DAFTAR PUSTAKA

Aycock, J. (2006). *Computer Viruses and Malware*. Canada: Springer.

Bayer, U., Comparetti, P. M., Hlauschek, C., Kruegel, C., & Kirda, E. (2009). 2009__Scalable, Behavior-Based Malware Clustering, 2009.pdf. *Secure Systems Lab*.

Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. *Justindo*, *2*(1), 19–30.

Jacob, G., Debar, H., & Filiol, E. (2008). Behavioral detection of malware: From a survey towards an established taxonomy. *Journal in Computer Virology*, *4*(3), 251–266. https://doi.org/10.1007/s11416-008-0086-0

Jain, M., & Bajaj, P. (2014). Techniques in Detection and Analyzing Malware Executables: A Review. *International Journal of Computer Science and Mobile Computing*, *35*(5), 930–935.

Jonker, J., & Pennink, B. (2009). The Essence of Research Methodology. In *The Essence of Research Methodology: A Concise Guide for Master and PhD Students in Management Science*. https://doi.org/10.1007/978-3-540-71659-4

Kim, Y. S., Wang, E., & Rho, H. M. (2001). Geometry-based machining precedence reasoning for feature-based process planning. *International Journal of Production Research*, *39*(10), 2077–2103. https://doi.org/10.1109/ACCESS.2018.2805301

Liu, W., Ren, P., Liu, K., & Duan, H. X. (2011). Behavior-based malware analysis and detection. *Proceedings - 2011 1st International Workshop on Complexity and Data Mining, IWCDM 2011*. https://doi.org/10.1109/IWCDM.2011.17

Maheswaran, M., & Krauter, K. (2001). A parameter-based approach to resource discovery in grid computing systems. *Grid Computing - Grid 2000*,

Proceedings, *1971*(April), 181–190. https://doi.org/10.1007/3-540-44444-0_17

Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to malware incident prevention and handling recommendations of the national institute of standards and technology. *Nist Special Publication 800-83*, 101.

Merialdo, G. (2012). Medusa. *Revista Medica de Homeopatia*, *5*(2), 61–62. https://doi.org/10.1016/S1888-8526(12)70139-X

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*, *50 LNICST*, 20–34. https://doi.org/10.1007/978-3-642-16161-2_2

Orebaugh, A., Ramirez, G., Burke, J., Pesce, L., Wright, J., & Morris, G. (2006). Wireshark & Ethereal Network Protocol Analyzer Toolkit. In *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. https://doi.org/10.1016/B978-159749073-3/50006-3

Perdisci, Roberto and Lee, Wenke and Feamster, N. (2010). Behavioral clustering of HTTP-based malware and signature generation using malicious network traces. *7th USENIX Conference on Networked Systems Design and Implementation*, 26--26. https://doi.org/10.1007/BF00386413

Sherlock, P., & Phill, S. (2015). *How Did That Happen ?: Practical Techniques for Analyzing Suspicious Traffic Phill " Sherlock " Shade*.

Shijo, P. V., & Salim, A. (2015). Integrated static and dynamic analysis for malware detection. *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2015.02.149

Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. *Computers & Security*. https://doi.org/10.1016/j.cose.2012.05.004

Uppal, D., Mehra, V., & Verma, V. (2014). Basic survey on Malware Analysis, Tools and Techniques. *International Journal on Computational Science & Applications*. https://doi.org/10.5121/ijcsa.2014.4110

Villeneuve, N., & Bennett, J. (2012). Detecting APT Activity with Network Traffic Analysis. *Trend Micro Incorporated*, 15. Retrieved from http://www.trendmicro.pl/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

Ismail, J. (2016, February 29). *Analisa Malware Metode Statik*. Dipetik September 26, 2018, dari https://julismail.staff.telkomuniversity.ac.id/analisa-malware-metode-statik/

Utama, W. (2017, May 28). *Apa Itu Malware, Pengertian, Penjelasan dan Jenis Malware yang Perlu Diwaspadai*. Dipetik December 3, 2018, dari Klik Mania: https://www.klikmania.net/apa-itu-malware

Webi. (2018, May 31). *Windows API Index*. Dipetik December 4, 2018, dari Microsoft Docs: https://docs.microsoft.com/en-us/windows/desktop/apiindex/windows-api-list#networking-and-internet