REFERENCES

Aaron Walker, M. F. A. and Sengupta, S., "Cuckoo's, Malware Threat Scoring and Classification: Friend or Foe," in "Cuckoo's, Malware Threat Scoring and Classification: Friend or Foe, 2019," IEEE, 2019.

Academy, U. R., "McRat Malware Analysis," , 2013, URL https://quequero.org/2013/04/mcrat-malware-analysis-part1/.

Afianian, A., Niksefat, S., Sadeghiyan, B., and Baptiste, D., "Malware Dynamic Analysis Evasion Techniques: A Survey," *ACM Computing Surveys (CSUR)*, volume 52(6) pp. 1–28, 2019.

Aroms, E. et al., "NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems," , 2012.

Assor, Y., "Anti-vm and anti-sandbox explained," , 2016.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P. et al., "Cyber SA: Situational awareness for cyber defense," in "Cyber situational awareness," pp. 3–13, Springer, 2010.

BitDefender, "Mid Year Threat Landscape Report," , 2019, URL https://www.bitdefender.com/files/News/CaseStudies/study/293/Bitdefender-WhitePaper-Mid-Year-Threat-Landscape-Report-2019.pdf.

Calvet, J., Lévesque, F. L., Fernandez, J. M., Marion, J., Traourouder, E., and Menet, F., "WaveAtlas: surfing through the landscape of current malware packers," in "Proc. Virus Bulletin Conf," , 2015.

Chen, P., Huygens, C., Desmet, L., and Joosen, W., "Advanced or not? A comparative study of the use of anti-debugging and anti-VM techniques in generic and targeted malware," in "IFIP International Conference on ICT Systems Security and Privacy Protection," pp. 323–336, Springer, 2016.

CIS, "Top 10 Malware January 2018," , 2018, URL https://www.cisecurity.org/blog/top-10-malware-january-2018/.

CIS, "Top 10 Malware January 2019," , 2019, URL https://www.cisecurity.org/blog/top-10-malware-january-2019/.

CIS, "Top 10 Malware January 2019," , 2020, URL https://www.cisecurity.org/blog/top-10-malware-january-2020/.

David, B., Filiol, E., and Gallienne, K., "Structural analysis of binary executable headers for malware detection optimization," *Journal of Computer Virology and Hacking Techniques*, volume 13(2) pp. 87–93, 2017.

Devi, D. and Nandi, S., "PE file features in detection of packed executables," *International Journal of Computer Theory and Engineering*, volume 4(3) p. 476, 2012.

Dinaburg, A., Royal, P., Sharif, M., and Lee, W., "Ether: malware analysis via hardware virtualization extensions," in "Proceedings of the 15th ACM conference on Computer and communications security," pp. 51–62, 2008.

Dini, G., Martinelli, F., Matteucci, I., Petrocchi, M., Saracino, A., and Sgandurra, D., "Risk analysis of Android applications: A user-centric solution," *Future Generation Computer Systems*, volume 80 pp. 505–518, 2018.

Elisan, C., *Advanced Malware Analysis*, McGraw-Hill Education, 2015.

Gandotra, E., Bansal, D., and Sofat, S., "Malware threat assessment using fuzzy logic paradigm," *Cybernetics and Systems*, volume 48(1) pp. 29–48, 2017.

Gao, S. and Lin, Q., "Debugging classification and anti-debugging strategies," in "Fourth International Conference on Machine Vision (ICMV 2011): Computer Vision and Image Analysis; Pattern Recognition and Basic Technologies," volume 8350, p. 83503C, International Society for Optics and Photonics, 2012.

Goldberg, R. P., "Survey of virtual machine research," *Computer*, volume 7(6) pp. 34–45, 1974.

Guo, F., Ferrie, P., and Chiueh, T.-C., "A study of the packer problem and its solutions," in "International Workshop on Recent Advances in Intrusion Detection," pp. 98–115, Springer, 2008.

Institute, I., "De-Obfuscating and Reversing the User-Mode Agent Dropper," , 2015, URL https://resources.infosecinstitute.com/step-by-step-tutorial-on-reverse-engineering-malware-the-zeroaccessmaxsmiscer-c#gref.

Jain, A. K. and Dubes, R. C., *Algorithms for clustering data*, Prentice-Hall, Inc., 1988.

Khan, T., Alam, M., Akhunzada, A., Hur, A., Asif, M., and Khan, M. K., "Towards augmented proactive cyberthreat intelligence," *Journal of Parallel and Distributed Computing*, volume 124 pp. 47–59, 2019.

Lee, W., "Malware and Attack Technologies Knowledge Area Issue," , 2019.

Lim, C., Ramli, K., Kotualubun, Y. S. et al., "Mal-flux: Rendering hidden code of packed binary executable," *Digital Investigation*, volume 28 pp. 83–95, 2019.

Liu, T., Xu, N., Liu, Q., Wang, Y., and Wen, W., "A system-level perspective to understand the vulnerability of deep learning systems," in "Proceedings of the 24th Asia and South Pacific Design Automation Conference," pp. 506–511, 2019.

Love, J., "A Brief history of malware, its evolution and impact," , 2018, URL https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/.

Maasberg, M., Ko, M., and Beebe, N. L., "Exploring a systematic approach to malware threat assessment," in "2016 49th Hawaii International Conference on System Sciences (HICSS)," pp. 5517–5526, IEEE, 2016.

Mack, M., *Cyber Security*, EDTECH, 2018.

Malin, C. H., Casey, E., and Aquilina, J. M., *Malware forensics: investigating and analyzing malicious code*, Syngress, 2008.

MalwareBytes, "2019 State of Malware Report," , 2019, URL https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf.

Martignoni, L., Christodorescu, M., and Jha, S., "Omniunpack: Fast, generic, and safe unpacking of malware," in "Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)," pp. 431–441, IEEE, 2007.

Microsoft, "Structured Exception Handling," , 2018, URL `https://docs.microsoft.com/en-us/windows/desktop/Debug/structured-exception-handling`.

Milosevic, N., "History of malware," , 2013.

Mohajit, R., Lim, C., and Syailendra, Y., "A Static and Dynamic Heuristic Analysis to Calculate Malware Threat Score," , 2020.

Monnappa, K., *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*, Packt Publishing Ltd, 2018.

Oktavianto, D. and Muhardianto, I., *Cuckoo Malware Analysis*, **, Packt Publishing, 2013.

Oosthoek, K. and Doerr, C., "SoK: ATT&CK Techniques and Trends in Windows Malware," in "International Conference on Security and Privacy in Communication Systems," pp. 406–425, Springer, 2019.

Or-Meir, O., Nissim, N., Elovici, Y., and Rokach, L., "Dynamic malware analysis in the modern era—A state of the art survey," *ACM Computing Surveys (CSUR)*, volume 52(5) pp. 1–48, 2019.

Osaghae, E. O., "Classifying packed programs as malicious software detected," *International Journal of Information Technology and Electrical Engineering*, volume 5 pp. 22–25, 2016.

Raffetseder, T., Kruegel, C., and Kirda, E., "Detecting system emulators," in "International Conference on Information Security," pp. 1–18, Springer, 2007.

Rahman, M., *Basic Graph Theory*, Undergraduate Topics in Computer Science, Springer International Publishing, 2017.

Sahay, S. K., Sharma, A., and Rathore, H., "Evolution of Malware and Its Detection Techniques," in "Information and Communication Technology for Sustainable Development," pp. 139–150, Springer, 2020.

Sikorski, M. and Honig, A., *Practical malware analysis: the hands-on guide to dissecting malicious software*, no starch press, 2012.

Song, D., Brumley, D., Yin, H., Caballero, J., Jager, I., Kang, M. G., Liang, Z., Newsome, J., Poosankam, P., and Saxena, P., "BitBlaze: A New Approach to Computer Security via Binary Analysis," in "Proceedings of the 4th International Conference on Information Systems Security. Keynote invited paper.", Hyderabad, India, 2008.

VirusBulletin, "Anti-unpacker tricks - part one," , 2008, URL `https://www.virusbulletin.com/virusbulletin/2008/12/anti-unpacker-tricks-part-one`.

Wu, J., *Advances in K-means clustering: a data mining thinking*, Springer Science & Business Media, 2012.

Zakeri, M., Faraji Daneshgar, F., and Abbaspour, M., "A static heuristic approach to detecting malware targets," *Security and Communication Networks*, volume 8(17) pp. 3015–3027, 2015.

Zhang, F., Leach, K., Stavrou, A., Wang, H., and Sun, K., "Using hardware features for increased debugging transparency," in "2015 IEEE Symposium on Security and Privacy," pp. 55–69, IEEE, 2015.