Malware-detection-using-Machine-Learning-Algorithms

INTRODUCTION:

In sort of machine learning that's found in a lot of antimalware software tries **to learn which files are malicious** and which are benign based on databases of both malicious and benign code. Proper machine learning requires Big Data processing and cloud-based systems. Here we proposed a solution for that.

GITHUB LINK:

https://github.com/Dharsansivaloganathan/TRINIT_ELITE-BITIANS_ML02

PROPOSED SOLUTION:

Current antivirus software's are effective against known viruses, if a malware with new signature is introduced then it will be difficult to detect that it is malicious. Signature-based detection is not that effective during zero-day attacks. Till the signature is created for new (unseen) malware, distributed to the systems and added to the anti-malware database, the systems can be exploited by that malware. But Machine learning methods can be used to create more effective antimalware software which is capable of detecting previously unknown malware, zero-day attack etc. We propose an approach that learns from the header data of PE32 files. We examine various features of the PE32 header and check those which are suitable for machine learning classifier. We hypothesize that machine learning classifiers can tell apart the difference between malware and benign software. Various machine learning methods such as Support Vector Machine (SVM), Decision tree, Logistic Regression and Naive Bayes will be use.

WORKDONE AND RESULTS:

This documentation of our project which provides a machine learning prototype helping in detection of any kind of malicious attack increasing the security of a system. We use the spyder editor which is the scientific python development environment is a free IDE that is included with anaconda. We made a python code based on machine learning that can differentiate the messages, emails, applications and all other such stuffs interacting with our computer system. And be able to detect malicious or not malicious one using machine learning algorithms which uses classifier. Our final code consists of many python packages and we have given package codes in the GitHub repositories to all these packages combined to do a classification of separating malicious or non malicious one using machine learning algorithms. We are in an attempt to create a web application based on machine learning that classifies the malicious or not malicious one and intimate the user with the the source of malicious attack when it is detected.

CONCLUSION:

here we proposed a app which overcomes that.

https://drive.google.com/file/d/1-LvFNw5SbsqBL3vGbKkJ7lwAC5-h11zn/view?usp=drivesdk