DAFTAR PUSTAKA

Abraham, B., Mandya, A., Bapat, R., Alali, F., Brown, D. E., & Veeraraghavan, M. (2018). A Comparison of Machine Learning Approaches to Detect Botnet Traffic. *International Joint Conference on Neural Networks (IJCNN), 2018–July*, 1–8. https://doi.org/10.1109/IJCNN.2018.8489096

Alejandre, F. V., Cortés, N. C., & Anaya, E. A. (2017). Feature selection to detect botnets using machine learning algorithms. *2017 International Conference on Electronics, Communications and Computers, CONIELECOMP 2017*. https://doi.org/10.1109/CONIELECOMP.2017.7891834

Andrews, S. (2018). McAfee Labs Threats Report, *8*(March), 1–19. https://doi.org/10.1177/0011128701047003005

Angrishi, K. (2017). Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets, 1–17. https://doi.org/10.1111/j.1468-0017.2004.00251.x

Antonakakis, M., April, T., Bailey, M., Bursztein, E., Cochran, J., Durumeric, Z., … Yi Zhou, B. (2017). Understanding the Mirai Botnet Manos. *Advanced Computing Systems Association (USENIX)*. Retrieved from https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Bastos, D., Shackleton, M., & El-Moussa, F. (2018). Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. *BT Research and Innovation*, 30 (7 pp.)-30 (7 pp.). https://doi.org/10.1049/cp.2018.0030

De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Security and Communication Networks*, *2018*, 1–30. https://doi.org/10.1155/2018/7178164

Fibrianda, M. F., & Bhawiyuga, A. 2018. Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer 2: 3112-3123.

Hairani, T. (2018). Deteksi Botnet Menggunakan Algoritma K-Nearest Neighbor.

Han, J., & Kamber , M. 2006. Data Mining: Concept and Techniques. New York: Morgan Kaufmann Publisher.

Ismiyushar, N. A., Kurniawan, M. T., & Widjajarto, A. (2018). Analisis Dampak Malware Berdasarkan Api Call Dengan Metode Anomali, *5*(2), 3084–3093.

Limantara, A. D., Cahyo, Y., Purnomo, S., & Mudjanarko, S. W. (2017). Pemodelan Sistem Pelacakan LOT Parkir Kosong Berbasis Sensor Ultrasonic Dan Internet Of Things (IOT) Pada Lahan Parkir Diluar Jalan. *Seminar Nasional Sains Dan Teknologi*, *1*(2), 1–10.

Nomm, S., & Bahsi, H. (2018). Unsupervised Anomaly Based Botnet Detection in IoT Networks. *International Conference on Machine Learning and Applications (ICMLA)*, 1048–1053. https://doi.org/10.1109/ICMLA.2018.00171

Sinanovic, H., & Mrdovic, S. (2017). Analysis of Mirai malicious software. *International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. https://doi.org/10.23919/SOFTCOM.2017.8115504

Wibowo, A. T., Saikhu, A., & Soelaiman, R. (2016). *Implementasi Algoritma Deteksi SPAM yang Tersisipi Informasi Citra dengan Metode SVM dan Random Forest*.