عنوان مقاله:

Malware Detection and Identification using Multi-View Learning based on Sparse Representation

نویسندگان:

Seyed Mehdi Hazrati Fard - *Ph.D., School of Computer Engineering and Information Technology, Shiraz University, Shiraz, Iran*

Elham Velayati - *Department of Information Technology Sharif University, Tehran, Iran*

خلاصه مقاله:

With the widespread using Internet in any device and services, several homes and workplace applications have been provided to avoid attacks. Connecting a system or device to an insecure network can create the possibility of being infected by unwanted files. Detecting such files is a vital task in any system. Employing machine learning (ML) is the most efficient method to detect these penetrations. On the other hand, malware programmers try to design malicious files that are hard to detect. A file can hide from detection in a feature view, but concealing in all views would be very difficult. In this paper, inspiring Multi-View Learning (MVL), we proposed to incorporate some various features such as Opcodes, Bytecodes, and System-calls to achieve complementary information to identify a file. In this way, we developed a modified version of Sparse Representation based Classifier (SRC) to aggregate the effect of all modalities in a unified classifier. To show the efficiency of the proposed method, we used several real datasets. Experimental results show the high performance of the proposed approach and its ability to cope with the imbalanced conditions.

کلمات کلیدی:

Multiview Learning, Sparse representation, Malware Detection, Malware Identification, Imbalanced Condition

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1035896