Abstract

In recent years, the internet of services has been more responsive to access through the development of various application program interfaces (API). Accessing an HTTP uniform resource locator (URL) contains malicious software intended by the attacker to create security breaches through the use of APIs from various services on the internet. By default, the non-attentive URL downloads and installs malware in the background without the user's knowledge. The host does not analyze the API-URL security certificate contract due to the feature access by the user. Therefore, the current Machine Learning (ML) techniques only check malware signatures and certificates rather than analyzing URL behaviour based on the impact of a URL accessed from the internet. To address this problem, we propose a novel intelligent malicious software based on URL-API intensity feature selection (IFS) and deep spectral neural classification (DSNC) for improving Host Security. Initially, the URL — successive certificate signing (SCS) of the user link accessibility is verified based on API download rate logs. This system identifies the best malware software. The Link Redirection Stability Rate (LRSR) is estimated based on the Redirection URL by accessing the direct link and redirect link. The domain transformation matrix (DTM) was created to create a pattern to access successive features. URL-API Intensity Feature Selection selects each estimated feature, and the selected features are based

on soft-max logical activation with a recurrent neural network (RNN) optimized for deep learning. RNN is trained in the spectral domain for improving computation and efficiency. It predicts the class based on the risk of malicious weight to categorize class by reference. The proposed IFS-DSNC achieves accuracy of 95.6% than the other algorithms such as KNN, NB, CNN, LCS, GCRNC AGSCR. The experimental result shows that the proposed method provides better performance in finding malware software than the existing approaches, thereby improving the security against host breaching.

Keywords: Application program interfaces ▪ uniform resource locator ▪ security breaches ▪ machine learning ▪ intensity feature selection ▪ deep spectral neural classification ▪ link redirection stability rate ▪ RNN