Deep learning–based classification model for botnet attack detection

Abdulghani Ali Ahmed[1], Waheb A. Jabbar[2], Ali Safaa Sadiq[3], Hiran Patel[3]

[1]Safecyber Systems Corporation, 26300 Kuantan, Pahang, Malaysia
[2]Faculty of Electrical and Electronics Engineering Technology, Universiti Malaysia Pahang, 26600 Pekan, Pahang, Malaysia
[3]School of Mathematics and Computer Science, University of Wolverhampton, Wulfruna Street, Wolverhampton WV1 1LY, UK

ABSTRACT

Botnets are vectors through which hackers can seize control of multiple systems and conduct malicious activities. Researchers have proposed multiple solutions to detect and identify botnets in real time. However, these proposed solutions have difficulties in keeping pace with the rapid evolution of botnets. This paper proposes a model for detecting botnets using deep learning to identify zero-day botnet attacks in real time. The proposed model is trained and evaluated on a CTU-13 dataset with multiple neural network designs and hidden layers. Results demonstrate that the deep-learning artificial neural network model can accurately and efficiently identify botnets.

KEYWORDS: Security; Botnet; Feed-forward; artificial neural network; Backpropagation; Deep learning

DOI: https://doi.org/10.1007/s12652-020-01848-9

ACKNOWLEDGEMENTS

Funding support was provided by the fund of COMSTECH-TWAS, Joint Research Grants Program for Young Scientists in OIC countries No. 14-340 RG/ITC/AS_C.