

REFERENCES

Bailey, M., Oberheide, J., Andersen, J., Mao, Z.M., Jahanian, F., & Nazario, J. 2007. *Automated Classification and Analysis of Internet Malware*.

Bayer, U. 2009. *Anubis: A Platform for the Analysis of Malicious Code*. Secure Systems Lab Technical University Vienna. [Presentation slides.]

Bayer, U., Kruegel, C., & Kirda, E. 2006. TTAalyze: A Tool for Analyzing Malware. *15th Annual Conference of the European Institute for Computer Antivirus Research*, Hamburg, Germany, pp. 180–192.

Brumley, D., Hartwig, C., Kang, M.G., Liang, Z., Newsome, J., Poosankam, P., Song, D., & Yin, H. 2007. *BitScope Automatically Dissecting Malicious Binaries*.

Christodorescu, M., Jha, S., & Kruegel, C. 2007. Mining Specifications of Malicious Behavior. *Proceedings of the 6th joint meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE) 2007*, September 3–7, Dubrovnik, Croatia. ACM.

Dai, J., Guha, R., & Lee, J. 2009. Feature Set Selection in Data Mining Techniques for Unknown Virus Detection – A Comparison Study. *CSIRW*, April 13-15, Oak Ridge, Tennessee, USA. ACM.

Ding, J., Jin, J., Bouvry, P., Hu, Y., & Guan, H. 2009. Behavior-based Proactive Detection of Unknown Malicious Codes. *Fourth International Conference on Internet Monitoring and Protection 2009*. IEEE.

Distler, D., & Hornat, C. 2007. *Malware Analysis: An Introduction*. SANS Institute.

Fawcett, T. 2006. An Introduction to ROC Analysis. *Pattern Recognition Letters*, 27, pp. 861–874.

Filiol, E., Jacob, G., & Liard, M.L. 2006. Evaluation methodology and theoretical model for antiviral behavioral detection strategies. *Third Journal of Computer Virology 2007*, pp. 23–37. France: Springer-Verlag.

Guizani, W., Marion, J., & Reynaud-Plantey, D. 2009. Server-Side Dynamic Code Analysis. *4th International Conference on Malicious and Unwanted Software - Malware 2009*, pp. 55-62. France: HAL.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I.H. 2009. *The WEKA Data Mining Software: An Update*, SIGKDD Explorations, Volume 11, Issue 1.

Hall, M.A. 2000. Correlation-based Feature Selection for Discrete and Numeric Class Machine Learning. *Proceeding of the 17th International Conference Data Mining*, Morgan Kaufmann Publishers Inc, pp. 359–366.

Ichinose, S. 2009. *Advanced Malware Analysis and Coordination*. Jakarta: JPCERT Coordination Center. [Course notes.]

Ichinose, S. 2009. *Malware Analysis Basics*. Jakarta: JPCERT Coordination Center. [Course notes.]

Jacob, G., Debar, H., & Filiol, E. 2008. Behavioral detection of malware from a survey towards an established taxonomy. *Fourth Journal of Computer Virology 2008*, pp. 251–266. France: Springer-Verlag.

Liu, H., & Motoda, H. 1998. *Feature Selection for Knowledge Discovery and Data Mining*. Kluwer Academic Publishers, Norwell, MA.

Rieck, K., Holz, T., Willems, C., Duessel, P., & Laskov, P. 2008. Learning and Classification of Malware Behavior. *DIMVA 2008*, LNCS 5137, pp. 108–125. Berlin Heidelberg: Springer-Verlag.

Rieck, K., Trinius, P., Willems, C., & Holz, T. *Automatic Analysis of Malware Behavior using Machine Learning*.

Russell, S., & Norwig, P. 2003. *Artificial Intelligence: A Modern Approach*. Prentice Hall.

Skoudis, E., & Zeltser, L. 2003. *Malware: Fighting Malicious Code*. Upper Saddle River, NJ: Prentice Hall PTR.

Tan, P., Steinbach, M., & Kumar, V. 2006. *Introduction to Data Mining*. Pearson Addison-Wesley.

Trinius, P., Willems, C., Holz, T., & Rieck, K. 2009. *A Malware Instruction Set for Behavior-Based Analysis*.

Wagener, G., State, R., & Dulaunoy, A. 2007. Malware behaviour analysis. *Third Journal of Computer Virology 2007*. France: Springer-Verlag.

Willems, C., Holz, T., & Freiling, F. 2007. Toward Automated Dynamic Malware Analysis Using CWSandbox. *IEEE Security and Privacy*, 5(2):32-39, March/April 2007.

Zhao, H., Zheng, N., Li, J., Yao, J., & Hou, Q. 2009. Unknown Malware Detection Based on the Full Virtualization and SVM. *International Conference on Management of e-Commerce and e-Government 2009*. IEEE.