REFERENCES

[1] A. Arabo, R. Dijoux, T. Poulain and G. Chevalier, "Detecting Ransomware Using Process Behavior Analysis," *Procedia Computer Science,* pp. 290-296, 2020.

[2] K. Thummapudi, P. Lama and R. V. Boppana, "Detection of ransomware attacks using processor and disk usage data," *IEEE,* pp. 51395 - 51407, 2023.

[3] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights,* vol. 1, 2021.

[4] N. Hampton, Z. Baig and S. Zeadally, "Ransomware behavioural analysis on windows platforms," *Journal of Information Security and Applications,* vol. 40, pp. 44-51, 2018.

[5] D. W. Fernando, N. Komninos and T. Chen, "A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques," *Lecture notes in computer science,* vol. 1, no. 2, pp. 551-604, 2020.

[6] S. Zollner and K.-K. R. Choo, "An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems," *IEEE Access,* vol. 7, pp. 158250-158263, 2019.

[7] M. . E. Russinovich, D. A. Solomon and A. Ionescu, Windows Internals Part 2, Redmond: Microsoft Press, 2012.

[8] L. Chappell, Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide, Carmel: Chappell University, 2017.

[9] C. Miess, "ProcDot: The Malware Analysis Tool," CERT.at, 05 April 2013. [Online]. Available: https://www.procdot.com. [Accessed 10 Januari 2024].

[10] K. K. Z. M. W. &. M. W. Cabaj, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," *Journal of Network and Computer Applications,* vol. 66, pp. 353-368, 2018.

[11] BBC News Indonesia, "BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank 'tidak kuat'," BBC News Indonesia, 16 Mei 2023. [Online]. Available: https://www.bbc.com/indonesia/articles/cn01gdr7eero. [Accessed 08 Januari 2024].

[12] H. Daku, P. Zavarsky and Y. Malik, "Behavioral-Based Classification and Identification of Ransomware Variants Using Machine Learning," *IEEE Access,* 2018.

[13] T. R. McIntosh, J. Jang-Jaccard and P. A. Watters, "Large Scale Behavioral Analysis of Ransomware Attacks," *Proceedings of the International Conference on Neural Information Processing,* vol. 11306, p. 217–229, 2018.

[14] Y. Lemmou and J. Lanet, "A behavioural in-depth analysis of ransomware infection," *IET Information Security,* vol. 15, no. 1, pp. 38-58, 2020.

[15] F. De Gaspari and D. Hitaj, "Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques," *Neural Computing and Applications,* vol. 34, no. 14, pp. 12077-12096, 2022.

[16] M. A. Ferrag, O. Friha and L. Maglaras, "Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis," *IEEE Access,* vol. 9, pp. 138509-138542, 2021.

[17] S. Gulmez, A. G. Kakisim and I. Sogukpinar, "Analysis of the Dynamic Features on Ransomware Detection Using Deep Learning-based Methods," *IEEE Access,* 2023.

[18] G. Karantzas and C. Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors," *Journal of Cybersecurity and Privacy,* vol. 1, no. 3, pp. 387-421, 2021.

[19] Z.-G. Chen, H.-S. Kang, S.-N. Yin and S.-R. Kim, "Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph," *Proceedings of the International Conference on Research in Adaptive and Convergent Systems,* vol. 196 , pp. 196-201, 2017.

[20] S. Jamalpur, Y. S. Navya, P. Raja, G. Tagore and . G. R. K. Rao, "Dynamic Malware Analysis Using Cuckoo Sandbox," *IEEE Access,* 2018.

[21] "Sysmon - System Monitor," Microsoft Docs., 23 07 2024. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.. [Accessed 15 08 2024].

[22] "Tcpdump/Libpcap public repository," Tcpdump, [Online]. Available: https://www.tcpdump.org/. [Accessed 15 08 2024].

[23] "The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community," Volatility, [Online]. Available: https://www.volatilityfoundation.org/. [Accessed 15 08 2024].

[24] J. A. H. Silva, L. I. B. López and Á. L. V. Caraguay, "A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters," *Remote Sens,* vol. 11, no. 10, p. 1168, 2019.

[25] D. Kirat, G. Vigna and C. Kruegel, "Barecloud: bare-metal analysis-based evasive malware detection," *USENIX Security Symposium,* pp. 287 - 301, 2014.