3087.

Nataraj, L., Karthikeyan, S., Jacob, G. and Manjunath, B. S. (2011), Malware images: visualization and automatic classification, *in* 'Proceedings of the 8th international symposium on visualization for cyber security', pp. 1–7.

Oh, S., Go, W. and Lee, T. (2017), A study on the behavior-based malware detection signature, *in* 'Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 11th International Conference On Broad-Band Wireless Computing, Communication and Applications (BWCCA–2016) November 5–7, 2016, Korea', Springer, pp. 663–670.

Pai, S., Troia, F. D., Visaggio, C. A., Austin, T. H. and Stamp, M. (2017), 'Clustering for malware classification', *Journal of Computer Virology and Hacking Techniques* **13**(2), 95–107.

Radwan, A. M. (2019), Machine learning techniques to detect maliciousness of portable executable files, *in* '2019 International Conference on Promising Electronic Technologies (ICPET)', IEEE, pp. 86–90.

Rezaei, T., Manavi, F. and Hamzeh, A. (2021), 'A pe header-based method for malware detection using clustering and deep embedding techniques', *Journal of Information Security and Applications* **60**, 102876.

Sahu, M. K., Ahirwar, M. and Shukla, P. K. (2015), Improved malware detection technique using ensemble based classifier and graph theory, *in* '2015 IEEE International Conference on Computational Intelligence & Communication Technology', IEEE, pp. 150–154.

Shafiq, M. Z., Tabish, S. and Farooq, M. (2009), Pe-probe: leveraging packer detection and structural information to detect malicious portable executables, *in* 'Proceedings of the Virus Bulletin Conference (VB)', Vol. 8.

Shafiq, M. Z., Tabish, S. M., Mirza, F. and Farooq, M. (2009), 'PE-Miner : Mining Structural Information to Detect Malicious Executables in Realtime Agenda Introduc1on to Domain Problem Defini1on Proposed Solu1on', pp. 121–141.
URL: *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.663.7013&rep=rep1&type=*

Udayakumar, N., Saglani, V. J., Cupta, A. V. and Subbulakshmi, T. (2018), 'Malware Classification Using Machine Learning Algorithms', *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018* pp. 1007–1012.

Vyas, R., Luo, X., McFarland, N. and Justice, C. (2017), Investigation of malicious portable executable file detection on the network using supervised

learning techniques, *in* '2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)', IEEE, pp. 941–946.

Wuechner, T., Cisłak, A., Ochoa, M. and Pretschner, A. (2017), 'Leveraging compression-based graph mining for behavior-based malware detection', *IEEE Transactions on Dependable and Secure Computing* **16**(1), 99–112.

Xia, S., Pan, Z., Chen, Z., Bai, W. and Yang, H. (2018), Malware classification with markov transition field encoded images, *in* '2018 Eighth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)', IEEE, pp. 1–5.

Xue, D., Li, J., Lv, T., Wu, W. and Wang, J. (2019), 'Malware classification using probability scoring and machine learning', *IEEE Access* **7**, 91641–91656.