เอกสารอ้างอิง

[1] C. Li, W. Jiang, and E.X. Zou, "Botnet: Survey and Case Study," *Proceedings of The Fourth International Conference on Innovative Computing, Information and Control*, IEEE,2009

[2] T. Strayer, D. Lapsley, R. Walsh, and C. Livadas, "Botnet Detection: Countering the Largest Security Threat," Vol. 36, Chapter Botnet Detection Based on Network Behavior, *Springer*, 2008.

[3] C. Livadas, R. Walsh, D. Lapsley, and T. Strayer, "Using machine learning techniques to identify botnet traffic," *Proceedings of 2006 31st IEEE Conference on Local Computer Network,* pp. 967-974, 2006.

[4] P. Sroufe, S. Phithakkitnukoon, R. Dantu, and J. Cangussu, "Email shape analysis for spam botnet detection," *In Sixth IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, pp. 1–2, January 2009.

[5] A. Brodsky, and D. Brodsky, "A distributed content independent method for spam detection," *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets*, Cambridge, MA, p. 3, 2007.

[6] R. Villamarin-Salomon, and J.C. Brustoloni, "Bayesian bot detection based on DNS traffic similarity," *Proceedings of the 2009 ACM Symposium on Applied Computing*, Honolulu, Hawaii, pp. 2035–2041, 2009.

[7] Y. Kugisaki, Y. Kasahara, Y. Hori, and K. Sakurai, "Bot detection based on traffic analysis," In *The 2007 International Conference on Intelligent Pervasive Computing, Jeju City*, pp. 303–306, October 2007.

[8] W. Lu, G. Rammidi, and Ali A. Ghorbani, "Clustering botnet communication traffic based on n-gram feature selection." *Computer Communications,* 2010.

[9] K. Wang, and S. Stolfo, "Anomalous payload-based network intrusion detection," In *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Sophia Antipolis, France, 2004.

[10] Wei Lu, Mathbod Tavallaee, Goaletsa Rammidi, and Ali A. Ghorbani, "BotCop: An Online Botnets Traffic Classifier," *Proceedings of the 7th Annual Conference on Communication Networks and Services Research (CNSR),* 2009.

[11] Guofei Gu, Junjie Zhang, and Wenke Lee, "BotShiffer: Detecting Botnet Command and Control Channels in Network Traffic," *Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08),* San Diego, CA, February 2008.

[12] J.R. Quinlan, "C4.5: Programs for Machine Learning," Morgan Kaufman Publishers, 1993.

[13] M. Akiyama, T. Kawamoto, M. Shimamura, T. Yokoyama, Y. Kadobayashi, and S. Yamaguchi, "A proposal of metrics for botnet detection based on its cooperative behavior," In *Proceedings of the 2007 International Symposium on Applications and the Internet Workshops*, pp. 82–85,2007.

[14] D. Pelleg, and A. Moore, "X-means : Extending K-means with Efficient Estimation of the Number of Clustering"

[15] M.N. Joshi, "Parallel K - Means Algorithm on Distributed Memory Multiprocessors," *Spring,* 2003.

[16] D. Arthur, and S. Vassilvitskii, "k-means++: The Advantages of Careful Seeding," SODA, 2007.

[17] Sandeep A Thorat, Amit K Khandelwal, Bezawada Bruhadeshwar, and K Kishore, "Payload Content based Network Anomaly Detection," *IEEE International Performance Computing and Communications Conference,* 2008.

[18] G.F. Gu, P. Porras, V. Yegneswaran, M. Fong, and W.K. Lee, "BotHunter: detecting malware infection through IDS-Driven dialog correlation," *Proceedings of the 16th USENIX Security Symposium,* Boston, MA, 2007.

[19] K. Wang, and S. Stolfo, "Anomalous payload-based network intrusion detection," *Proceedings of the* 7th *International Symposium on Recent Advances in Intrusion Detection (RAID),* Sophia Antipolis, France, 2004.

[20] A. Tangpong and G. Kesidis, "A controlled environment for botnet traffic generation," [Online]. Available: http://www.cse.psu.edu/tangpong/botnet/

[21] D. Arthur, and S. Vassilvitskii, "k-means++: The Advantages of Careful Seeding," SODA, 2007.

[22] J. Tian, L. Zhu, S. Zhang, and L. Liu, "Improvement and parallelism of k-means clustering algorithm," *Tsignhue Science and Technology,* vol. 10, No. 3, pp. 277-281, 2005.

[23] q8bot. [Online]. Available: http:// www.securitydot.net/exploits/bots/

[24] Wireshark. [Online]. Available: http://www.wireshark.org

[25] VMware. [Online]. Available: http://www.vmware.com