DAFTAR PUSTAKA

[1] Carrier, T. (2021, December 1). *Detecting obfuscated malware using memory feature engineering*. UNB Scholar Research Repository. https://unbscholar.lib.unb.ca/handle/1882/37374

[2] Alrayes, F. S., Zakariah, M., Driss, M., & Boulila, W. (2023). Deep Neural Decision Forest (DNDF): A novel approach for enhancing intrusion detection systems in network traffic analysis. Sensors, 23(20), 8362. https://doi.org/10.3390/s23208362

[3] Kaliappan, J., Bagepalli, A. R., Almal, S., Mishra, R., Hu, Y.-C., & Srinivasan, K. (2023). Impact of cross-validation on machine learning models for early detection of intrauterine fetal demise. Diagnostics, 13(10), 1692. https://doi.org/10.3390/diagnostics13101692

[4] Farhangi, F., Sadeghi-Niaraki, A., Razavi-Termeh, S. V., & Choi, S.-M. (2021). Evaluation of tree-based machine learning algorithms for accident risk mapping caused by driver lack of alertness at a national scale. Sustainability, 13(18), 10239. https://doi.org/10.3390/su131810239

[5] Talukder, S., & Talukder, Z. (2020). *A survey on malware detection and Analysis Tools*. International Journal of Network Security & Its Applications, 12(2), 37–57. https://doi.org/10.5121/ijnsa.2020.12203

[6] Alani, M. M., Mashatan, A., & Miri, A. (2023). *XMal: A lightweight memory-based explainable obfuscated-malware detector*. Computers Security, 133, 103409. https://doi.org/10.1016/j.cose.2023.103409

[7] Brewer, R. (2016). *Ransomware attacks: Detection, prevention and cure. Network Security*, 2016(9), 5–9. https://doi.org/10.1016/s1353-4858(16)30086-1

[8] *Zeus malware:variants,methods and history*, https://www.cynet.com/networkattacks/zeus-malware-variants-methods-and-history/ , 2021, (Diakses pada 18/11/2023).

[9] Grammatikakis, K. P., Koufos, I., Kolokotronis, N., Vassilakis, C., & Shiaeles, S. (2021). *Understanding and mitigating banking trojans: From zeus to emotet*.

2021 IEEE International Conference on Cyber Security and Resilience (CSR). https://doi.org/10.1109/csr51186.2021.9527960

[10] Morales, J. A., Al-Bataineh, A., Xu, S., & Sandhu, R. (2010). *Analyzing and exploiting network behaviors of malware*. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 20–34. https://doi.org/10.1007/978-3-642-16161-2_2

[11] Rhode, M., Burnap, P., & Jones, K. (2018). *Early-stage malware prediction using recurrent neural networks*. Computers & Security, 77, 578–594. https://doi.org/10.1016/j.cose.2018.05.010

[12] Trojan.win32.reconycl, https://www.trendmicro.com/vinfo/us/threatencyclopedia/malware/trojan.win32.reconyc.afjl , (Diakses pada 18/11/2023).

[13] Akhtar, Z. (2021). Malware Detection and Analysis: Challenges and Research Opportunities. https://doi.org/10.48550/arXiv.2101.08429

[14]] Threats of computing in a virus-filled world, https://ewh.ieee.org/r4/iail/OctPresentation-ProtectingPC.ppt , (Diakses pada 18/11/2023).

[15] What to know about spyware - software tested, https://softwaretested.com/malware/what-is-spyware/ , (Diakses pada 18/11/2023).

[16] Umar, R., Riadi, I., & Kusuma, R. S. (2021). Analysis of conti ransomware attack on computer network with live forensic method. IJID (International Journal on Informatics for Development), 10(1), 53–61. https://doi.org/10.14421/ijid.2021.2423

[17] Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. International Journal of Computer Science and Network Security, 19(2), 136.

[18] Suzuki, Y. E., & Monroy, S. A. (2021). Prevention and mitigation measures against phishing emails: A sequential schema model. Security Journal, 35(4), 1162–1182. https://doi.org/10.1057/s41284-021-00318-x

[19] Atapour-Abarghouei, A., McGough, A. S., & Wall, D. S. (2020). Resolving the cybersecurity data sharing paradox to scale up cybersecurity via a

co-production approach towards Data Sharing. 2020 IEEE International Conference on Big Data (Big Data). https://doi.org/10.1109/bigdata50022.2020.9378014

[20] Poudyal, S., & Dasgupta, D. (2021). Analysis of crypto-ransomware using ML-based multi-level profiling. IEEE Access, 9, 122532–122547. https://doi.org/10.1109/access.2021.3109260

[21] Alrayes, F. S., Zakariah, M., Driss, M., & Boulila, W. (2023). Deep Neural Decision Forest (DNDF): A novel approach for enhancing intrusion detection systems in network traffic analysis. Sensors, 23(20), 8362. https://doi.org/10.3390/s23208362

[22] Louk, M. H., & Tama, B. A. (2022). Tree-based classifier ensembles for PE malware analysis: A performance revisit. Algorithms, 15(9), 332. https://doi.org/10.3390/a15090332

[23] Dener, M., Ok, G., & Orman, A. (2022). Malware detection using memory analysis data in Big Data Environment. Applied Sciences, 12(17), 8604. https://doi.org/10.3390/app12178604

[24] Roy, K. S., Ahmed, T., Udas, P. B., Karim, Md. E., & Majumdar, S. (2023). MalHyStack: A hybrid stacked ensemble learning framework with feature engineering schemes for obfuscated malware analysis. Intelligent Systems with Applications, 20, 200283. https://doi.org/10.1016/j.iswa.2023.200283

[25] Talukder, Md. A., Hasan, K. F., Islam, Md. M., Uddin, Md. A., Akhter, A., Yousuf, M. A., Alharbi, F., & Moni, M. A. (2023). A dependable hybrid machine learning model for network intrusion detection. Journal of Information Security and Applications, 72, 103405. https://doi.org/10.1016/j.jisa.2022.103405

[26] Mezina, A., & Burget, R. (2022). Obfuscated malware detection using dilated Convolutional Network. 2022 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). https://doi.org/10.1109/icumt57764.2022.9943443

[27] Naeem, H., Dong, S., Falana, O. J., & Ullah, F. (2023). Development of a deep stacked ensemble with process based volatile memory forensics for platform independent malware detection and classification. Expert Systems with Applications, 223, 119952. https://doi.org/10.1016/j.eswa.2023.119952

[28] Gorment, N. Z., Selamat, A., & Krejcar, O. (2023). Obfuscated malware detection: Impacts on detection methods. Recent Challenges in Intelligent Information and Database Systems, 55–66. https://doi.org/10.1007/978-3-031-42430-4_5