ETSNS0008 - 2D2N: A Dynamic Degenerative Neural Network for Classification of Images of Live Network Data

Abstract

The detection of new, novel attacks on organizational networks is a problem of ever-increasing relevance in today's society. Research in the area is focused on the detection of "Zero-Day" and "Black Swan" events through the use of machine learning technologies. Where previous technologies needed a known example of malicious behavior to detect a similar event, recent advances in anomaly detection on network activity has shown promise of detecting novel attacks. In a real word environment however, novel behavior occurs relatively frequently as users utilize new software applications and new standards in networking. Changes such as these, while of notable importance to network security technicians may not present themselves as an imminent threat to a network. This paper proposes a novel method for the detection and classification of changes in networking behavior. Through the use of a Dynamic Degenerative Neural Network (2D2N), changes in recognizable user activity are dynamically classified and stored for future reference. Through the use of a time-based entropy function, infrequent activity can be analyzed and given precedence over frequent activity. This aids in the classification of abnormal activity for fast, efficient assessment by the relevant persons in an organization. The proposed method enables the detection, classification and scoring of any and all user activity on a network. Evaluation of the proposed method is based upon live data gathered from a large, multinational organization.

Index Terms - Convolutional Neural Network, Network Security, Net Flow Analysis, Image Change Detection.