

ABSTRACT

A system for detecting and preventing execution of malware on a target system includes an interface for receiving training data. The training data includes domain names known to be legitimate and domain names known to be associated with malware. The system includes a processor in communication with the interface; and non-transitory computer readable media in communication with the processor that stores instruction code. The instruction code is executed by the processor and causes the processor to train a first model to classify the domain names in the training data as being legitimate domain names or malware-associated domain names using a supervised learning methodology. The processor trains a second model to predict a correct domain name associated with domain names in the training data using an unsupervised learning methodology. The processor trains a third model to classify the domain names in the training data as being legitimate domain names or malware-associated domain names based on an output of the first learning model and an output of the second learning model. Subsequent to training of the first, second, and third models, the processor receive a new domain name and processes the new domain name through the trained models to determine whether the domain name is considered to be a legitimate domain name or a malware-associated domain name. The processor communicates a report to the target system based on the processing to thereby facilitate removal of the malware from the target system.

Fig. 1