FAST AUTO BLACK BOX ANALYSIS WITH INFECTION VECTOR IDENTIFICATION

DESCRIPTION

A customized automated malware sandbox with the capability to identify the vector of infection by using the behaviour analysis logs and also to reduce dependency on manual or static analysis.

PROBLEM STATEMENT

Black box analysis is often the preferred first line used in malware analysis as it does not involve reverse engineering the malware right away, but instead, observing the behavior in a controlled environment, due to the fact that manual static analysis being time consuming.

The entry point in which the malware is able to arrive to the system, such as emails, phishing or exploit, is commonly known as infection vector. For attack investigations, infection vector identification plays an important part in order to minimize future incoming threat of similar nature. Identifying this manually is time consuming as analyst needs to identify samples on a case by case basis.

There are a few online sites that are freely offering such service, however, those were not customizable according to the specific needs of the organization.

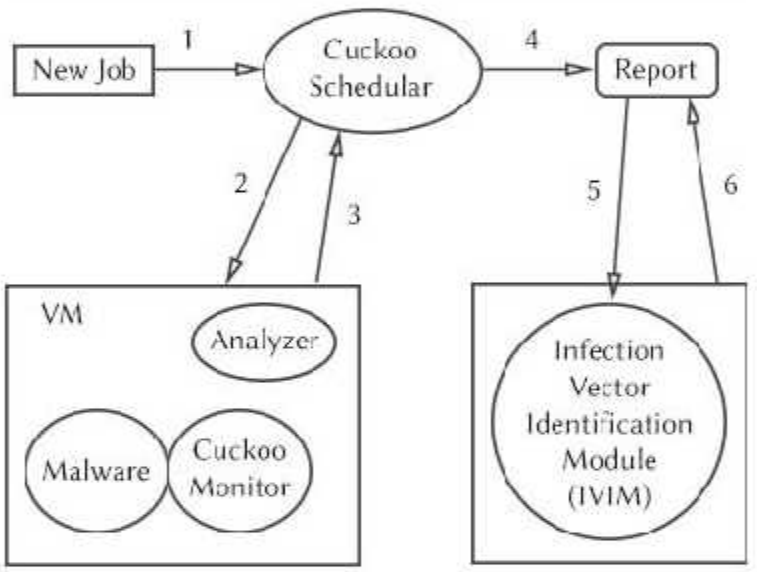
OBJECTIVE

The primary objective is to be able to create a customized automated malware sandbox system by creating an extension module that will allow analyst to identify the possible infection vector or any other possible major clue to its very existence for a given malware sample.

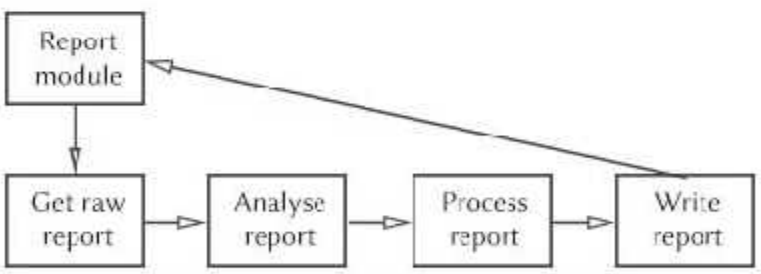
NOVELTY

This new module provides identification of possible infection vector and it should also provide an easier way for system administrators or normal end users on where to look out for and avoid getting infected. By using this malware sandbox, time will be saved because system administrators can use this blackbox to identify the vector of infection in a system and network and take mitigation steps fast.

Proposed Malware Analysis Framework Overview Diagram



Proposed Infection Vector Identification Module (IVIM) Diagram



COMMERCIAL POTENTIAL

Malware infections in the wild have increased exponentially, and time spent analyzing samples are crucial. With malware getting more complex in nature and the number of malware samples to be analyzed daily, this proves to be the biggest challenge faced by analysts. By automating the identification of infection vector of malwares, time can be saved and thus increasing the efficiency of analysts by focusing on more meaningful jobs, and by having efficient workflow, this would in turn increase the competitiveness of a company, in terms of being fast in rleasing malware signatures. As a side effect, this could probably be crucial in influencing the market shareof the company's products.

Researched by Navein Chanderan (34460)

A big thank you to Dr. Johari for his guidance in doing this project and to Mr. Jose Cequena for insights into the industry and guiding me in understanding malware analysis.