DAFTAR PUSTAKA

[1] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, and M. Rajarajan, "Android security: A survey of issues, malware penetration, and defenses," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 998–1022, 2015.

[2] AV-TEST Institute, "Malware Statistics & Trends Report," https://www.av-test.org/en/statistics/malware/, 2024, accessed: December 2024.

[3] X. Ugarte-Pedrero, I. Santos, I. García-Ferreira, S. Huerta, B. Sanz, and P. G. Bringas, "On the adoption of anomaly detection for packed executable filtering," *Computers & Security*, vol. 43, pp. 126–144, 2014.

[4] J. Z. Kolter and M. A. Maloof, "Learning to detect malicious executables in the wild," in *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '04, 2004, pp. 470–478.

[5] D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," *Computers & Security*, vol. 81, pp. 123–147, 2019.

[6] D. Gibert, C. Mateu, and J. Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," *Journal of Network and Computer Applications*, vol. 153, p. 102526, 2020.

[7] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[8] V. Vapnik, *The Nature of Statistical Learning Theory*. New York: Springer, 1999.

[9] B. Schölkopf and A. J. Smola, *Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond*. The MIT Press, 2001.

[10] J. Saxe and K. Berlin, "Deep neural network based malware detection using two dimensional binary program features," in *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, 2015, pp. 11–20.

[11] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ: Wiley-Interscience, 2006.

[13] R. Lyda and J. Hamrock, "Using entropy analysis to find encrypted and packed malware," *IEEE Security & Privacy*, vol. 5, no. 2, pp. 40–45, 2007.

[14] E. Raff, J. Sylvester, and C. Nicholas, "Learning the pe header, malware detection with minimal domain knowledge," in *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*, ser. AISec '17, 2017, pp. 121–132.

[15] E. Raff, J. Barker, J. Sylvester, R. Brandon, B. Catanzaro, and C. K. Nicholas, "Malware detection by eating a whole exe," in *AAAI Workshops*, 2017.

[16] M. Z. Shafiq, S. M. Tabish, F. Mirza, and M. Farooq, "Pe-miner: Mining structural information to detect malicious executables in realtime," in *Recent Advances in Intrusion Detection*. Springer Berlin Heidelberg, 2009, pp. 121–141.

[17] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon, and K. Rieck, "Drebin: Effective and explainable detection of android malware in your pocket," in *Network and Distributed System Security Symposium*, 2014.

[18] H. Oz, G. S. Tuncay, A. Aris, A. Kharraz, and S. Uluagac, "Beyond the upload button: A 10-year retrospective on security issues within file upload," *IEEE Communications Magazine*, vol. 63, no. 2, pp. 104–110, 2025.

[19] abuse.ch, "MalwareBazaar: Malware Sample Exchange," https://bazaar.abuse.ch/, 2020, accessed: December 2024.

[20] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[21] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '16, 2016, pp. 785–794.

[22] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. The MIT Press, 2016.

[23] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Information Processing & Management*, vol. 45, no. 4, pp. 427–437, 2009.

[24] D. M. W. Powers, "Evaluation: From precision, recall and f-measure to roc, informedness, markedness and correlation," *Journal of Machine Learning Technologies*, vol. 2, no. 1, pp. 37–63, 2011.

[25] M. Ahmadi, D. Ulyanov, S. Semenov, M. Trofimov, and G. Giacinto, "Novel feature extraction, selection and fusion for effective malware family classification,"

in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '16, 2016, pp. 183–194.

[26] H. S. Anderson and P. Roth, "Ember: An open dataset for training static pe malware machine learning models," *arXiv preprint arXiv:1804.04637*, 2018. [Online]. Available: https://arxiv.org/abs/1804.04637

[27] A. Kumar, K. S. Kuppusamy, and G. Aghila, "A learning model to detect maliciousness of portable executable using integrated feature set," *Journal of King Saud University – Computer and Information Sciences*, vol. 31, no. 2, pp. 252–265, 2019.

[28] M. S. Akhtar and T. Feng, "Malware analysis and detection using machine learning algorithms," *Symmetry*, vol. 14, no. 11, p. 2304, 2022.

[29] C. Connors and D. Sarkar, "Machine learning for detecting malware in pe files," *arXiv preprint arXiv:2212.13988*, 2022. [Online]. Available: https://arxiv.org/abs/2212.13988

[30] C.-C. Chang and C.-J. Lin, "Libsvm: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, no. 3, 2011.

[31] C.-W. Hsu, C.-C. Chang, and C.-J. Lin, "A practical guide to support vector classification," Department of Computer Science, National Taiwan University, Tech. Rep., 2003.

[32] N.-T. Chau and S. Jung, "An entropy-based solution for identifying android packers," *IEEE Access*, vol. 7, pp. 28 412–28 421, 2019.

[33] M. Bat-Erdene, H. Park, H. Li, H. Lee, and M.-S. Choi, "Entropy analysis to classify unknown packing algorithms for malware detection," *International Journal of Information Security*, vol. 16, pp. 227–248, 2017.

[34] M. C. Amirani, M. Toorani, and A. Beheshti, "A new approach to content-based file type detection," in *2008 IEEE Symposium on Computers and Communications*, 2008, pp. 1103–1108.

[35] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images: visualization and automatic classification," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11. Association for Computing Machinery, 2011.

[36] M. Mimura, "Evaluation of printable character-based malicious pe file-detection method," *Internet of Things*, vol. 19, p. 100521, 2022.

[37] S. M. Tabish, M. Z. Shafiq, and M. Farooq, "Malware detection using statistical analysis of byte-level file content," in *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics*, ser. CSI-KDD '09. Association for Computing Machinery, 2009, pp. 23–31.

[38] Microsoft, "PE Format," https://learn.microsoft.com/en-us/windows/win32/debug/pe-format, 2024, accessed: December 2024.

[39] TIS Committee, "Tool Interface Standard (TIS) Executable and Linking Format (ELF) Specification Version 1.2," TIS Committee, Tech. Rep., 1995. [Online]. Available: https://refspecs.linuxfoundation.org/elf/elf.pdf

[40] Apple Inc., "Mach-O Programming Topics," https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/MachOTopics/, 2024, accessed: December 2024.

[41] J. H. Friedman, "Greedy function approximation: A gradient boosting machine," *The Annals of Statistics*, vol. 29, no. 5, pp. 1189–1232, 2001. [Online]. Available: http://www.jstor.org/stable/2699986

[42] W. Hu and Y. Tan, "Black-box attacks against rnn based malware detection algorithms," in *AAAI Workshops*, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:1044188

[43] G. J. Myers, C. Sandler, and T. Badgett, *The Art of Software Testing*, 3rd ed. John Wiley & Sons, 2011.

[44] M. Fowler, *UML Distilled: A Brief Guide to the Standard Object Modeling Language*, 3rd ed. Addison-Wesley Professional, 2003.

[45] P. P.-S. Chen, "The Entity-Relationship Model—Toward a Unified View of Data," *ACM Transactions on Database Systems*, vol. 1, no. 1, pp. 9–36, 1976.

[46] J. J. Garrett, *The Elements of User Experience: User-Centered Design for the Web and Beyond*, 2nd ed. New Riders, 2011.

[47] P. Chapman, J. Clinton, R. Kerber, T. Khabaza, T. Reinartz, C. Shearer, and R. Würth, "Crisp-dm 1.0: Step-by-step data mining guide," SPSS Inc., Tech. Rep., 2000.

[48] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, 2nd ed., ser. Springer Series in Statistics. Springer, 2009.

[49] A. Gholamy, V. Kreinovich, and O. Kosheleva, "Why 70/30 or 80/20 relation between training and testing sets: A pedagogical explanation," Department of Computer Science, University of Texas at El Paso, Tech. Rep. 1209, 2018. [Online]. Available: https://scholarworks.utep.edu/cs_techrep/1209/

[50] V. R. Joseph, "Optimal ratio for data splitting," *Statistical Analysis and Data Mining: The ASA Data Science Journal*, vol. 15, no. 4, pp. 531–538, 2022.

[51] R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," in *Proceedings of the 14th International Joint Conference on Artificial Intelligence*, vol. 14, no. 2, 1995, pp. 1137–1145.

[52] FIRST.Org, Inc., "Common Vulnerability Scoring System v3.1: Specification Document," https://www.first.org/cvss/v3-1/specification-document, 2019, forum of Incident Response and Security Teams.

[53] Joint Task Force Transformation Initiative, "Guide for Conducting Risk Assessments," National Institute of Standards and Technology, Tech. Rep. SP 800-30 Rev. 1, 2012.

[54] J. Platt, "Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods," in *Advances in Large Margin Classifiers*. MIT Press, 1999, pp. 61–74.