[52] R. Mosli, R. Li, B. Yuan, and Y. Pan, “A behavior-based approach for malware detection,” in IFIP Advances in Information and Communication Technology, 2017, vol. 511, pp. 187–201.
[53] G. Willems, T. Holz, and F. Freiling, “Toward automated dynamic malware analysis using CWSandbox,” IEEE Security and Privacy, vol. 5, no. 2. pp. 32–39, 2007.
[54] M. H. Ligh, S. Adair, B. Hartstein, and M. Richard, Malware analyst’s cookbook and DVD: tools and techniques for fighting malicious code. Wiley Publishing, 2011.
[55] Adlice Software, “Rootkits hooks,” 2014. [Online]. Available: https://www.adlice.com/.
[56] S. Kim, J. Park, K. Lee, I. You, and K. Yim, “A Brief Survey on Rootkit Techniques in Malicious Codes,” J. Internet Serv. Inf. Secur., vol. 3, no. 4, pp. 134–147, 2012.
[57] A. Hosseini, “Ten Process Injection Techniques: A Technical Survey Of Common And Trending Process Injection Techniques,” 2017. [Online]. Available: https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process.
[58] J. Berdajs and Z. Bosnic, “Extending applications using an advanced approach to DLL injection and API hooking,” Softw. - Pract. Exp., vol. 40, no. 7, pp. 567–584, 2010.
[59] J. Butler, J. L. Undercoffer, and J. Pinkston, “Hidden processes: The implication for intrusion detection,” in IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 2003, pp. 116–121.
[60] S. T. Jones, A. C. Arpaci-Dusseau, and R. H. Arpaci-Dusseau, “VMM-based hidden process detection and identification using Lycosid,” in Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments - VEE ’08, 2008, pp. 91–100.
[61] A. Schuster, “Searching for processes and threads in Microsoft Windows memory dumps,” Digit. Investig., vol. 3, no. SUPPL., pp. 10–16, 2006.
[62] K. Lee, H. Hwang, K. Kim, and B. N. Noh, “Robust bootstrapping memory analysis against anti-forensics,” Digit. Investig., vol. 18, pp. S23–S32, 2016.
[63] A. Moser, C. Kruegel, and E. Kirda, “Limits of static analysis for malware detection,” in Proceedings - Annual Computer Security Applications Conference, ACSAC, 2007, pp. 421–430.
[64] J. Okolica and G. Peterson, “A compiled memory analysis tool,” in IFIP Advances in Information and Communication Technology, 2010, vol. 337 AICT, pp. 195–204.
[65] V. ATLURI, Anoop Chowdary; TRAN, Botnets threat analysis and detection. Cham, 2017.
[66] Endgame, “Ember,” 2018. [Online]. Available: https://www.endgame.com/blog/technical-blog/introducing-ember-open-source-classifier-and-dataset.
[67] Microsoft, “Microsoft Malware Classification Challenge (BIG 2015),” 2015. [Online]. Available: https://www.kaggle.com/c/malware-classification.