DAFTAR PUSTAKA

Alazab, M. (2015). Profiling and classifying the behavior of malicious codes. *Journal of Systems and Software, 100,* 91-102. Diakses pada 15 Juni, 2019, diambil dari https://www.sciencedirect.com/science/article/pii/S0164121214002283.

Aman, W. (2014). A Framework for Analysis and Comparison of Dynamic Malware Analysis Tools. *International Journal of Network Security & Its Applications,6*(5), 63-74. Diakses pada July 2, 2019, diambil dari https://arxiv.org/abs/1410.2131.

Arbez, G., & Birta, L. G. (2016). A tutorial on ABCmod: An Activity Based discrete event Conceptual modelling framework. *2016 Winter Simulation Conference (WSC)*. Diakses pada 1 Oktober, 2018, diambil dari https://ieeexplore.ieee.org/document/7822082.

Aslan, O., & Samet, R. (2017). Investigation of Possibilities to Detect Malware Using Existing Tools. *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*. Diakses pada 10 Juni, 2019, diambil dari https://ieeexplore.ieee.org/document/8308437.

Bailey, M., Oberheide, J., Andersen, J., Mao, Z. M., Jahanian, F., & Nazario, J. (2007, September 05). Automated Classification and Analysis of Internet Malware. Diakses pada 9 Juni, 2019, diambil dari https://link.springer.com/chapter/10.1007/978-3-540-74320-0_10.

Bazrafshan, Z., Hashemi, H., Fard, S. M., & Hamzeh, A. (2013). A survey on heuristic malware detection techniques. *The 5th Conference on Information and Knowledge Technology*. Diakses pada 8 Juni, 2019, diambil dari https://www.researchgate.net/publication/260729684_A_survey_on_heuristic_malware_detection_techniques.

Bhojani, N. (2014, October). Malware Analysis. Diakses pada 5 Juni, 2019, diambil dari https://www.researchgate.net/publication/267777154_Malware_Analysis.

Budiman, J. (2016). Analysis on Remote Access Trojan Role in Advance Persistent Threat. Diakses pada 5 Juni, 2019, diambil dari https://figshare.com/articles/Analysis_on_Remote_Access_Trojan_Role_in_Advance_Persistent_Threat_A_Concern_for_Cyber_Criminal_Investigations/3510224/1.

Cloonan, J. (2017, April 11). Advanced Malware Detection - Signatures vs. Behavior Analysis. Diakses pada 23 September, 2018, diambil dari https://www.infosecurity-magazine.com/opinions/malware-detection-signatures/

Eze, A. O., & Chukwunonso, C. (2018). Malware Analysis and Mitigation in Information Preservation. *IOSR Journal of Computer Engineering (IOSR-JCE),20*(4), 1st ser., 53-62. Diakses pada 1 Juni, 2019, diambil dari http://www.iosrjournals.org/iosr-jce/papers/Vol20-issue4/Version-1/H2004015362.pdf

Gardåsen, K. T. (2014). Detecting Remote Administration Trojans through Dynamic Analysis using Finite-State. *MachinesMaster of Science in Information Security 30 ECTS*. Diakses pada 18 Mei, 2019, diambil dari https://brage.bibsys.no/xmlui/bitstream/handle/11250/198379/KTGardasen.pdf.

Gavitt, B. D. (2008). Forensic Analysis of the Windows Registry in Memory. *The Digital Forensic Research Conference DFRWS 2008 USA*. Diakses pada 5 Juni, 2019, diambil dari https://www.sciencedirect.com/science/article/pii/S1742287608000297.

Gierow, H., & Benzmüller, R. (2018, September 07). More attacks are launched from the web. Read more to find out about the most recent malware targeting users. Diakses pada 25 September, 2018, diambil dari https://www.gdatasoftware.com/blog/2018/09/31037-malware-figures-first-half-2018-danger-web

Gupta, S., Sharma, H., & Kaur, S. (2016). Malware Characterization Using Windows API Call Sequences. *Security, Privacy, and Applied Cryptography*

*Engineering Lecture Notes in Computer Science,*271-280. Diakses pada 22 Mei, 2019, diambil dari https://link.springer.com/chapter/10.1007/978-3-319-49445-6_15.

Insikt Group. (2019, March 14). Talking to RATs: Assessing Corporate Risk by Analyzing Remote Access Trojan Infections. Diakses pada 25 Juni, 2019, diambil dari https://www.recordedfuture.com/rat-corporate-risk-assessment/

Meshram, M. G. (2015). Investigating the Artifacts Using Windows Registry and Log Files. *International Journal of Computer Science and Mobile Computing,4*(6), 625-631. Diakses pada 4 Juni, 2019, diambil dari https://www.semanticscholar.org/paper/Investigating-the-Artifacts-Using-Windows-Registry-Meshram-Kapgate/fd29b30b1df9917a498e7d28bba7b62fc96c576a.

Mujumdar, A., & Masiwal, G. (2013). Analysis of Signature-Based and Behavior-Based Anti-Malware Approaches. *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 2*(6). Diakses pada 20 Mei, 2019, diambil dari https://www.semanticscholar.org/paper/Analysis-of-Signature-Based-and-Behavior-Based-Mujumdar-Masiwal/418bbd845325f7634f8b99d91fac722bef1c2bb5.

Rao, V., & Hande, K. (2017). A comparative study of static, dynamic and hybrid analysis techniques for android malware detection. *The International Journal of Engineering Development and Research,5*(2). Diakses pada 2 Juli, 2019, diambil dari https://www.researchgate.net/publication/288905288_A_comparison_of_static_dynamic_and_hybrid_analysis_for_malware_detection.

Saputra, R. W. (2016). A Survey of Cyber Crime in Indonesia. *2016 International Conference on ICT For Smart Society*. Diakses pada 15 September, 2018, diambil dari https://ieeexplore.ieee.org/document/7792846.

Sihwail, R., Omar, K., & Ariffin, K. A. (2018). A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis. *International*

Journal on Advanced Science, Engineering and Information Technology,8(4-2), 1662. Diakses 2 Juli, 2019, diambil dari http://www.insightsociety.org/ojaseit/index.php/ijaseit/article/view/6827

Sikorski, M., & Honig, A. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. Diakses pada 25 September, 2018, diambil dari https://repo.zenk-security.com/Virus-Infections-Detections-Preventions/Practical_Malware_Analysis.pdf.

Tahir, R. (2018). International Journal of Education and Management Engineering. *A Study on Malware and Malware Detection Techniques,8*(2), 20-30. Diakses pada 15 Mei, 2019, diambil dari https://www.researchgate.net/publication/324592375_A_Study_on_Malware_and_Malware_Detection_Techniques.

Uppal, D., Mehra, V., & Verma, V. (2014). International Journal on Computational Science & Applications. *Basic Survey on Malware Analysis, Tools and Techniques,4*(1), 103-112. Diakses pada 5 April, 2019, diambil dari https://www.semanticscholar.org/paper/Basic-survey-on-Malware-Analysis,-Tools-and-Uppal-Mehra/b25479a230816e8566df0937d9ff9265754f826d.

Zalavadiya, N. (2017). International Journal of Innovative Research in Computer and Communication Engineering. *A Methodology of Malware Analysis, Tools and Technique for Windows Platform – RAT Analysis,5*(3). Diakses pada 25 September, 2018, diambil dari http://www.ijircce.com/upload/2017/march/253_A Methodology.pdf

Zolkipli, M. F., & Jantan, A. (2010). 2010 Second International Conference on Network Applications, Protocols and Services. *Malware Behavior Analysis: Learning and Understanding Current Malware Threats*. Diakses pada 14 Mei, 2019, diambil dari https://ieeexplore.ieee.org/document/5635801.