REFERENCES

Afianian, A., Niksefat, S., Sadeghiyan, B., and Baptiste, D., "Malware dynamic analysis evasion techniques: A survey," *arXiv preprint arXiv:1811.01190*, 2018.

Aghakhani, H., Gritti, F., Meccay, F., Lindorferz, M., Ortolanix, S., Balzarotti, D., Vigna, G., and Kruegel, C., "When Malware is Packin'Heat; Limits of Machine Learning Classifiers Based on Static Analysis Features," in "Network and Distributed Systems Security (NDSS) Symposium 2020," , 2020.

Alazab, M., Layton, R., Venkatraman, S., and Watters, P., "Malware detection based on structural and behavioural features of api calls," , 2010.

Amini, A., Banitsas, K., and Cosmas, J., "A comparison between heuristic and machine learning techniques in fall detection using Kinect v2," in "2016 IEEE International Symposium on Medical Measurements and Applications (MeMeA)," pp. 1–6, IEEE, 2016.

Anonymous, "Day 60: Windows API Use in SpyEye Banking Trojan," , 2020, URL `https://medium.com/@int0x33/day-60-windows-api-use-in-spyeye-banking-trojan-ca8e8694bccd`, (accessed June 13, 2020).

Arnborg, S., Brynielsson, J., Artman, H., and Wallenius, K., "Information awareness in command and control: Precision, quality, utility," in "Proceedings of the Third International Conference on Information Fusion," volume 2, pp. THB1–25, IEEE, 2000.

A.S.L, "Exeinfo PE," , 2020, URL `http://www.exeinfo.xn.pl/`, (accessed May 29, 2020).

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.

Bazrafshan, Z., Hashemi, H., Mehdi, S. H. F., and Hamzeh, A., "A survey on heuristic malware detection techniques," in "The 5th Conference on Information and Knowledge Technology," pp. 113–120, IEEE, 2013.

Bellard, F., "QEMU, a fast and portable dynamic translator," in "USENIX Annual Technical Conference, FREENIX Track," volume 41, p. 46, 2005.

Bilar, D., "Opcodes as predictor for malware," *International journal of electronic security and digital forensics*, volume 1(2) pp. 156–168, 2007.

Blunden, B., *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System (2nd edition)*, 2009.

Bobritsky, E., Breiman, E., and Moyal, O., "Systems and methods for malware evasion management," , 2017, uS Patent 9,846,775.

Center for Internet Security, "CISecurity Top 10 Malware January 2018," , 2018a, URL https://www.cisecurity.org/blog/top-10-malware-january-2018/, (accessed May 13, 2020).

Center for Internet Security, "CISecurity Top 10 Malware July 2018," , 2018b, URL https://www.cisecurity.org/blog/top-10-malware-july-2018/, (accessed May 13, 2020).

Center for Internet Security, "CISecurity Top 10 Malware March 2018," , 2018c, URL https://www.cisecurity.org/blog/top-10-malware-march-2018/, (accessed May 13, 2020).

Center for Internet Security, "CISecurity Top 10 Malware January 2019," , 2019a, URL https://www.cisecurity.org/blog/top-10-malware-march-2019/, (accessed May 13, 2020).

Center for Internet Security, "CISecurity Top 10 Malware June 2019," , 2019b, URL https://www.cisecurity.org/blog/top-10-malware-june-2019/, (accessed May 13, 2020).

Center for Internet Security, "CISecurity Top 10 Malware March 2019," , 2019c, URL https://www.cisecurity.org/blog/top-10-malware-march-2019/, (accessed May 13, 2020).

Center for Internet Security, "Top 10 Malware 2019," , 2019d, URL https://fossbytes.com/top-malware-2019/, (accessed May 13, 2020).

Center for Internet Security, "CISecurity Top 10 Malware February 2020," , 2020a, URL https://www.cisecurity.org/blog/top-10-malware-february-2020/, (accessed May 13, 2020).

Center for Internet Security, "CISecurity Top 10 Malware January 2020," , 2020b, URL https://www.cisecurity.org/blog/top-10-malware-january-2020/, (accessed May 13, 2020).

Chailytko, A. and Skuratovich, S., "Defeating sandbox evasion: how to increase the successful emulation rate in your virtual environment," in "ShmooCon 2017," , 2017.

Choi, J., Kim, H., Choi, J., and Song, J., "A Malware Classification Method Based on Generic Malware Information," in "International Conference on Neural Information Processing," pp. 329–336, Springer, 2015.

Choi, M.-J., Ban, J., Kim, J., Kim, H., and Moon, Y.-S., "All-in-One Framework for Detection, Unpacking, and Verification for Malware Analysis," *Security and Communication Networks*, volume 2019, 2019.

Choi, Y.-s., Kim, I.-k., Oh, J.-t., and Ryou, J.-c., "PE File Header analysis-based packed PE file detection technique (PHAD)," in "International Symposium on Computer Science and its Applications," pp. 28–31, IEEE, 2008.

CrowdStrike, "Automated Malware Analysis and Sandbox: Falcon Sandbox," , 2020, URL https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/, (accessed May 13, 2020).

Dai, C., Pang, J., Zhang, X., Liang, G., and Bai, H., "A novel information fusion model for assessment of malware threat," *International Journal of Security and Its Applications*, volume 1(1) p. 8, 2016.

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.

Dube, T. E., Raines, R. A., Grimaila, M. R., Bauer, K. W., and Rogers, S. K., "Malware target recognition of unknown threats," *IEEE Systems Journal*, volume 7(3) pp. 467–477, 2012.

Dubyk, M., "Leveraging the PE Rich Header for Static Malware Detection and Linking," , 2020.

Egele, M., Scholte, T., Kirda, E., and Kruegel, C., "A survey on automated dynamic malware-analysis techniques and tools," *ACM computing surveys (CSUR)*, volume 44(2) pp. 1–42, 2008.

Endsley, M. R., "Design and evaluation for situation awareness enhancement," in "Proceedings of the Human Factors Society annual meeting," volume 32, pp. 97–101, SAGE Publications Sage CA: Los Angeles, CA, 1988.

Franke, U. and Brynielsson, J., "Cyber situational awareness–a systematic review of the literature," *Computers & security*, volume 46 pp. 18–31, 2014.

Gandotra, E., Bansal, D., and Sofat, S., "Malware analysis and classification: A survey," *Journal of Information Security*, volume 2014, 2014.

Gandotra, E., Bansal, D., and Sofat, S., "Malware Threat Assessment Using Fuzzy Logic Paradigm," *Cybernetics and Systems*, volume 48(1) pp. 29–48, 2017, URL http://dx.doi.org/10.1080/01969722.2016.1262704.

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

Guarnieri, C., "Cuckoo Sandbox," , 2019, URL https://cuckoosandbox.org/, (accessed May 13, 2020).

Guarnieri, C., "Cuckoo Community Signatures," , 2020, URL https://github.com/cuckoosandbox/community/tree/master/modules/signatures/windows, (accessed June 07, 2020).

Gupta, S., Sharma, H., and Kaur, S., "Malware characterization using windows API call sequences," in "International Conference on Security, Privacy, and Applied Cryptography Engineering," pp. 271–280, Springer, 2016.

hiddenillusion, "PEScanner," , 2014, URL https://github.com/hiddenillusion/AnalyzePE/blob/master/pescanner.py, (accessed May 29, 2020).

Hosseini, A., "Ten process injection techniques: A technical survey of common and trending process injection techniques," , 2017, URL https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trendi
(accessed June 07, 2020).

Hudak, T., "MASTIFF," , 2019, URL https://git.korelogic.com/mastiff.git/, (accessed May 29, 2020).

Ivchenko, G. and Honov, S., "On the jaccard similarity test," *Journal of Mathematical Sciences*, volume 88(6) pp. 789–794, 1998.

Jamalpur, S., Navya, Y. S., Raja, P., Tagore, G., and Rao, G. R. K., "Dynamic Malware Analysis Using Cuckoo Sandbox," in "2018 Second international conference on inventive communication and computational technologies (ICICCT)," pp. 1056–1060, IEEE, 2018.

JusticeRage, "Manalyze," , 2020, URL https://github.com/JusticeRage/Manalyze, (accessed May 29, 2020).

Kantchelian, A., Tschantz, M., Carl, Afroz, S., Miller, B., Shankar, V., Bachwani, R., Joseph, A. D., and Tygar, J. D., "Better malware ground truth: Techniques for weighting anti-virus vendor labels," *AISec 2015 - Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security, co-located with CCS 2015*, pp. 45–56, 2015.

Karim, M. E., Walenstein, A., Lakhotia, A., and Parida, L., "Malware phylogeny generation using permutations of code," *Journal in Computer Virology*, volume 1(1-2) pp. 13–23, 2005.

Kim, S., "PE header analysis for malware detection," , 2018.

Kramer, S. and Bradfield, J. C., "A general definition of malware," *Journal in Computer Virology*, volume 6(2) pp. 105–114, 2010.

Lau, B. and Svajcer, V., "Measuring virtual machine detection in malware using DSD tracer," *Journal in Computer Virology*, volume 6(3) pp. 181–195, 2010.

Lim, C., Kotualubun, Y. S., Ramli, K., and Suryadi, "Mal-Xtract: Hidden Code Extraction using Memory Analysis," in "Journal of Physics: Conference Series," volume 801, p. 012058, IOP Publishing, 2017.

Lim, C. and Nicsen, "Mal-Eve: Static detection model for evasive malware," *Proceedings of the 2015 10th International Conference on Communications and Networking in China, CHINACOM 2015*, pp. 283–288, 2016.

Lim, C., Ramli, Suryadi, Kalamullah, and Kotualubun, Y. S., "Mal-Flux: Rendering hidden code of packed binary executable," *Digital Investigation*, volume 28 pp. 83–95, 2019.

Lindorfer, M., Kolbitsch, C., and Comparetti, P. M., "Detecting Environment-Sensitive Malware," pp. 338–357, 2011.

Lyda, R. and Hamrock, J., "Using entropy analysis to find encrypted and packed malware," *IEEE Security & Privacy*, volume 5(2) pp. 40–45, 2007.

Maasberg, M., Ko, M., and Beebe, N. L., "Exploring a systematic approach to malware threat assessment," *Proceedings of the Annual Hawaii International Conference on System Sciences*, volume 2016-March pp. 5517–5526, 2016.

Malwarebytes Labs, "2020 Malwarebytes Labs State of Malware Report February 2020," , 2020, URL https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf, (accessed June 07, 2020).

Marpaung, J. A., Sain, M., and Lee, H. J., "Survey on malware evasion techniques: State of the art and challenges," *International Conference on Advanced Communication Technology, ICACT*, (Mic) pp. 744–749, 2012.

McAfee, "What Is Fileless Malware," , 2016, URL https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html, (accessed May 7, 2020).

Mehnaz, Shagufta, Mudgerikar, Anand, Bertino, and Elisa, "Rwguard: A real-time detection system against cryptographic ransomware," pp. 114–136, 2018.

Microsoft Corporation, "Microsoft portable executable and common object file format specification," , 1999.

Milošević, N., "History of Malware," *A Memoir of Central India*, pp. 22–57, 2013.

Moser, A., Kruegel, C., and Kirda, E., "Limits of Static Analysis for Malware Detection," , 2007, URL https://auto.tuwien.ac.at/{~}chris/research/doc/acsac07{_}limits.pdf{%}0Ahttps://ieeexplore-ieee-org.proxy1.ncu.edu/abstract/document/4413008.

Nieto, J., "Static analysis of a packed malware sample with Cuckoo Part 1," , 2013, URL http://www.behindthefirewalls.com/2013/10/

tatic-analysis-packed-malware-cuckoo.html, (accessed May 29, 2020).

Niu, W., Zhang, X., Yang, G., Zhu, J., and Ren, Z., "Identifying APT malware domain based on mobile DNS logging," *Mathematical Problems in Engineering*, volume 2017, 2017.

Nugraha, J. D., Budiyono, A., and Almaarif, A., "Analisis Malware Berdasarkan Api Call Memory Dengan Metode Deteksi Signature-based," *eProceedings of Engineering*, volume 6(2), 2019.

Nunes, Matthew, Burnap, Pete, Rana, Omer, Reinecke, Philipp, Lloyd, and Kaelon, "Getting to the root of the problem: A detailed comparison of kernel and user level data for dynamic malware analysis," *Journal of Information Security and Applications*, volume 48 p. 102365, 2019.

Oberhumer, M., "UPX," , 2020, URL https://upx.github.io/.

Ochsenmeier, M., "PEStudio," , 2020, URL https://www.winitor.com/, (accessed May 29, 2020).

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.

Oyama, Y., "Trends of anti-analysis operations of malwares observed in API call logs," *Journal of Computer Virology and Hacking Techniques*, volume 14(1) pp. 69–85, 2018.

Patten, D., "The Evolution to Fileless Malware," p. 13, 2017, URL https://infosecwriters.com/Papers/DPatten{_}Fileless.pdf.

Payload Security, "Hybrid Analysis Free Malware Analysis Service," , 2020, URL https://www.hybrid-analysis.com/, (accessed July 13, 2020).

Plohmann, D., Clauss, M., Enders, S., and Padilla, E., "Malpedia: a collaborative effort to inventorize the malware landscape," *Proceedings of the Botconf*, 2017.

Ponemon Institute LLC, "The Cost of Malware Containment," (January) pp. 1–19, 2015, URL http://www.ponemon.org/local/upload/file/DamballaMalwareContainmentFINAL3.pdf.

Poslušnỳ, M. and Kálnai, P., "RICH HEADERS: LEVERAGING THIS MYSTERIOUS ARTIFACT OF THE PE FORMAT," , 2019.

Santos, I., Devesa, J., Brezo, F., Nieves, J., and Bringas, P. G., "Opem: A static-dynamic approach for machine-learning-based malware detection," in "International Joint Conference CISIS'12-ICEUTE 12-SOCO 12 Special Sessions," pp. 271–280, Springer, 2013.

Saxe, J. and Sanders, H., *Malware Data Science: Attack Detection and Attribution*, No Starch Press, 2018.

Sharp, R., "An Introduction to Malware," *The Network Security Test Lab*, pp. 331–363, 2015.

Sikorski, M. and Honig, A., *Practical malware analysis: the hands-on guide to dissecting malicious software*, No Starch Press, 2012.

Singh, A., *Identifying malicious code through reverse engineering*, volume 44, Springer Science & Business Media, 2009.

snaker, "PEid," , 2020, URL https://www.aldeid.com/wiki/PEiD, (accessed May 29, 2020).

Solutionary NTT Group, "White paper: How Malware Analysis Benefits Incident Response," Technical report, 2012, URL https://informationsecurity.report/Resources/Whitepapers/51e831f9-aeef-41a4-b2e9-5162a2ac5f65_How%20Malware%20Analysis.pdf, (accessed July 26, 2020).

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., Whitley, S. M., and Wolf, R. D., "Finding cyber threats with ATT&CK-based analytics," *The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202*, 2017.

Suwanda, A., Lim, C., and Lukas, *Malware Threat Scoring Using Static and Dynamic Analysis Features*, Master's thesis, Tangerang, Indonesia, 2020.

Symantec LLC, "Internet Security Threat Report VOLUME 24, FEBRUARY 2019," *Network Security*, volume 24(February), 2019, URL http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947.

The MITRE Corporation, "Mitre ATT&CK Navigator Enterprise," , 2020, URL https://attack.mitre.org/, (accessed July 10, 2020).

Thomassen, C., "Decompositions of highly connected graphs into paths of length 3," *Journal of Graph Theory*, volume 58(4) pp. 286–292, 2008.

Ugarte-Pedrero, X., Santos, I., and Bringas, P. G., "Structural feature based anomaly detection for packed executable identification," in "Computational intelligence in security for information systems," pp. 230–237, Springer, 2011.

Vasilescu, M., Gheorghe, L., and Tapus, N., "Practical malware analysis based on sandboxing," in "2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference," pp. 1–6, IEEE, 2014.

Vijayalakshmi, Y., Natarajan, N., Manimegalai, P., and Babu, S. S., "Study on Emerging Trends in Malware Variants," *International Journal of Pure and Applied Mathematics*, volume 116(22) pp. 479–489, 2017.

VirusTotal Team, "VirusTotal," , 2020, URL https://www.virustotal.com/gui/intelligence-overview, (accessed July 12, 2020).

Wong, W. and Stamp, M., "Hunting for metamorphic engines," *Journal in Computer Virology*, volume 2(3) pp. 211–229, 2006.

Xie, P., Lu, X., Su, J., Wang, Y., and Li, M., "iPanda: A comprehensive malware analysis tool," in "The International Conference on Information Networking 2013 (ICOIN)," pp. 481–486, IEEE, 2013.

Yantis, D., "Windows Functions in Malware Analysis – Cheat Sheet," , 2020, URL https://gist.github.com/404NetworkError/a81591849f5b6b5fe09f517efc189c1d, (accessed June 13, 2020).

Ye, Y., Li, T., Adjeroh, D., and Iyengar, S. S., "A survey on malware detection using data mining techniques," *ACM Computing Surveys (CSUR)*, volume 50(3) pp. 1–40, 2017.

Yin, H. and Song, D., "Temu: Binary code analysis via whole-system layered annotative execution," *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2010-3*, 2010.

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

zed-0xff, "PEDump," , 2020, URL `https://github.com/zed-0xff/pedump`, (accessed May 29, 2020).

Zhao, G., Xu, K., Xu, L., and Wu, B., "Detecting APT malware infections based on malicious DNS and traffic analysis," *IEEE Access*, volume 3 pp. 1132–1142, 2015.