Bibliography

"x86 Opcode and Instruction Reference," , 2017, URL http://ref.x86asm.net/coder32.html, (Date last accessed 1 March 2017).

Armadillo, "Armadillo, Overlays packer and obfuscator," , 2017, URL http://the-armadillo-software-protection-system.software.informer.com, (Date last accessed 1 March 2017).

AVTEST, "AV TEST - The Independent IT Security Institute," , 2017, URL https://www.av-test.org/en/statistics/malware/, (Date last accessed 1 March 2017).

Aycock, J., *Computer viruses and malware*, volume 22, Springer Science & Business Media, 2006, URL http://dx.doi.org/10.1007/0-387-34188-9.

Bat-Erdene, M., Park, H., Li, H., Lee, H., and Choi, M.-S., "Entropy analysis to classify unknown packing algorithms for malware detection," *International Journal of Information Security*, pp. 1–22, 2016.

Bayer, U., Moser, A., Kruegel, C., and Kirda, E., "Dynamic analysis of malicious code," *Journal in Computer Virology*, volume 2(1) pp. 67–77, 2006, URL https://dx.doi.org/10.1007/s11416-006-0012-2.

Baysa, D., Low, R. M., and Stamp, M., "Structural entropy and metamorphic malware," *Journal of computer virology and hacking techniques*, volume 9(4) pp. 179–192, 2013, URL https://dx.doi.org/10.1007/s11416-013-0185-4.

Benninger, C. A., *Maitland: analysis of packed and encrypted malware via paravirtualization extensions*, Ph.D. thesis, University of Victoria, 2012.

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

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

Bruening, D., Garnett, T., and Amarasinghe, S., "An infrastructure for adaptive dynamic optimization," in "Code Generation and Optimization, 2003. CGO 2003. International Symposium on," pp. 265–275, IEEE, 2003.

Cheatham, M. and Hitzler, P., "String similarity metrics for ontology alignment," in "International Semantic Web Conference," pp. 294–309, Springer, 2013.

Christensson, P., ""Malware Definition." Tech Terms. Sharpened Productions," , 2006, URL http://techterms.com/definition/malware, (Date last accessed 1 March 2017).

Christodorescu, M. and Jha, S., "Static Analysis of Executables to Detect Malicious Patterns," in "USENIX Security Symposium," , 2003.

Cohen, M., Bilby, D., and Caronni, G., "Distributed forensics and incident response in the enterprise," *digital investigation*, volume 8 pp. S101–S110, 2011.

Danchev, D., "Malware–future trends," *Information Technology*, 2006.

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, URL https://doi.org/10.1145/1455770.1455779.

Dolan-Gavitt, B. F., Hodosh, J., Hulin, P., Leek, T., and Whelan, R., "Repeatable reverse engineering for the greater good with panda," Technical report, Department of Computer Science, Columbia University, 2014, URL http://dx.doi.org/10.7916/D8WM1C1P.

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) p. 6, 2012.

Elisan, C., *Advanced Malware Analysis*, McGraw-Hill Education, 2015, URL https://books.google.co.id/books?id=17SUAwAAQBAJ.

Euzenat, J. and Valtchev, P., "Similarity-based ontology alignment in OWL-lite," in "Proceedings of the 16th European conference on artificial intelligence," pp. 323–327, IOS press, 2004.

Eye, F., "FireEye," , 2017, URL https://www.fireeye.com, (Date last accessed 1 March 2017).

Fang, H., Wu, Y., Wang, S., and Huang, Y., "Multi-stage binary code obfuscation using improved virtual machine," in "International Conference on Information Security," pp. 168–181, Springer, 2011.

Foundation, S. S., "Packer Statistics," , 2016, URL https://www.shadowserver.org/wiki/pmwiki.php/Stats/PackerStatistics, (Date last accessed 1 March 2017).

FSG, "FSG 2.0, F[ast] S[mall] G[ood] perfect compressor for executable files," , 2017, URL http://www.downloadpcsoft.com/Windows/Development/Other/FSG_24767.html, (Date last accessed 1 March 2017).

Gandotra, E., Bansal, D., and Sofat, S., "Malware analysis and classification: A survey," *Journal of Information Security*, volume 2014, 2014, URL https://dx.doi.org/10.4236/jis.2014.52006.

GDATA, "History of Malware," *GDATA*, 2014, URL https://www.gdatasoftware.com/securitylabs/information/history-of-malware, (Date last accessed 1 March 2017).

Gendreau, J. and Pisupati, R., "Portable executable software architecture," , 2003, uS Patent App. 10/350,090.

Grégio, A., Bonacin, R., Nabuco, O., Afonso, V. M., De Geus, P. L., and Jino, M., "Ontology for malware behavior: A core model proposal," in "WETICE Conference (WETICE), 2014 IEEE 23rd International," pp. 453–458, IEEE, 2014.

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.

HexRays, "IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger," , 2017, URL https://www.hex-rays.com/products/ida/, (Date last accessed 1 March 2017).

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

Institute, I., "API Hooking," , 2013, URL http://resources.infosecinstitute.com/api-hooking/, (Date last accessed 1 March 2017).

Jadhav, A., Vidyarthi, D., and Hemavathy, M., "Evolution of evasive malwares: A survey," in "Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on," pp. 641–646, IEEE, 2016.

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, URL http://dx.doi.org/10.1109/MALWARE.2010.5665789.

Jordan, M., "Dealing with metamorphism," *Virus Bulletin*, 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, URL https://doi.org/10.1145/1314389.1314399.

Lengyel, T. K., Maresca, S., Payne, B. D., Webster, G. D., Vogl, S., and Kiayias, A., "Scalability, Fidelity and Stealth in the DRAKVUF Dynamic Malware Analysis System," in "Proceedings of the 30th Annual Computer Security Applications Conference," , 2014.

Leong, J., "Automated static analysis of virtual-machine packers," , 2013.

Li, M., Chen, X., Li, X., Ma, B., and Vitányi, P. M., "The similarity metric," *IEEE transactions on Information Theory*, volume 50(12) pp. 3250–3264, 2004, URL https://doi.org/10.1109/TIT.2004.838101.

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, URL http://dx.doi.org/10.1109/EISIC.2011.77.

Ligh, M., Adair, S., Hartstein, B., and Richard, M., *Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code*, Wiley Publishing, 2010.

Lim, C., Sulistyan, D. Y., Ramli, K. et al., "Experiences in Instrumented Binary Analysis for Malware," *Advanced Science Letters*, volume 21(10) pp. 3333–3336, 2015, URL https://doi.org/10.1166/asl.2015.6487.

Lock, H.-Y. and Kliarsky, A., "(Indicators of Compromise) in Malware Forensics," *SANS Institute InfoSec Reading Room*, 2013.

Lueker, G. S., "Improved bounds on the average length of longest common subsequences," *Journal of the ACM (JACM)*, volume 56(3) p. 17, 2009, URL https://doi.org/10.1145/1516512.1516519.

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," *IEEE Security & Privacy*, volume 5(2) pp. 40–45, 2007, URL https://doi.org/10.1109/MSP.2007.48.

MANDIANT, "Open IOC," , 2017, URL http://www.openioc.org, (Date last accessed 1 March 2017).

Marak, V., *Windows Malware Analysis Essentials*, Packt Publishing Ltd, 2015.

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, URL http://dx.doi.org/10.1109/ACSAC.2007.15.

McAfeeLabs, "History of Malware," *McAfee Labs*, 2014, URL http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q2-2014.pdf, (Date last accessed 1 March 2017).

McAfeeLabs, "McAfee Whitepaper: The Good, The Bad, And The Unknown," *McAfee Labs*, 2015, URL http://www.mcafee.com/sg/resources/white-papers/wp-good-bad-the-unknown.pdf, (Date last accessed 1 March 2017).

Mew, "MEW," , 2017, URL http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/MEW-SE.shtml, (Date last accessed 1 March 2017).

Molebox, "Molebox, a free executable compression and encryptor," , 2017, URL https://molebox.en.softonic.com, (Date last accessed 1 March 2017).

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," *ACM computing surveys (CSUR)*, volume 33(1) pp. 31–88, 2001.

Net-informatics, "Portable Executables (PE) File Format," *Net-informatics*, 2011, URL http://vb.net-informations.com/framework/portable-executable.htm, (Date last accessed 1 March 2017).

Nethercote, N., *Dynamic binary analysis and instrumentation*, Ph.D. thesis, PhD thesis, University of Cambridge, 2004.

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

Nikam, R., "Introduction to Malware and Malware Analysis," *ClubHackMag*, 2011, URL http://www.chmag.in/article/sep2011/introduction-malware-malware-analysis, (Date last accessed 1 March 2017).

Nilakantan, S., Lerner, S., Hempstead, M., and Taskin, B., "Can You Trust Your Memory Trace? A Comparison of Memory Traces from Binary Instrumentation and Simulation," in "VLSI Design (VLSID), 2015 28th International Conference on," pp. 135–140, IEEE, 2015.

Obrst, L., Chase, P., and Markeloff, R., "Developing an Ontology of the Cyber Security Domain." in "STIDS," pp. 49–56, 2012.

O'Kane, P., Sezer, S., and McLaughlin, K., "Obfuscation: The hidden malware," *Security & Privacy, IEEE*, volume 9(5) pp. 41–47, 2011, URL `http://dx.doi.org/10.1109/MSP.2011.98`.

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

PANDA, "PANDA - open-source Architecture-Neural Dynamic Analysis," , 2017, URL `https://github.com/panda-re/panda`.

PEC2, "PECompact2, Windows Executable Compressor," , 2017, URL `http://pecompact2.software.informer.com`, (Date last accessed 1 March 2017).

PEStudio, "PEStudio," , 2017, URL `https://winitor.com`, (Date last accessed 1 March 2017).

Pietrek, M., "Peering inside the PE: a tour of the win32 (R) portable executable file format," *Microsoft Systems Journal-US Edition*, pp. 15–38, 1994.

Pomeran, H., "Detecting Malware with Memory Forensic," *SANS Institute*, 2012, URL `http://www.deer-run.com/~hal/Detect_Malware_w_Memory_Forensics.pdf`, (Date last accessed 1 March 2017).

QEMU, "QEMU - Open Source Processor Emulator," , 2017, URL `http://wiki.qemu.org/Main_Page`, (Date last accessed 1 March 2017).

Rad, B. B., Masrom, M., and Ibrahim, S., "Camouflage in malware: from encryption to metamorphism," *International Journal of Computer Science and Network Security*, volume 12(8) pp. 74–83, 2012, URL `http://paper.ijcsns.org/07_book/201208/20120813.pdf`.

Radware, "The History of Malware," *Radware*, 2014, URL http://www.radware.com/Resources/malware_timeline.aspx, (Date last accessed 1 March 2017).

Rhoades, D., "Machine actionable indicators of compromise," in "Security Technology (ICCST), 2014 International Carnahan Conference on," pp. 1–5, IEEE, 2014.

Rolles, R., "Unpacking virtualization obfuscators," in "3rd USENIX Workshop on Offensive Technologies.(WOOT)," , 2009, URL http://dl.acm.org/citation.cfm?id=1855877.

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, URL http://dx.doi.org/10.1109/ACSAC.2006.38.

Russinovich, M. E., Solomon, D. A., and Allchin, J., *Microsoft Windows Internals: Microsoft Windows Server 2003, Windows XP, and Windows 2000*, volume 4, Microsoft Press Redmond, 2005.

Security, J., "How does Joe Sandbox Works," , 2011, URL http://www.joesecurity.org/products.php?index=3, (Date last accessed 1 March 2017).

Shannon, C. E., "W. Weaver The mathematical theory of communication," *Urbana: University of Illinois Press*, volume 29, 1949.

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, URL http://dx.doi.org/10.1109/SP.2009.27.

Sharif, M., Yegneswaran, V., Saidi, H., Porras, P., and Lee, W., "Eureka: A Framework for Enabling Static Malware Analysis," in "Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security," pp. 481–500, Springer-Verlag, 2008, URL http://dx.doi.org/10.1007/978-3-540-88313-5_31.

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

Solutions, N., "Norman sandbox whitepaper," , 2003.

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, URL https://dx.doi.org/10.1007/978-3-540-89862-7_1.

Song, W., *a framework for automated similarity analysis of malware*, Ph.D. thesis, Concordia University, 2014.

Sun, L., Versteeg, S., Boztaş, S., and Yann, T., "Pattern recognition techniques for the classification of malware packers," in "Information security and privacy," pp. 370–390, Springer, 2010, URL http://dx.doi.org/10.1007/978-3-642-14081-5_23.

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

Themida, "Themida, a commercial executable protector," , 2017, URL http://www.oreans.com/, (Date last accessed 1 March 2017).

Timm, K., "Malware Validation Techniques," , 2010, URL http://blogs.cisco.com/security/malware_validation_techniques, (Date last accessed 1 March 2017).

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 "SSP 2015, IEEE Symposium on Security and Privacy, May 18-20, 2015, San Jose, CA, USA," San Jose, UNITED STATES, 2015, URL http://dx.doi.org/10.1109/SP.2015.46.

UPX, "UPX, a free and open source, cross-platform runtime packer," , 2017, URL http://upx.sourceforge.net/, (Date last accessed 1 March 2017).

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

Visual, C. and Unit, B., "Microsoft portable executable and common object file format specification," , 1999.

VMprotect, "VMProtect, a commercial executable virtualization," , 2017, URL http://vmpsoft.com/, (Date last accessed 1 March 2017).

Volatility, "Volatility: open source memory forensics," , 2017, URL http://www.volatilityfoundation.org, (Date last accessed 1 March 2017).

Willems, C., Holz, T., and Freiling, F., "Toward automated dynamic malware analysis using cwsandbox," *IEEE Security and Privacy*, volume 5(2) pp. 32–39, 2007, URL https://doi.org/10.1109/MSP.2007.45.

Winitor, "PEStudio," , 2017, URL https://www.winitor.com, (Date last accessed 1 March 2017).

WinUPack, "WinUPack, a freeware runtime packer," , 2016, URL http://www.softpedia.com/get/PORTABLE-SOFTWARE/Compression-Tools/Windows-Portable-Applications-Portable-WinUpack.shtml, (Date last accessed 1 March 2017).

Wu, Z., Gianvecchio, S., Xie, M., and Wang, H., "Mimimorphism: A new approach to binary code obfuscation," in "Proceedings of the 17th ACM conference on Computer and communications security," pp. 536–546, ACM, 2010, URL https://doi.org/10.1145/1866307.1866368.

Yin, H. and Song, D., *Automatic Malware Analysis: An Emulator Based Approach*, Springer Science & Business Media, 2012, URL https://dx.doi.org/10.1007/978-1-4614-5523-3.