Botnet Detection Using a Feed-Forward Backpropagation Artificial Neural Network

Abdulghani Ali Ahmed(✉)

Systems Network & Security (SysNetS) Research Group,
Faculty of Computer Systems & Software Engineering,
Universiti Malaysia Pahang, 26300 Kuantan, Malaysia
abdulghani@ump.edu.my

Abstract. Botnet represent a critical threat to computer networks because their behavior allows hackers to take control of many computers simultaneously. Botnets take over the device of their victim and performs malicious activities on its system. Although many solutions have been developed to address the detection of Botnet in real time, these solutions are still prone to several problems that may critically affect the efficiency and capability of identifying and preventing Botnet attacks. The current work proposes a technique to detect Botnet attacks using a feed-forward backpropagation artificial neural network. The proposed technique aims to detect Botnet zero-day attack in real time. This technique applies a backpropagation algorithm to the CTU-13 dataset to train and evaluate the Botnet detection classifier. It is implemented and tested in various neural network designs with different hidden layers. Results demonstrate that the proposed technique is promising in terms of accuracy and efficiency of Botnet detection.

Keywords: Botnet · Feed-forward · Artificial Neural Network Backpropagation

11. Singh, k, Guntuku, S.C., Thakur, A., Hota, C.: Big data analytics framework for peer-to-peer botnet detection using random forests. Inform. Sci. **278**, 488–497 (2014)
12. Svozil, D., Kvasnicka, V., Pospichal, J.: Introduction to multi-layer feed-forward neural networks. Chemometr. Intell. Lab. Syst. **39**(1), 43–62 (1997)
13. Garcia, S., Grill, M., Stiborek, J., Zunino, A.: An empirical comparison of botnet detection methods. Comput. Secur. **45**, 100–123 (2014)
14. Karasaridis, A., Rexroad, B., Hoeflin, D.A.: Wide-scale botnet detection and characterization. HotBots **7**, 7 (2007)
15. Gu, G., Zhang, J., Lee, W.: BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic. In: NDSS, vol. 8, pp. 1–18 (2008)
16. Al-Duwairi, B., Al-Ebbini, L.: BotDigger: A fuzzy inference system for botnet detection. In: 2010 Fifth International Conference on Internet Monitoring and Protection (ICIMP), pp. 16–21. IEEE (2010)
17. Masud, M.M., Al-Khateeb, T., Khan, L., Thuraisingham, B., Hamlen, K.W.: Flow-based identification of botnet traffic by mining multiple log files. In: First International Conference on Distributed Framework and Applications, DFmA, pp. 200–206. IEEE (2008)
18. Rumelhart, D.E., Durbin, R., Golden, R., Chauvin, Y.: Backpropagation: the basic theory. In: Backpropagation: Theory, Architectures and Applications, pp. 1–34 (1995)