REFERENCES

AV-TEST, "AV-TEST âĂŞ The Independent IT-Security Institute," , 2017, URL https://www.av-test.org/en/statistics/malware/.

Aycock, J., *Computer viruses and malware*, volume 22, Springer Science & Business Media, 2006.

Bat-Erdene, M., Park, H., Li, H., Lee, H., and Choi, M.-S., "Entropy analysis to classify unknown packing algorithms for malware detection," volume 16(3) pp. 227–248, 2017.

Bayer, U., Kruegel, C., and Kirda, E., *TTAnalyze: A tool for analyzing malware*, na, 2006.

Bayuk, J., *CyberForensics: Understanding Information Security Investigations*, Springer Science & Business Media, 2010.

Bazrafshan, Z., Hashemi, H., Fard, S. M. H., and Hamzeh, A., "A survey on heuristic malware detection techniques," in "Information and Knowledge Technology (IKT), 2013 5th Conference on," pp. 113–120, IEEE, 2013.

Beek, C., Matrosov, A., Paget, F., Peterson, E., Pradeep, A., Schmugar, C., Simon, R., Sommer, D., Sun, B., Surgihalli, S., Walter, J., and Wosotowsky, A., "McAfee Labs Threat Report 2015," , 2015, URL http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q4-2014.pdf.

Blunden, B., *The Rootkit arsenal: Escape and evasion in the dark corners of the system*, Jones & Bartlett Publishers, 2012.

Borello, J.-M. and MÃl', L., "Code obfuscation techniques for metamorphic viruses," volume 4(3) pp. 211–220, 2008.

Brosch, T. and Morgenstern, M., "Runtime packers: The hidden problem," , 2006.

Bruening, D., "Efficient, transparent, and comprehensive runtime code manipulation," , 2004.

Burks, A. W., *Essays on cellular automata*, University of Illinois Press, 1970.

Caballero, J., Yin, H., Liang, Z., and Song, D., "Polyglot: Automatic extraction of protocol message format using dynamic binary analysis," in "Proceedings of the 14th ACM conference on Computer and communications security," pp. 317–329, ACM, 2007.

Christodorescu, M. and Jha, S., "Static analysis of executables to detect malicious patterns," , 2006.

Cohen, F., "Computer viruses: theory and experiments," volume 6(1) pp. 22–35, 1987.

Damodaran, A., Di Troia, F., Visaggio, C. A., Austin, T. H., and Stamp, M., "A comparison of static, dynamic, and hybrid analysis for malware detection," volume 13(1) pp. 1–12, 2017.

Danchev, D., "MalwareâĂŞfuture trends," volume 9, 2006.

Deng, Z., Zhang, X., and Xu, D., "Spider: Stealthy binary program instrumentation and debugging via hardware virtualization," in "Proceedings of the 29th Annual Computer Security Applications Conference," pp. 289–298, ACM, 2013.

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, ACM, 2008.

Dolan-Gavitt, B. F., Hodosh, J., Hulin, P., Leek, T., and Whelan, R., "Repeatable reverse engineering for the greater good with panda," , 2014.

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

GDATA, "History of Malware," , 2014, URL `https://www.gdatasoftware.com/securitylabs/information/history-of-malware`.

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

Hazelwood, K., "Dynamic binary modification: Tools, techniques, and applications," volume 6(2) pp. 1–81, 2011.

Henderson, A., Prakash, A., Yan, L. K., Hu, X., Wang, X., Zhou, R., and Yin, H., "Make it work, make it right, make it fast: Building a platform-neutral whole-system dynamic binary analysis platform," in "Proceedings of the 2014 International Symposium on Software Testing and Analysis," pp. 248–258, ACM, 2014.

Hunt, G. and Brubacher, D., "Detours: Binaryinterception ofwin 3 2 functions," in "3rd usenix windows nt symposium," , 1999.

Idika, N. and Mathur, A. P., "A survey of malware detection techniques," , 2007.

Institute, I., "A History of Malware, Part One," , 2014, URL `http://resources.infosecinstitute.com/history-malware-part-one-1949-1988/`.

Isawa, R., Kamizono, M., and Inoue, D., "Generic Unpacking Method Based on Detecting Original Entry Point," in "Neural Information Processing," pp. 593–600, Springer, 2013.

Islam, R., Tian, R., Batten, L. M., and Versteeg, S., "Classification of malware based on integrated static and dynamic features," volume 36(2) pp. 646–656, 2013.

Jeong, G., Choo, E., Lee, J., Bat-Erdene, M., and Lee, H., "Generic unpacking using entropy analysis," in "Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on," pp. 98–105, IEEE, 2010.

Jiang, X., Xu, D., Wang, H. J., and Spafford, E. H., "Virtual playgrounds for worm behavior investigation," in "International Workshop on Recent Advances in Intrusion Detection," pp. 1–21, Springer, 2005.

Jordan, M., "Dealing with metamorphism," volume 1(10) pp. 4–6, 2002.

Kang, M. G., Poosankam, P., and Yin, H., "Renovo: A hidden code extractor for packed executables," in "Proceedings of the 2007 ACM workshop on Recurring malcode," pp. 46–53, ACM, 2007.

Kendall, K. and McMillan, C., "Practical malware analysis," in "Black Hat Conference, USA," p. 10, 2007.

Lanzi, A., Sharif, M. I., and Lee, W., "K-Tracer: A System for Extracting Kernel Malware Behavior." in "NDSS," , 2009.

Li, X., Loh, P. K., and Tan, F., "Mechanisms of polymorphic and metamorphic viruses," in "Intelligence and Security Informatics Conference (EISIC), 2011 European," pp. 149–154, IEEE, 2011.

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

Long, A., "Detecting Malicious Software with Behavioral Malware Analysis," , 2017.

Lueker, G. S., "Improved bounds on the average length of longest common subsequences," volume 56(3) p. 17, 2009.

Luk, C.-K., Cohn, R., Muth, R., Patil, H., Klauser, A., Lowney, G., Wallace, S., Reddi, V. J., and Hazelwood, K., "Pin: building customized program analysis tools with dynamic instrumentation," in "Acm sigplan notices," volume 40, pp. 190–200, ACM, 2005.

Lyda, R. and Hamrock, J., "Using entropy analysis to find encrypted and packed malware," volume 5(2), 2007.

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

McAfeeLabs, "McAfee Whitepaper: The Good, The Bad, And The Unknown," , 2015, URL `http://www.mcafee.com/sg/resources/white-papers/wp-good-bad-the-unknown.pdf`.

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

Moser, A., Kruegel, C., and Kirda, E., "Limits of static analysis for malware detection," in "Computer security applications conference, 2007. ACSAC 2007. Twenty-third annual," pp. 421–430, IEEE, 2007.

Navarro, G., "A guided tour to approximate string matching," volume 33(1) pp. 31–88, 2001.

Net-informatics, "Portable Executables (PE) File Format," , 2011, URL http://vb.net-informations.com/framework/portable-executable.htm.

Nethercote, N. and Seward, J., "Valgrind: a framework for heavyweight dynamic binary instrumentation," in "ACM Sigplan notices," volume 42, pp. 89–100, ACM, 2007.

Noreen, S., Murtaza, S., Shafiq, M. Z., and Farooq, M., "Evolvable malware," in "Proceedings of the 11th Annual conference on Genetic and evolutionary computation," pp. 1569–1576, ACM, 2009.

O'Kane, P., Sezer, S., and McLaughlin, K., "Obfuscation: The hidden malware," volume 9(5) pp. 41–47, 2011.

Pomeran, H., "Detecting Malware with Memory Forensic," , 2012, URL http://www.deer-run.com/hal/Detect_Malware_w_Memory_Forensics.pdf.

Rad, B. B., Masrom, M., and Ibrahim, S., "Camouflage in malware: from encryption to metamorphism," volume 12(8) pp. 74–83, 2012.

Radware, "The History of Malware," , 2014, URL http://www.radware.com/Resources/malware_timeline.aspx.

Roundy, K. A. and Miller, B. P., "Binary-code obfuscations in prevalent packer tools," volume 46(1) p. 4, 2013.

Royal, P., Halpin, M., Dagon, D., Edmonds, R., and Lee, W., "Polyunpack: Automating the hidden-code extraction of unpack-executing malware," in "Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual," pp. 289–300, IEEE, 2006.

Says, T. p., "Cybercrime Reaches New Heights in the Third Quarter," , 2016, URL http://www.pandasecurity.com/mediacenter/pandalabs/pandalabs-q3/.

Schultz, M. G., Eskin, E., Zadok, F., and Stolfo, S. J., "Data mining methods for detection of new malicious executables," in "Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on," pp. 38–49, IEEE, 2001.

Shannon, C., "A mathematical theory of communication," volume 27(3) pp. 379–423, 1948.

Sharif, M., Lanzi, A., Giffin, J., and Lee, W., "Automatic reverse engineering of malware emulators," in "2009 30th IEEE Symposium on Security and Privacy," pp. 94–109, IEEE, 2009.

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., Liang, Z., Newsome, J., Poosankam, P., and Saxena, P., "BitBlaze: A new approach to computer security via binary analysis," pp. 1–25, 2008.

Song, W., "a framework for automated similarity analysis of malware," , 2014.

Spafford, E. H., "Computer viruses as artificial life," volume 1(3) pp. 249–265, 1994.

Sun, L., Versteeg, S., BoztaÅ§, S., and Yann, T., "Pattern recognition techniques for the classification of malware packers," in "Information security and privacy," pp. 370–390, Springer, 2010.

Sung, A. H., Xu, J., Chavez, P., and Mukkamala, S., "Static analyzer of vicious executables (save)," in "Computer Security Applications Conference, 2004. 20th Annual," pp. 326–334, IEEE, 2004.

Szor, P., *The art of computer virus research and defense*, Pearson Education, 2005.

Ugarte-Pedrero, X., Balzarotti, D., Santos, I., and Bringas, P. G., "SoK: deep packer inspection: a longitudinal study of the complexity of run-time packers," in "2015 IEEE Symposium on Security and Privacy," pp. 659–673, IEEE, 2015.

Ugarte-Pedrero, X., Santos, I., Sanz, B., Laorden, C., and Bringas, P. G., "Countering entropy measure attacks on packed software detection," in "Consumer Communications and Networking Conference (CCNC), 2012 IEEE," pp. 164–168, IEEE, 2012.

Vasudevan, A. and Yerraballi, R., "Stealth breakpoints," in "Computer security applications conference, 21st Annual," pp. 10–pp, IEEE, 2005.

Vasudevan, A. and Yerraballi, R., "Cobra: Fine-grained malware analysis using stealth localized-executions," in "Security and Privacy, 2006 IEEE Symposium on," pp. 15–pp, IEEE, 2006a.

Vasudevan, A. and Yerraballi, R., "Spike: engineering malware analysis tools using unobtrusive binary-instrumentation," in "Proceedings of the 29th Australasian Computer Science Conference-Volume 48," pp. 311–320, Australian Computer Society, Inc., 2006b.

Verma, A., Rao, M., Gupta, A., Jeberson, W., and Singh, V., "A literature review on malware and its analysis," volume 5(16) pp. 71–82, 2013.

Wang, Y.-M., Beck, D., Jiang, X., Roussev, R., Verbowski, C., Chen, S., and King, S., "Automated web patrol with strider honeymonkeys," in "Proceedings of the 2006 Network and Distributed System Security Symposium," pp. 35–49, 2006.

Willems, C., Holz, T., and Freiling, F., "Toward automated dynamic malware analysis using cwsandbox," volume 5(2), 2007.

Wu, Y., Chiueh, T.-c., and Zhao, C., "Efficient and automatic instrumentation for packed binaries," in "International Conference on Information Security and Assurance," pp. 307–316, Springer, 2009.

Ye, Y., Li, T., Adjeroh, D., and Iyengar, S. S., "A survey on malware detection using data mining techniques," volume 50(3) p. 41, 2017.

Yegneswaran, V., Saidi, H., Porras, P., Sharif, M., and Mark, W., "Eureka: A framework for enabling static analysis on malware," pp. 481–500, 2008.