Allen-thesis-s23

Repository

https://github.com/isseclab-udayton/allen-thesis-s23

Background

The Aim of this thesis is to create a Dynamic Malware detection model, which is a updated version of the already working Static Malware Detection Model (Webguard browser add-on). A machine learning model will be deployed to achieve the desired results.

Approach/Plan

Collect data/information from the browser by using functions calls. This collected information will then be passed to machine learning model which in turn will be able to help in applying/enforcing policies, preventing/avoiding malicious website, links etc.

Outcomes/results

Using the above mentioned approch we should be able to monitor functions and their properties that are being used through out the website and collect information from them, this in turn helps to train the machine learning model that is being implemented.

Concepts/Topics learned

So far i was able to understand the key difference between properties of the object being used/created as well as creating new instance of a given function so that it can be monitored and policies/other function calls can be embedded in them. This concept of intercepting the function call and applying/enforcing policies or other function calls helps to give users more control of their data as well as blocking unwanted re-direction which prevents drive by downloads and other unwanted installations.

Related work

A NOVEL APPROACH FOR ANALYZING AND CLASSIFYING MALICIOUS WEB PAGES link: https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=dayton1620393519333858&disposition=inline

Team Members

Allen Varghese

Mentor

Dr. Phu Phung

Timeline

Update for September 30th

Updated the repository with data for sprint 1 and sprint 2. created overleaf for the Webguard app updated the repository with the API test functionality Understand the working/execution of the Webguard app.

Update for October 7th

Created a function to set cookie Working on the monitoring part (gives error when trying to access the object property values).

Update for October 21st

Created monitoring functions and was also able to collect the number of times the function was called within the website in a object variable in the form of key-value pairs.Next task will be to use this on a live webpage and call them within a loop without manual intervention.